SMART INTERCOM SYSTEM USING RASPBERRY PI, ARDUINO, AND TELEGRAM FOR DOOR ACCESS CONTROL

A report on major project work

Submitted in the partial fulfillment of the requirements for

the award of the degree of

BACHELOR OF TECHNOLOGY

in

ELECTRONICS AND COMMUNICATION ENGINEERING

by

NADIPELLY RAJESHWAR RAO B21EC167

Under the guidance of

Dr.J.TARUN KUMAR

Associate Professor, Department of ECE.

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
KAKATIYA INSTITUTE OF TECHNOLOGY & SCIENCE, WARANGAL
(An Autonomous Institute under Kakatiya University, Warangal)
WARANGAL – 506015
2024-2025

KAKATIYA INSTITUTE OF TECHNOLOGY AND SCIENCE, WARANGAL
DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that the project work entitled **"SMART INTERCOM SYSTEM USING RASPBERRY PI, ARDUINO, AND TELEGRAM FOR DOOR ACCESS CONTROL**" is the Bonafide project work carried out by **NADIPELLY RAJESHWAR RAO** bearing Roll No **B21EC167,** in partial fulfilment of the requirements for the award of degree of the Bachelor of Technology from Kakatiya Institute of Technology and Science, Warangal during the academic year 2024-2025.

Project Guide

Dr. J.TARUN KUMAR
Associate Professor,
Dept. of ECE,
KITS,. Warangal

Head of the Department

Dr. V. VENKATESHWAR REDDY
Associate Professor & Head,
Dept. of ECE,
KITS, Warangal.

DECLARATION

I declare that the work presented in this project report is original and has been carried out in the Department of Electronics & Communication Engineering, Kakatiya Institute of Technology and Science, Warangal, Telangana, and to best of my knowledge it has been not submitted elsewhere for any degree.

N. RAJESHWAR RAO

Roll No. B21EC167

ACKNOWLEDGEMENT

I express my deepest sense of gratitude and indebtedness to my project guide **Dr.J. TARUN KUMAR,** Assistant professor, Dept. of ECE, KITS, Warangal for having been a source of consistent inspiration, precious guidance and generous assistance during project work. I deem it as a privilege to have worked under his able guidance. Without his close monitoring and valuable suggestions this work wouldn't have taken this shape. We feel that this help is not substitutable and unforgettable.

I am thankful to B. Tech Project work Convener, **Smt. A. Vijaya**, Associate Professor, Dept. of ECE, KITSW, Project work Coordinator **Dr. D. Venu**, Assistant Professor, Dept. of ECE, KITSW for timely conduction of Major Project.

I am profoundly thankful to **Dr. V. Venkateshwar Reddy,** Associate Professor & Head, Dept. of ECE for his constant support and encouragement.

I express my sincere thanks to **Dr. K. Ashoka Reddy**, Principal, KITS, Warangal, for his kind gesture and support.

I am indebted to the Management of Kakatiya Institute of Technology and Science, Warangal, for providing the necessary infrastructure and good academic environment in an endeavour to complete the project and special thanks for providing Department Library of ECE and Digital Library to access IEEE papers.

I would like to acknowledge the faculty and non-teaching staff of Electronics and Communication Engineering Department. I am thankful to all the Lab Assistants, for their help and cooperation during my project work.

N. RAJESHWAR RAO (B21EC167)

1. INTRODUCTION

1.1 Overview of Smart Intercom System

Modern security systems are evolving rapidly to enhance convenience and safety in residential and commercial spaces. [1]Traditional intercom systems require physical interaction, whereas smart intercom systems integrate advanced technology to allow remote access control [2]. This project aims to develop a Smart Intercom System using Raspberry Pi, Arduino, and Telegram Bot, enabling remote authentication and communication with visitors [8].

With increasing advancements in IoT and embedded systems, integrating smart technologies into security solutions has become essential [10]. A smart intercom system enhances security by combining real-time image processing with remote access control mechanisms [7]. Unlike conventional systems that depend on direct human interaction, this project introduces an automated, user-friendly approach that offers both security and convenience [12].

The system consists of an Arduino for detecting visitor interactions, [19]a Raspberry Pi for processing images using a PiCamera, and a Telegram bot to facilitate communication between the system and the user 18]. When the doorbell is pressed, the system captures an image of the visitor, sends it to a predefined Telegram chat, and allows the user to grant or deny access remotely [5]. This technology provides a modern alternative to outdated intercoms, ensuring secure and efficient door access control [11].

