DESIGN AND DEVELOPMENT OF AN IoT-BASED FACE RECOGNITION SMART ACCESS CONTROL SYSTEM

Nnajiofor George Anayo[1] Cosmas Kemdirim Agubor[2] Longinus Sunday Ezema[3] Amadi Christopher Chidi[4]

Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria.

DOI: 10.31364/SCIRJ/v13.i04.2025.P04251020
http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

ABSTRACT
This thesis presents a smart IoT-based face recognition access control system. Initially, users must enter a password. If the password is correct, the door unlocks automatically; if incorrect, the system triggers an alarm, captures images of the user, and sends a security alert with the photos to the rightful owner via the Telegram application. The system captures the intruder's face and denies access to unauthorized users if the captured face does not match the stored one. It allows authorized users to enter and exit restricted areas and features real-time image capture and transmission of the intruder's photos.

Methodology: The system uses face recognition technology with an ESP32 camera module connected to a solenoid lock via a DC relay. A 4x4 keypad was linked to the microcontroller for password entry. The ESP32 camera was integrated with the owner's Telegram account. The system connects to a network through a router or phone hotspot, providing global accessibility.

Results: A functional prototype was developed, implemented, and tested in real-time, successfully sending intruder photos when incorrect passwords were entered. This system significantly enhances security by accurately identifying individuals based on unique facial features, reducing the risk of unauthorized access through stolen keys, access cards, or PIN codes, thus improving security for homes, offices, and other facilities.

Keywords: ESP32 Camera, IoT, RSSI, Arduino IDE, Solenoid lock, MATLAB, Telegram application, Keypad, Password, WiFi.

1.1 INTRODUCTION

Due to the prevalence of insecurity in our society today, and the rate of unwanted intrusion into restricted areas the need for a trusted security system is required in various aspects of our lives. One of such is the use of a smart access control system with automatic picture capturing and notification of intruders. For the security of lives and organisation properties, it is essential to control and monitor how homes and offices are accessed, security is the life wire of all organisations and guarantees the sustainability of any organization. Automatic monitoring and capturing of images of personnel in an access control system is very vital for proper notification of unwanted intruders who try to gain access illegally (Mukhtar, 2021).

Safety and security are the most challenging issues in modern time society, to prevent people's lives and their valuable assets from illegal handling. As a result, safety and security extend to personal social security to protect every individual’s personal information, valuable things, and their day-to-day activities. Hence, personal security services are moving towards the integration of video

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

surveillance, and door locks access control systems based on authorization information to avoid access conflicts in personalized monitored areas.

1.2 LITERATURE REVIEW

According to the work done by Divya and Neetu in Performance Analysis of Authentication System: A Systematic Literature Review, Data authentication is vital nowadays, as the development of the internet and its applications allow users to have all-time data availability, attracting attention towards security and privacy and leading to authenticating legitimate users. There are diversified means to gain access to restricted areas, like passwords, biometrics, and smartcards, even by merging two or more techniques or various factors of authentication. This paper presents a systematic literature review of papers published from 2010 to 2022 and gives an overview of all the authentication techniques available in the market. This study provides a comprehensive overview of all three authentication techniques with all the performance metrics (Accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR)), security, privacy, memory requirements, and usability (Acceptability by user)) that will help one choose a perfect authentication technique for any access control device (Singla, 2023).

This chapter will present us with numerous advantages of how to effectively implement an energy management system and coordinate electrical appliances from a single control source(Aalase et al., 2023). Alkar and Buhur (2005) carried out, an Internet-based wireless flexible solution where a home piece of equipment is connected to a slave node. The slave nodes interact with the master node through Radio Frequency (RF) and the master node has a serial RS232 link with the Personal Computer server. The nodes are based on PIC 16F877μc. PC server is formed of a user interface component, the database, and the web server components. An Internet page is set up to run on a Web server. The user interface and the Internet front end are connected to a backend database server. The control of physical objects is established and their states are monitored through the Internet (Bhat et al, 2017).

Tan and Soy (2002) developed a system for controlling home electrical appliances over the Internet by using Bluetooth wireless technology to provide a link from the appliance to the Internet and Wireless Application Protocol (WAP) to provide a data link between the Internet and a mobile phone. However, technical details relating to the controller are not revealed (Bhat et al., 2017).

Table 2.1: Summary of Selected Related Literature Reviews

S/N	TITLE	AUTHOR	YEAR	RESULTS	LIMITATION(S)
1	A smart access control system is a system that automates entry and exit	Postulka	2019	The system used biometrics to grant access to places.	No picture feedback in the event of an unauthorized attempt to gain access

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

1.2.1

	into apartments,				
2	An intrusion detection system (IDS)	Salikhov et al.,	2021	The system was able to detect movements within target areas and gives an alarm notification.	It couldn't send notifications to remote users over the internet.
3	RF Module-Based Wireless Secured Access Control System	Snehal et al.,	2018	It worked perfectly	It wasn't accessible over the internet due to the technology deployed.
4	Access control Using ZigBee	Hinal	2017)	The system worked and was able to control an electric door as proposed by the author	It wasn't accessible over the internet due to the technology deployed.

Research Gaps

After the review of related works, it was observed that the systems implemented lacked some key features such as face recognition only or password only, which this study addresses. The IFRSACS has the following smart features:

i. Ability to auto-capture unauthorized persons and send the captured photos to the concerned authority for notification of an illegal attempt to access a restricted area.

ii. Ability to notify the security personnel of any suspicious movements, especially at night hours for appropriate actions to be taken.

iii. Ability to communicate with the concerned authority remotely regardless of distance, provided that there is a strong between the sending end (IFRSACS) and the receiving end (user's smartphone).

1.3 Materials and Methods

1.3.1 Hardware materials

The following electronic components were used in the design and implementation of the system

i. ESP32 Camera module: This is an Internet Protocol (IP) camera that will be used in the remote monitoring and photo capturing of the activities during examinations at the various halls where this proposed system is installed.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

ii. **Voltage regulator:** This will be used in stepping down the voltage level to the amount the intended circuit requires without damage.

iii. **Bipolar junction transistor (BJT):** This will be used in the amplification of current in the circuit design.

iv. **Fixed resistor:** This will be used in biasing the base of the transistor mentioned in (v) for seamless performance of the device.

v. **Liquid Crystal Display (LCD):** LCD is a type of flat panel display that uses liquid crystals in its primary form of operation.

vi. **Reset button:** This will be used to refresh the system in the event of any abnormality.

vii. **Keypad:** For implementing the input panel. This is used for inputting values to the system.

viii. **Solenoid Lock:** The solenoid lock denotes a latch for electrical locking and unlocking.

1.3.2 Research Design

i. **Development of a system that permits authorized persons to enter and exit, and deny entry to unauthorized persons into restricted areas:**

This is the first research specific objective. It involves the sub-block diagrams as shown Figure 3.2. The following smaller block diagrams made up the door lock unit system. Camera module is responsible for capturing the picture of the intruder. An image is captured and passed to a face detection algorithm (e.g., using a pre-trained Haar cascade). The algorithm identifies a face and returns the coordinates of the bounding box. The cascade classifier is a multi-stage classifier where each stage consists of a strong classifier. Stages are designed to reject non-face regions quickly, allowing the classifier to focus computational resources on promising regions that may contain faces (Viola & Jones, 2022). The keypad module takes input from the user and compares with the programmed password.

The data storage unit saves the pictures in the cloud for future reference. The door lock control unit is the interfacing circuit of the DC relay that controls the opening and closing the door.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

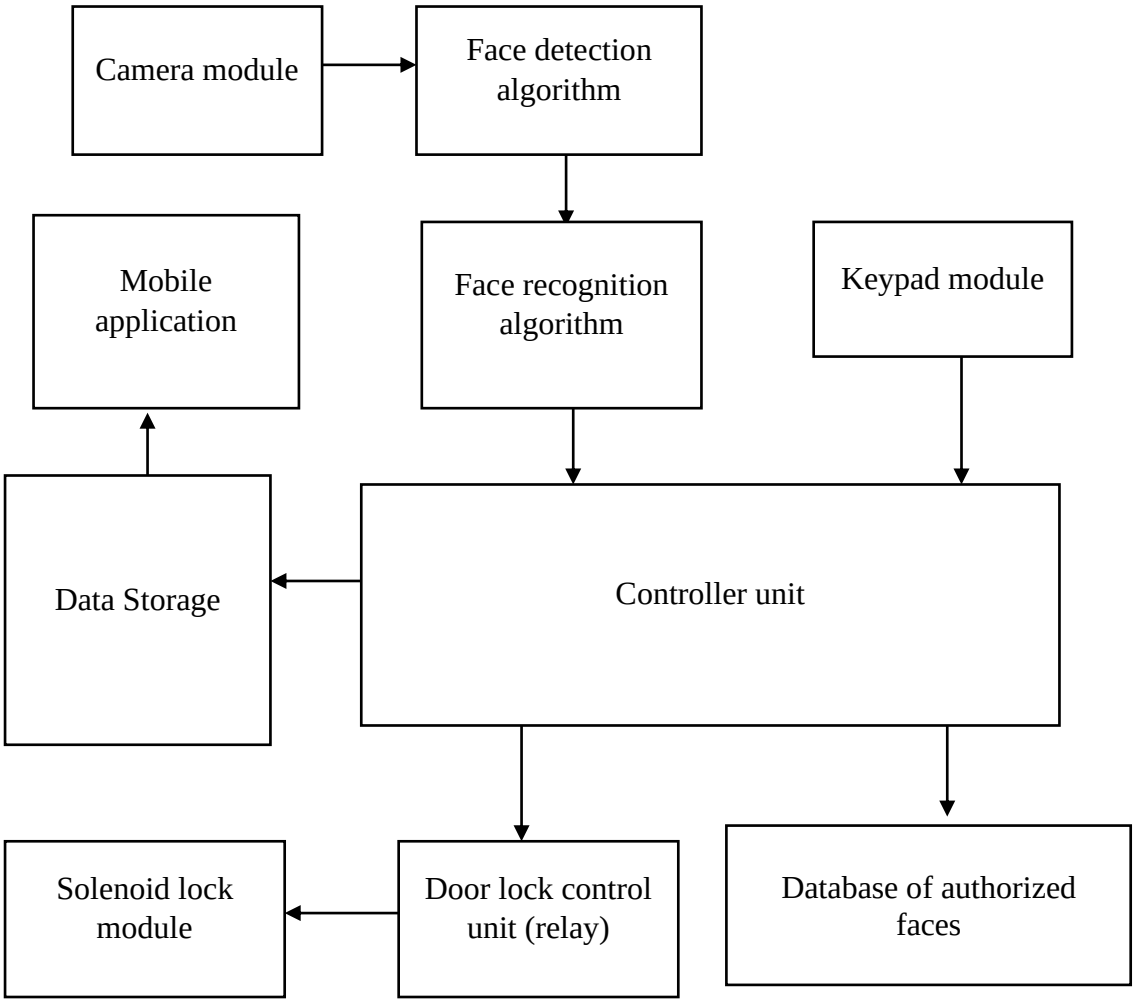

Figure 3.2: The block diagram of face recognition access control unit

The flowchart for the face recognition door lock system illustrates the step-by-step process and interactions between components. The system begins by capturing an image of the person at the door, followed by pre-processing steps like resizing and normalization to enhance detection accuracy. A face detection algorithm analyzes the image to locate a face, after which the system determines whether the face is recognized. If recognized, access is granted, and the door opens; otherwise, access is denied, and the process ends. This structured representation provides a clear overview of the system's operations and decision points. Figure 3.3 shows the detailed signal flow.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