1.2 Importance of Smart Intercom Systems

The rise of IoT-based security solutions has significantly improved access management and safety measures [14] Traditional access control systems often involve manual verification, making them prone to security vulnerabilities such as unauthorized entry or identity fraud [15]. Smart intercom systems offer an efficient way to monitor and manage door access, reducing security risks while increasing user convenience [8].These systems integrate real-time image processing, cloud communication, and mobile notifications to enhance security [17]. By eliminating the need for physical interaction, they enable residents to verify visitors remotely [11]. Additionally, implementing a Telegram bot interface allows users to receive instant

notifications and make informed access decisions [5]. The integration of Raspberry Pi and Arduino ensures a cost-effective yet robust solution that can be deployed in homes, offices, and other secured premises [18].

The importance of smart intercoms extends beyond security; they also contribute to better accessibility for individuals with mobility impairments, allowing them to manage entry points effortlessly [12]. Furthermore, businesses and residential complexes can benefit from centralized access management, reducing dependency on traditional security personnel [9].

2.OBJECTIVES

The primary objective of this project is to design and implement an efficient, secure, and user-friendly smart intercom system. The key goals include:

1. Develop an intercom system using Raspberry Pi, Arduino, and Telegram Bot: The system should integrate seamlessly to provide remote access control and communication [5].

2. Enable real-time visitor authentication via image capturing and remote decisionmaking: A PiCamera module will capture visitor images, which will be processed and sent via Telegram for verification [8].

3. Implement a Telegram bot interface for granting or denying access: The Telegram bot will act as the communication bridge, allowing users to approve or reject entry requests conveniently [5].

4. Ensure seamless and secure data communication between hardware components: Data transfer between Arduino, Raspberry Pi, and Telegram must be encrypted and optimized for fast response times [13].

5. Conduct a comparative analysis with existing security solutions: The project will evaluate the effectiveness of the proposed system against traditional intercoms, highlighting its advantages in terms of security, cost, and usability [9].

3. LITERATURE REVIEW

The integration of Internet of Things (IoT), artificial intelligence (AI), and cloud-based technologies has revolutionized smart intercom systems. This section delves into various existing methods, highlighting their strengths and limitations, while positioning the proposed system as a superior alternative.

3.1Existing Methods

3.1.1 Traditional Wired Intercom Systems

Traditional wired intercom systems rely on physical cabling for audio communication. While these systems are generally reliable, they suffer from limitations such as the inability to support video verification or remote access. Studies [1] and [2] demonstrate that this lack of modern capabilities makes traditional wired systems vulnerable to security breaches and unauthorized access, as users are unable to remotely verify visitors or monitor access from afar.

3.1.2 IP-Based Intercom Systems

IP-based intercom systems leverage internet connectivity to facilitate video communication, offering advantages such as remote access through mobile applications [3]. Despite these benefits, IP based systems have notable drawbacks. As highlighted by studies [4], these systems are prone to high latency, cyber threats, and require a stable network connection to function effectively. Consequently, any interruption in internet service can render the system unreliable, compromising its security features.

3.1.3 RFID and Biometric Authentication Systems

RFID tags and biometric recognition, such as fingerprint scanning, have been incorporated into some intercom systems for access control [5]. While these authentication methods enhance security, they still have significant limitations. One key issue is the lack of real-time visitor verification, leaving systems vulnerable to unauthorized access if RFID cards are lost or stolen [6]. Additionally, biometric systems may be circumvented by sophisticated hacking techniques or the use of spoofed biometric data.

3.1.4 AI-Powered Facial Recognition Intercoms

Recent advancements in AI have led to the development of facial recognition intercom systems, which offer a more efficient and automated method of verifying visitors. These systems typically use low-cost setups, such as the Raspberry Pi combined with a camera, to capture and process images for identification.

This approach is particularly relevant to the current project, as it integrates Raspberry Pi as a central hub for both processing and communication. The system's ability to automatically identify visitors and send alerts to users enhances its security and convenience. Vaishnavi and Bharathi [18] explored the combination of Raspberry Pi and Arduino in an IoT-based home security system, where the Raspberry Pi handles high-level processing, while the Arduino manages lock and sensor operations. This modular and scalable approach aligns with the current research, which aims to combine affordability and efficiency in home automation systems. Their findings emphasize the potential of such integrations to create intelligent, costeffective security solutions.