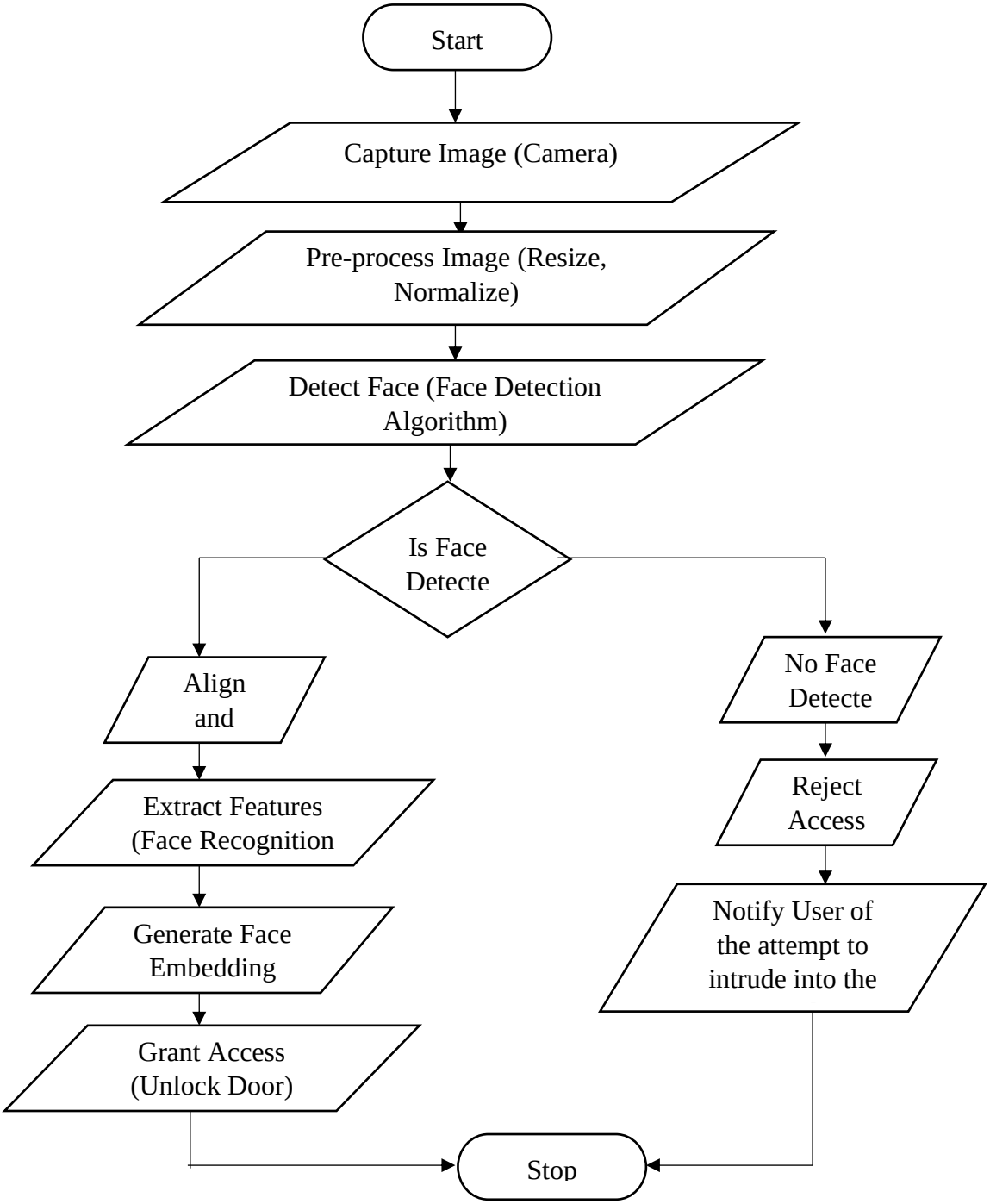

Figure 3.3: The flowchart of the face recognition and door lock control unit

i. **Implementation of a sub-system capable of real-time picture capture and notification to the security personnel, of attempts to gain unauthorized access into restricted areas**

The second objective of this work is to design and implement a sub-system capable of capturing real-time images and notifying security personnel when there are attempts to gain unauthorized access into restricted areas. This enhances the security infrastructure by providing immediate visual evidence and timely alerts. Some of the major components in the design included: The Camera Module was used for real-time picture capture. ESP32 Microcontroller controlled the camera, processed images, and handled

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

communication. The communication module used for sending notifications to security personnel was the IoT gateway, and it alerts the security personnel through various channels (e.g., SMS, email, telegram app, and security monitoring system and so on). However, this work specifically used the telegram application as the notification medium between the system and the user. The block diagram of the real-time picture capture and notification unit is represented in figure 3.4. To achieve this, the ESP-32 CAM was used to take pictures of events in real time, process these pictures and then send out a notification of its identification. Notifications are messages used on devices that alert users to information that are important. The notification feature of this thesis will be able to notify its users of the motion detected. The computer-based system we are using in this case is the ESP-32 controller, its main use will be to execute and control all the features of this system from within. The methods were adopted in achieving the specific objectives in chronological order:

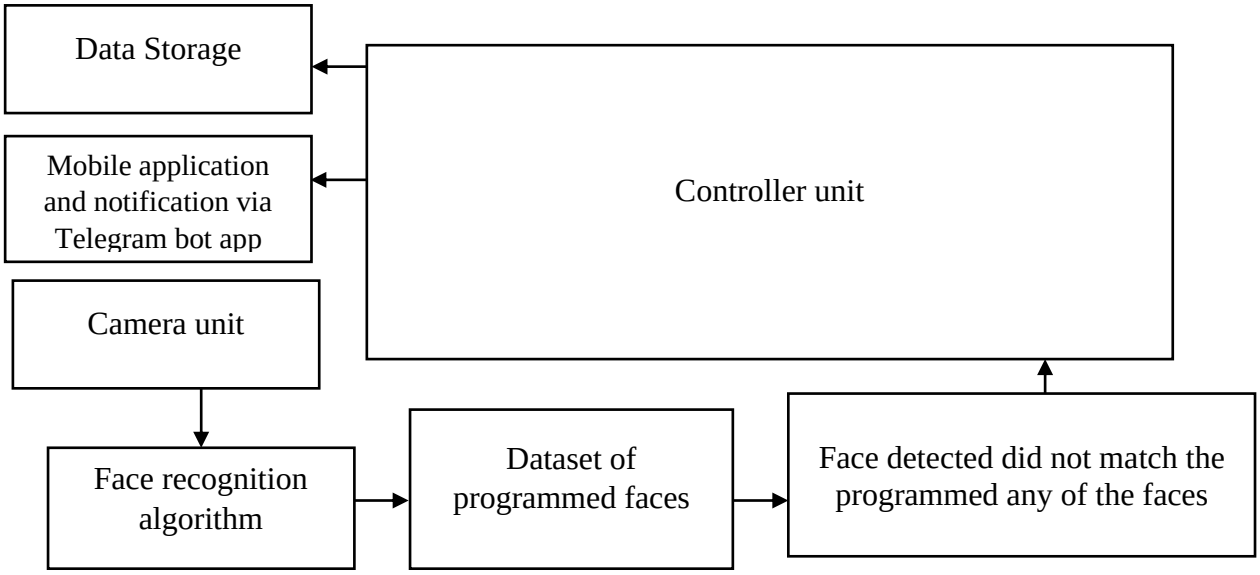

Figure 3.4: The block diagram of the real-time picture capture and notification unit

The implementation of a real-time picture capture and notification sub-system significantly enhanced the security aspect of this design by providing immediate visual verification and timely alerts of unauthorized access attempts. It leverages IoT gateway technology to ensure prompt and effective response, thereby safeguarding restricted areas against potential security breaches. Figure 3.5 shows a clearer view of the design in a flowchart.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

The power supply circuit was designed and routed into a PCB, as shown in Figures 3.7 and 3.8. EasyEDA was used for component placement and wiring, with changes automatically saved to the server for future retrieval. Figure 3.8 also includes the ESP32 Camera and follows a similar design process. The entire PCB design can be accessed online whenever needed.

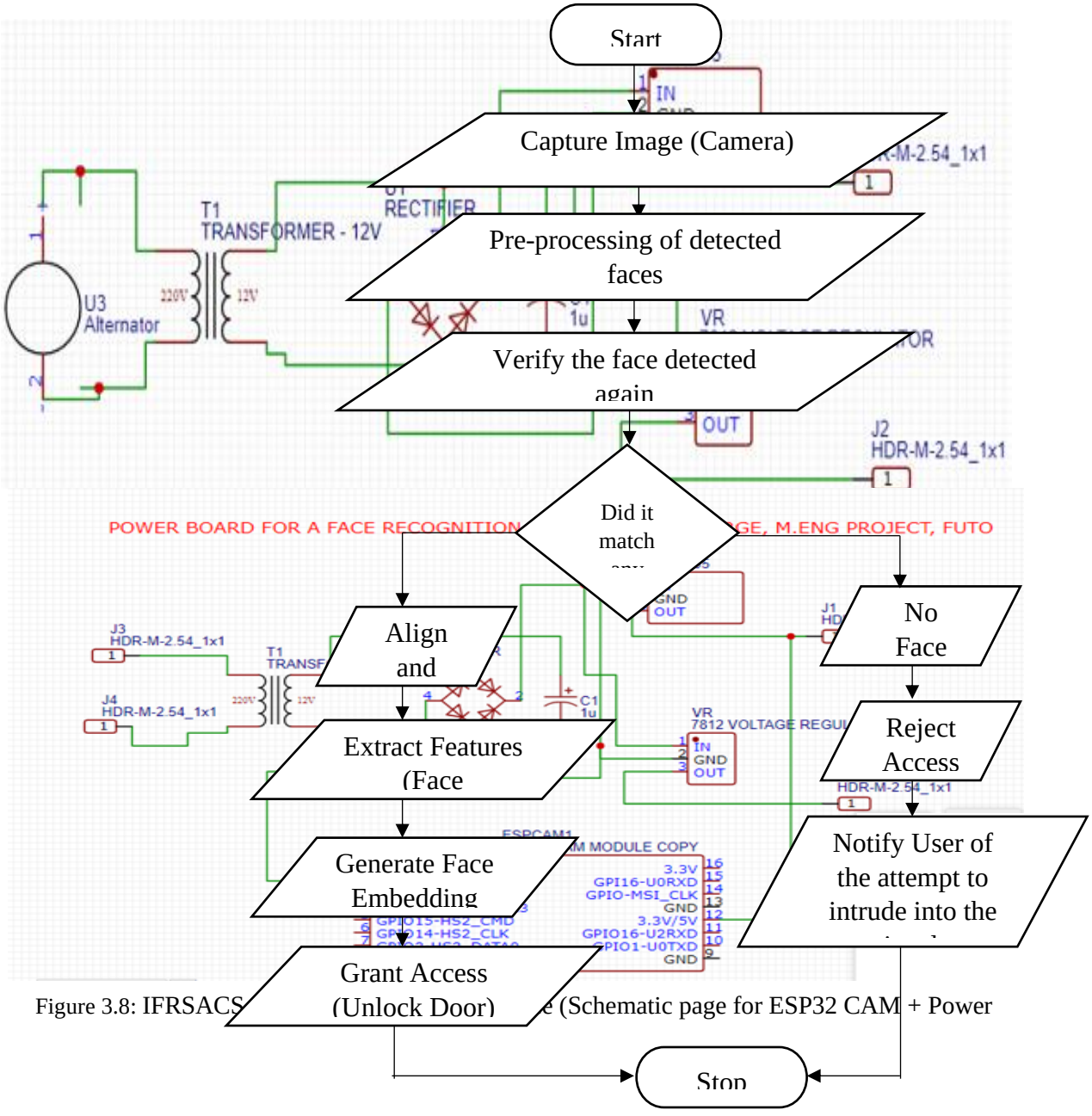

Figure 3.8: IFRSACS e (Schematic page for ESP32 CAM + Power

Figure 3.5: The flowchart of the real-time picture capture and notification

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

3.2.6 Biasing

Resistor value and Transistor calculations

BC547 has two operation statuses: forward bias and reverse bias. In the status of the forward bias, the current can pass when the collector and emitter are connected. While in the status of the reverse bias, it acts as a disconnect switch and current cannot pass. BC 547 common-emitter current gain and the associated calculations:

From the datasheet of the BC547 NPN transistor:

The following values were obtained;

(i) Emitter current = I_E = -100mA

(ii) Base current = I_B = 20mA

(iii) Collector current = I_C = 100mA

(iv) Base-Emitter Voltage = V_{BE} = 0.7v

Calculating the gain factor (β) of the NPN transistor used:

Recall:

$$\text{Gain factor } (\beta) = \frac{I_C}{I_B} \quad \textbf{(3.1)}$$

$$= \frac{100 \times 10^{-3}}{20 \times 10^{-3}} = 5$$

This implies that an input current to the emitter will have a gain factor of 5.

This is enough to switch the DC relay in the circuit.

Finding the relationship of collector current (output current) to emitter current (input current) known as α. It's calculated thus;

$$\alpha = \frac{\Delta I_C}{\Delta I_E} \text{ or } = \frac{\beta}{\beta + 1} \quad \textbf{(3.2)}$$

$$\text{Therefore } \alpha = \frac{\beta}{\beta+1} = \frac{5}{5+1} = \frac{5}{6} = 0.83$$

This implies that the input current at the emitter reached the collector at 83% output current to input current.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

To find the accurate value for the biasing resistor connected at the base of the transistor, Plate 3.9 was used in accordance with the associated equations.

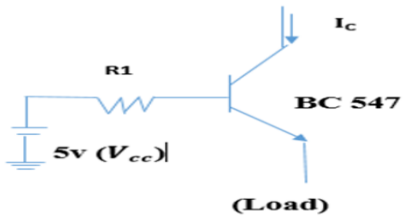

Plate 3.9: Relay Switching transistor (BC 547)

Recall Ohm's law;

$$V = IR \tag{3.3}$$

Base-emitter of BC 547 transistor = 0.7v (Datasheet). That is V_{BE} = 0.7v

$$\text{The voltage across R1 resistor} = \frac{V_{CC-V_{BE}}}{I_B} \tag{3.4}$$

$$= \frac{5v-0.7v}{20\,x \times 10^{-3}}$$

$$= \frac{4.3}{20 \times 10^{-3}}$$

$$= \frac{4.3}{2}\, x\, 10^2$$

$$= 2.15 \times 10^2$$

$$= 215\Omega.$$

The biasing resistor value is 215Ω, approximately 220Ω which is commonly available in the market.

1.3.3 System Circuit Diagram

The Circuit Diagram for the ESP32-CAM Faces Recognition Door Lock System is combined with an FTDI board, Relay Module, and Solenoid Lock. The FTDI board is employed to flash the code into ESP32-CAM because it doesn't have a USB connector while the relay module is employed to modify the Solenoid lock on or off. The door lock system using an ESP32 CAMERA includes several components that work together to provide security and access control. Here's a basic circuit diagram explanation for the system: the system circuit is shown in Plate 3.4.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