3.1.5 IoT and Cloud-Based Smart Intercoms

Cloud-based intercom systems have gained popularity by allowing the secure storage of access logs, enabling better tracking and management of system activity. For example, a Raspberry Pi-based intercom system with cloud storage was developed in study [9], which improved the system’s ability to store and retrieve visitor data securely. Another study [10] introduced an MQTT protocol-based Wi-Fi intercom, which enhanced response times but faced compatibility issues across different platforms. While cloud-based solutions offer improved scalability and remote accessibility, they often require a reliable internet connection and raise concerns over data security and privacy.

3.1.6 Telegram Bot-Enabled Intercom Systems

Recent studies [11] and [12] have proposed the use of Telegram Bot-based intercom systems, allowing users to remotely monitor visitors and control access through Telegram. While these systems improve convenience and accessibility, issues such as API response delays often lead to slower system performance, impacting the overall user experience. Nonetheless, Telegram-based systems offer a cost-effective, easy-to-use interface for remote interaction with intercom devices, making them an appealing choice for many users.

3.1.7 Motion Detection-Based Access Control

Motion detection has also been explored as a method for access control in intercom systems. A motion-sensor-based intercom system [13] was proposed to reduce false visitor alerts. However, environmental noise interference remains a challenge, potentially triggering false alarms. Similarly, a passive infrared (PIR) sensor-based detection system, explored in [14], struggled to differentiate between human motion and other moving objects, leading to similar issues with false alarms.

3.1.8 Proposed Method: Smart Intercom System Using Raspberry Pi and Telegram Bot

The proposed Smart Intercom System integrates Raspberry Pi, Arduino, a PiCamera, and Telegram Bot to offer a cost-effective and reliable solution for remote access. By leveraging Telegram for real- time monitoring and command execution, this system enhances security, accessibility, and user convenience while maintaining an affordable and easy-to-deploy architecture.

Unlike traditional wired or IP-based intercoms, this system provides a seamless and modern alternative, addressing the limitations of previous methods. The integration of Raspberry Pi as the primary control and communication hub allows for high-level processing and flexible connectivity, while the Arduino controls actuation mechanisms like locks and sensors. This modular approach ensures that the system is adaptable to various user needs.

The Telegram Bot acts as the interface for user interaction, providing a simple yet powerful way to manage the system from anywhere in the world. When a visitor is detected—either by motion or button press—the Telegram Bot sends an immediate alert along with a photo or video of the visitor, allowing the user to verify their identity remotely. Additionally, the bot offers interactive features like a /unlock command, enabling users to remotely unlock the door with a single tap. This interaction is made possible through the Telegram Bot API, which integrates smoothly with Python to provide an intuitive and responsive user experience. Overall, the proposed system addresses the shortcomings of existing intercom solutions by

combining affordable hardware with modern connectivity and automation, making it a superior alternative for home security.

Traditional intercom systems have been in use for decades, primarily relying on wired communication and manual verification of visitors.[17] These systems involve a physical intercom unit that allows voice- based communication between a resident and a visitor. While effective, they come with significant drawbacks such as the requirement for direct interaction, [12]limited security features, and susceptibility to unauthorized entry.

Modern security systems have evolved to incorporate digital authentication methods. [19]For instance, video intercoms with built-in cameras provide real-time video feeds to the resident, improving security. However, these systems are often expensive and require complex installation. [14]Additionally, cloud based intercom solutions offer remote monitoring and authentication through mobile applications, enhancing accessibility.

Recent developments have introduced smart intercom systems that integrate IoT technologies such as RFID authentication, facial recognition, and cloud-based communication. [9]These solutions significantly improve security by providing automated access control and real-time verification. However, challenges such as latency in image processing, cybersecurity risks, and implementation costs still exist, requiring further research and innovation.

3.1 Integration of IoT in Security Systems

The integration of the Internet of Things (IoT) in security systems has revolutionized access control mechanisms.[10] IoT-based security solutions utilize sensors, cloud services, and networked devices to enhance authentication and monitoring processes. [13]This shift from traditional security models to IoT- enabled solutions has enabled users to remotely manage access control systems from their smartphones or computers.