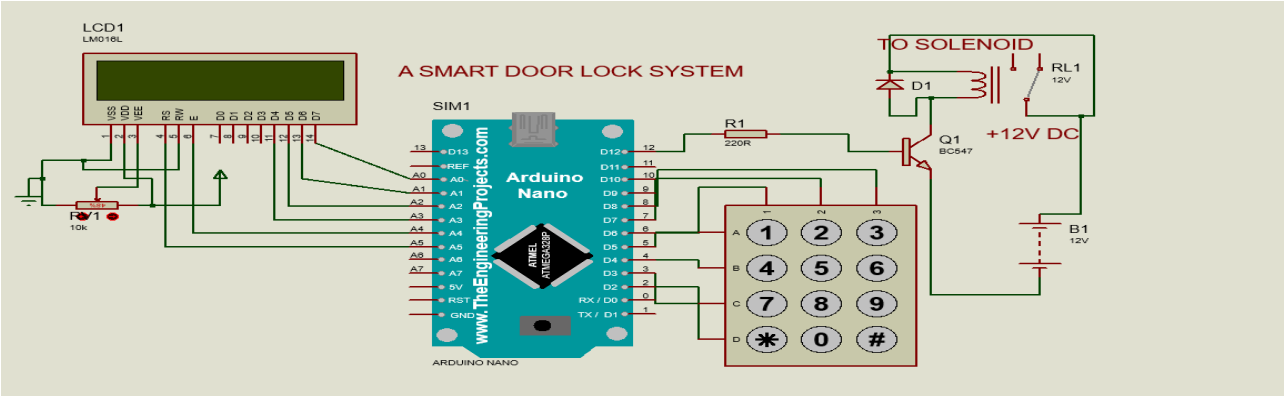

Plate 3.4: A Smart door lock system circuit diagram

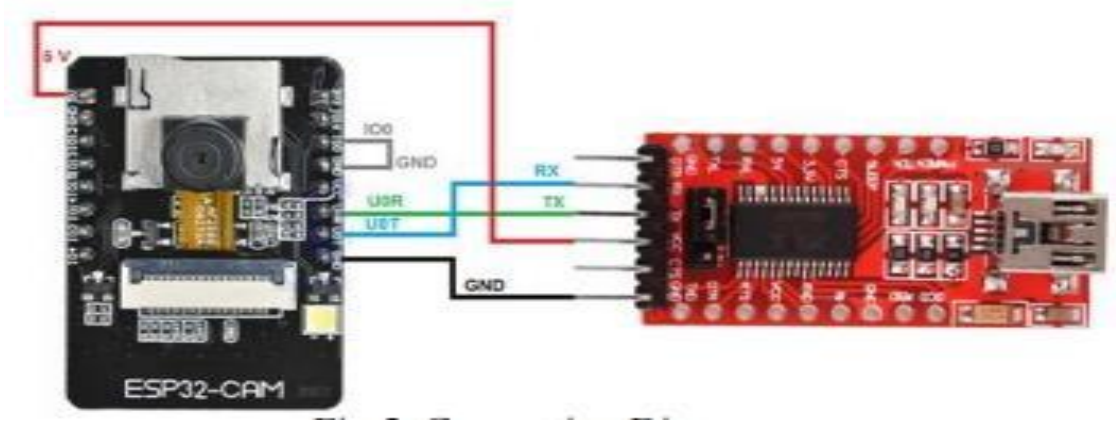

Plate 3.11: Esp32 Camera Module and the FTDI Programmer

The ESP32-CAM module was connected to a local network via a phone hotspot or router, allowing it to function as a station for real-time photo transmission through a web server. The module, similar to an Arduino, was easily programmed using Arduino software.

Plate 3.11 illustrates the programming circuit involving the ESP32-CAM and the FTDI Programmer. The FTDI cable, a USB-to-Serial TTL converter, enables simple USB connectivity. The ESP32-CAM's TX pin was connected to the FTDI RX pin, and vice versa. The VCC (5V) and GND of both modules were also linked to complete the connection.

After completing the Requirements Gathering, Analysis, and Design phases, the system was implemented. The software aspect involved translating the design into source code and integrating system components. The hardware implementation used an ESP32-CAM connected to the Cloud and paired with a mobile application for command transmission. Additionally, a solenoid lock was used for the mechanical aspect.

Plates 3.13 and 3.14 show the implementation and testing process, while Plate 3.12 displays 64 photos stored in EEPROM for face recognition. If a user's face matches any of the stored images, the system activates the relay, unlocking the solenoid lock to grant access.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

Plate 3.12: 64 photo signatures used on the system for the face recognition configuration

1.3.4 Results:

The implementation of a face recognition door lock system using the ESP32-CAM has proven to be accurate, efficient, and practical. Through testing, the system reliably identifies and authenticates individuals based on facial features captured by the ESP32-CAM. The combination of the ESP32's built-in Wi-Fi and Bluetooth with an image-processing camera module has enabled a compact and versatile access control solution.

Experimental results demonstrate high accuracy in recognizing authorized users while denying access to unauthorized individuals. The system performs well under various lighting and environmental conditions, ensuring real-world applicability. Authentication response times remain within acceptable limits, providing a smooth user experience. These findings confirm the effectiveness of using the ESP32-CAM for face recognition-based access control. Plate 4.1 displays the Serial Monitor page of the smart door lock and the Telegram dashboard.

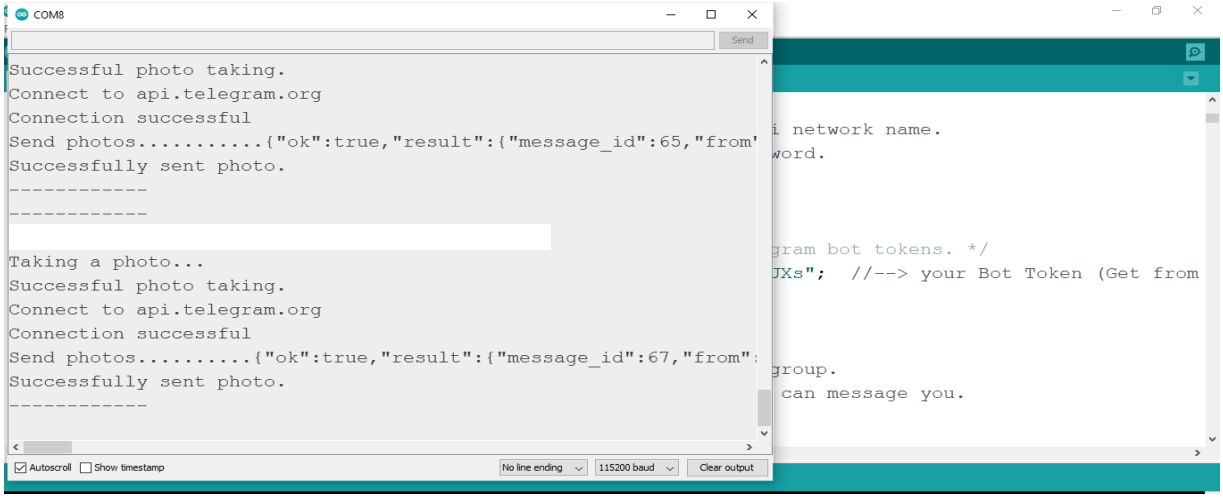

Plate 4.1: Serial monitor and Telegram page showing ESP32 camera taking picture intruders

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

Plate 4.2 shows the complete system in testing mode. It prompts the user to look at the camera eye and if successfully validated, it quickly prompts the user to enter the correct password.

Plate 4.2: A Smart door lock system showing power up state

Plate 4.3 shows the complete system in operation mode. The camera validates the user's face and then quickly prompts the user to enter the correct password. And when the correct password was entered, the system granted the user access. After five (5) seconds, the door locks again and expects the next user tom follow the aforementioned prompts to gain access. It is also shown in Plate 4.3 where the solenoid lock was switched on and access was granted.

Plate 4.3: The smart door lock in operation showing access granted

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

1.3.5 System WiFi Communication Range and Received Signal Strength Indicator (RSSI) values

The ESP32-CAM WiFi module measures the signal strength between the prototype (transmitter) and the user's smartphone (receiver) using the Received Signal Strength Indicator (RSSI). During system testing in an open space, the RSSI remained highly stable, with only minor fluctuations observed as the distance varied.

The recorded RSSI values are presented in Table 4.1, with a graphical representation shown in Plate 4.4. The average output power in milliwatts (mW) was calculated using Equation 4.1:

$$\text{Output power (Pout)} = 10\frac{\text{dBm}}{10} \quad (4.1)$$

where the average RSSI is the input parameter measured in dBm.

Table 4.1: Communication Range and RSSI values at distance >> 50 meters (1 unit division)

Distance (m)	Largest RSSI Value (dBm)	Smallest RSSI Value (dBm)	Average (Round off) RSSI Value (dBm)	Average Output Power (mW)
1	-54	-53	-53.5	0.0000029
2	-54	-53	-53.5	0.0000029
3	-54	-54	-54	0.0000040
4	-54	-52	-53	0.0000050
5	-54	-53	-53.5	0.0000029
6	-55	-54	-54.5	0.0000035
7	-56	-54	-55	0.0000032
8	-54	-53	-53.5	0.0000029
9	-54	-52	-53	0.0000050
10	-55	-54	-54.5	0.0000035
11	-54	-51	-52.5	0.0000056
12	-54	-53	-53.5	0.0000029
13	-53	-50	-51.5	0.0000071
14	-54	-51	-52.5	0.0000056
15	-55	-53	-54	0.0000040
16	-54	-52	-53	0.0000050
17	-57	-53	-55	0.0000032
18	-51	-50	-50.5	0.0000089
19	-51	-50	-50.5	0.0000089
20	-51	51	-51	0.0000079

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

1.3.6 Discussion Summary

The implementation of a face recognition door lock system using the ESP32-CAM, keypad, and solenoid lock presents key discussions on functionality, performance, and potential improvements. The average output power analysis from Table 4.1 indicates minimum and maximum power levels at RSSI values of -53.5 dBm and -50.5 dBm, respectively.

1.3.7 Output (Received) Power Measurement

In wireless networks, signal strength and quality are measured in dBm, with RSSI values closer to 0 dBm indicating stronger signals. Calculations showed that the average output power was higher at -50.5 dBm, meaning that as the user's smartphone moved closer to the receiver (prototype device), the output power increased. The maximum output power recorded was 0.0000089 mW, while the minimum was 0.0000029 mW, as detailed in Table 4.1. Plate 4.5 provides a graphical representation of RSSI variations at distances exceeding 50m. Some fluctuations were observed due to common network challenges.

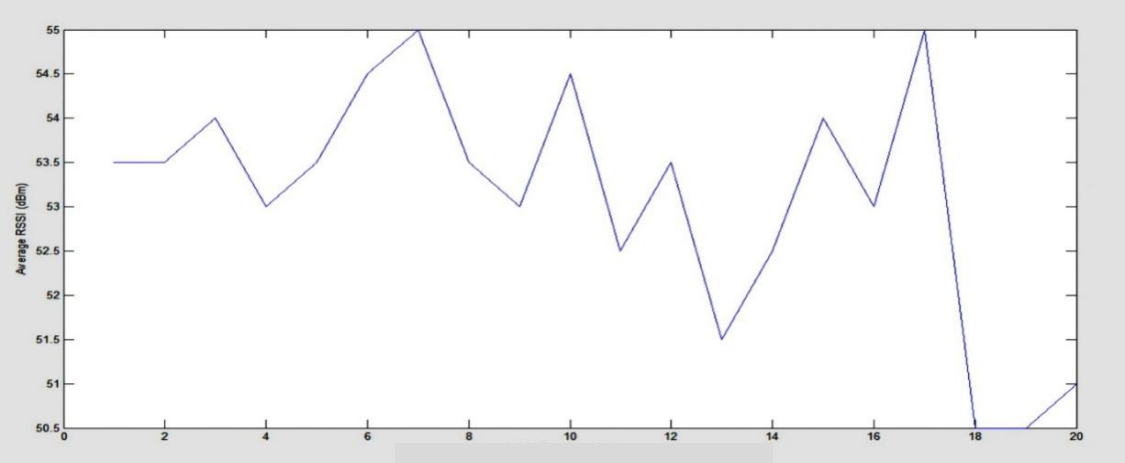

Plate 4.5: Graphical representation of RSSI values obtained as recorded in table 4.1

1.3.8 Conclusion

The face recognition door lock system has been successfully designed, implemented, and tested, providing a secure and convenient access control solution. By integrating machine learning and computer vision, the system ensures accurate and efficient authentication, making it suitable for various applications. Its adaptability to different environments enhances practicality for real-world use. This research advances face recognition-based access control, highlighting security, usability, and privacy considerations while paving the way for future improvements in access management.

1.3.9 Recommendations

To enhance the system's performance and reliability, developers should continue refining algorithms, upgrading hardware, and improving the user experience to ensure greater accuracy and efficiency. Security measures must be continuously updated through encryption protocols, software patches, and protections against spoofing or hacking. The system should be designed to accommodate diverse facial features, ensuring inclusivity and minimizing bias. Additionally, seamless integration with smart home and building automation systems will enhance functionality. Privacy considerations must also be prioritized, with clear guidelines for data protection and user consent to maintain compliance with regulations and build user trust.

ACKNOWLEDGEMENTS: The efforts of my two supervisors in the persons of **Engr. Dr. Cosmas Kemdirim Agubor** and **Engr. Dr. Longinus Sunday Ezema** are highly appreciated. I really tender my unalloyed gratitude for the fatherly assistance offered to me at one point or the other.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

REFERENCES

Aalase, A., Bandgar, P., Kamble, K., Bhosale, S., & Udgave, A. A. (2023). International Journal of Research Publication and Reviews Surveillance Monitoring Using ESP32-CAM Module. International Journal of Research Publication and Reviews, 4(3), 4297–4300. www.ijrpr.com

Adak, D., Pain, M. K., & Dey, U. K. (2017). Rfid Based Security System Using. International Journal of Scientific and Engineering Research, 8(3), 143–145.

Ahmed ElShafee, K. A. H. (2012). Design and Implementation of a WiFi Based Home Automation System", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 6, No: 8. 6(8), 1074–1080.

Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESp32. Procedia Computer Science, 157, 673–682. https://doi.org/10.1016/j.procs.2019.08.218

Andrew, A. M. (2019). Intelligent Control Systems: An Introduction with Examples. Kybernetes, 32(4), 1–29. https://doi.org/10.1108/k.2003.06732dae.003

Arsić, N., Jakšić, B., & Petrovic, M. (2016). Overview, Characteristics and Advantages of IP Camera Video Surveillance Systems Compared to Systems with other Kinds of Camera Creating the Network of Knowledge Labs for Sustainable and Resilient Environments-KLABS View project. Certified International Journal of Engineering Science and Innovative Technology (IJESIT, 9001(5), 356–362. https://www.researchgate.net/publication/355484230

Bhat, A., Sharma, S., Pranav, K. R., & G, M. R. H. (2017). HOME AUTOMATION USING INTERNET OF THINGS. 917–920.

Borkar, A. A., & Karande, R. R. (2017). Web Hosting and Live Streaming Using Raspberry-Pi for Home Automation. 3, 598–602.

Computing, M. (2015). GSM-Based Home Automation System Using App-Inventor For Android Mobile Phones. International Journal of Computer Science and Mobile Computing, 4(4), 158–167.

G. C. Manjunath, Mr. B. Mahendra, Ms. Rashmi, Mrs G. Bhuvana, & Ms Keerthi. (2022). Home Security System using ESP32-CAM and Telegram Application. International Journal of Advanced Research in Science, Communication and Technology, May, 580–582. https://doi.org/10.48175/ijarsct-5093

Gaikwad, P., Narule, S., Thakre, N., & Chandekar, P. (2017). RFID Technology-Based Attendance Management System. International Journal Of Engineering And Computer Science, 2–7. https://doi.org/10.18535/ijecs/v6i3.10

IEA Report, 2014. (2017). Voice Recognition Based Home Automation System for Paralyzed People. 3(02).

Kantha & Priyanka, P. (2020). Realization of an IoT System to Ensure Doorway Security by Integrating ESP32-CAM with Cloud Server. 1235–1238.

Kazi, R., & Tiwari, G. (2016). IoT based Interactive Industrial Home wireless system, Energy management system and embedded data acquisition system to display on web page using GPRS, SMS & E-mail alert. International Conference on Energy Systems and Applications, ICESA 2015, August, 290–295. https://doi.org/10.1109/ICESA.2015.7503358

Kumar, A., & Tiwari, N. (2015). Energy Efficient Smart Home Automation System. 3(1), 11–13.

Kumar, M., & Shimi, S. L. (2015). Voice Recognition Based Home Automation System for Paralyzed People. 4(10), 2508–2515.

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020

Kundu, D., Nandy, S., & Kumar, A. (2019). Development of an Attendance System for Students with SMS Notification to Parents. Ijarcce, 6(6), 49–54. https://doi.org/10.17148/iarjset.2019.6607

Mukhtar, A. (2021). Nigeria's Security Challenges and the Crisis of Development: Towards a New Framework for Analysis. International Journal of Developing Societies, 1(3), 107–116.

Online, I., Chasokela, D., Tshuma, L. S., Matshe, K., & Sibanda, M. (2022). Indiana Journal of Multidisciplinary Research Password Based Door Locking System. 1–5.

Postulka, M. B. and J. (2019). Open Access books Built by scientists , for scientists TOP 1 %. Intech, 32(July), 137–144.

Putra, W. S., & Setyawan, A. (2021). Room Security System Design using ESP32 CAM with Fuzzy Algorithm. Mobile and Forensics, 3(2), 66–74. https://doi.org/10.12928/mf.v3i2.5554

Ravi, K. S., Varun, G. H., Vamsi, T., & Pratyusha, P. (2019). RFID based security system. International Journal of Innovative Technology and Exploring Engineering, 2(5), 132–134.

Salikhov, R. B., Abdrakhmanov, V. K., & Safargalin, I. N. (2021). Internet of things (IoT) security alarms on ESP32-CAM. Journal of Physics: Conference Series, 2096(1). https://doi.org/10.1088/1742-6596/2096/1/012109

Sehgal, T., & More, S. (2017). Home Automation using IOT and Mobile App. International Research Journal of Engineering and Technology (IRJET), 694–698.

Shah, H., Chauhan, V., & Sharma, R. (2017). Home Automation Using ZigBee. 6(3), 99–102.

Singla, D. (2023). Performance Analysis of Authentication system : A Systematic Literature Review Performance Analysis of Authentication system : A. 0–26.

Snehal Arun Khulape; Sakshi Rajendra Malage; Manasi Sudhir Patil; Arfa Aslam Bargir; Sagar V. Chavan. (2018). Home Automation Android-Based GSM System. International Journal of Trend in Scientific Research and Development, 2(6), 774–777. url: http://www.ijtsrd.com/papers/ijtsrd18740.pdf%0ADirect Link: http://www.ijtsrd.com/engineering/computer-engineering/18740/home-automation-android-based-gsm-system/miss-snehal-arun-khulape

Snehal N. Bawane, P. Gautam, Ashish Dewase, V. Mishra, S. G. (2017). Automation of Irrigation System using Android Technology. International Journal Of Engineering Science And Computing, 7(3), 5580–5582.

Soe, Z. N., Win, D. A. M., & Thoung, D. T. H. (2018). Implementation of Fingerprint-based Student Attendance System with Notification by GSM Module. International Journal of Science and Engineering Applications, 7(9), 260–264. https://doi.org/10.7753/ijsea0709.1002

Viola, P., & Jones, M. (2022). Rapid object detection using a boosted cascade of simple features. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1(July). https://doi.org/10.1109/cvpr.2001.990517

http://dx.doi.org/10.31364/SCIRJ/v13.i04.2025.P04251020