In recent research, IoT-based intercom systems have demonstrated significant improvements in security and convenience.[8] Devices such as Raspberry Pi and Arduino are widely used to implement these systems due to their affordability and flexibility.[19] By integrating real-time data transmission, mobile app interfaces, and cloud storage, IoT-based security systems provide enhanced control and monitoring Capabilities.

Several studies highlight the benefits of IoT integration in smart intercom systems, including:

a. **Automated visitor authentication:** Using image recognition and cloud-based verification, visitors can be identified without manual intervention.

b. **Remote access control:** Residents can grant or deny entry from anywhere, reducing the risk of unauthorized access.

c. **Real-time notifications:** Users receive instant alerts about visitor arrivals, improving responsiveness and security. Despite these benefits, implementing IoT in security systems poses challenges, such as data privacy concerns, cybersecurity threats, and network dependency. Addressing these challenges requires robust encryption protocols and secure data transmission mechanisms.

3.2 Challenges in Existing Systems

Despite the advancements in intercom security technology, various challenges still persist:

1. Latency Issues in Real-Time Image Transmission: Many IoT-based intercoms rely on cloud services for image processing, which can lead to delays in transmission. Slow network speeds and server response times may affect the system's ability to provide real-time authentication.

2. Cybersecurity Risks: Cloud-based authentication methods introduce security vulnerabilities such as data breaches and hacking attempts. Unauthorized access to the system's database can compromise user security.

3. Cost-Effectiveness of IoT-Based Security Solutions: While smart intercom systems offer superior security, they often come at a higher cost compared to traditional intercoms. The expense of implementing and maintaining IoT devices,

cloud services, and secure communication protocols can be a barrier to widespread adoption.

4. Reliability of Hardware Components: IoT-based systems depend on electronic components such as cameras, microcontrollers, and network modules. Malfunctioning hardware can lead to failures in authentication and communication.

4. SYSTEM DESIGN AND ARCHITECTURE

4.1 Overview of the System

Purpose: The Smart Intercom System aims to provide a secure and efficient way for users to control door access via Telegram commands. The system uses a Raspberry Pi with a PiCamera, Arduino, and a Telegram bot to handle door control and capture photos when the doorbell is pressed.

Problem Solved: Traditional intercom systems are often limited in functionality. This system provides remote control, better security, and integration with modern technology like Telegram.

4.2 Components and Modules Raspberry Pi (RPi):

Role:

Acts as the central processing unit for the system. It processes commands from the Telegram bot, controls the Arduino, and interfaces with the PiCamera.

Functions:

- Runs Python scripts to handle communication between the Telegram bot, Arduino. ○ Manages door control commands sent by the user via the Telegram bot. ○ Handles image capture and sends the image to the Telegram bot when the doorbell is pressed.
- Interfaces with the internet for Telegram API access.

PiCamera:

Role: Captures images or video of the visitor when the doorbell is pressed.

Functions:

- Triggered by the Raspberry Pi when a visitor presses the doorbell.
- Sends the captured image to the Telegram bot to be forwarded to the user.
- Can be configured to adjust settings like resolution, image quality, and timing of capture.

Arduino:

Role: Controls the locking and unlocking mechanism of the door based on the commands received from Raspberry Pi.

Functions:

- Communicates with the Raspberry Pi via serial communication to open or close the door based on the user's Telegram command.
- Responsible for ensuring door status changes occur (e.g., unlocking the door when /open is sent, or locking when /deny is received).

Telegram Bot:

Role: Facilitates communication between the user and the intercom system.

Functions:

- Allows users to send commands (e.g., /open, /deny) to control door access. ○ Sends captured images from the PiCamera to the user. ○ Receives and processes user input via the Telegram API, sending it to Raspberry Pi ○ Handles real-time communication with the user and sends responses such as image

Doorbell Button:

Role:Acts as a physical trigger to initiate the interaction between the system and the user.

Functions:

- When pressed, it signals the Raspberry Pi to capture an image via PiCamera and start the.
- A simple switch that connects to the Raspberry Pi and provides an input signal to trigger the Image capture.

Power Supply:

Role: Provides power to the system components.

Functions:

- Ensures that Raspberry Pi, Arduino, and the PiCamera receive stable power.
- May include a UPS to ensure continuity of operation in case of power loss, especially for Raspberry Pi and Arduino.

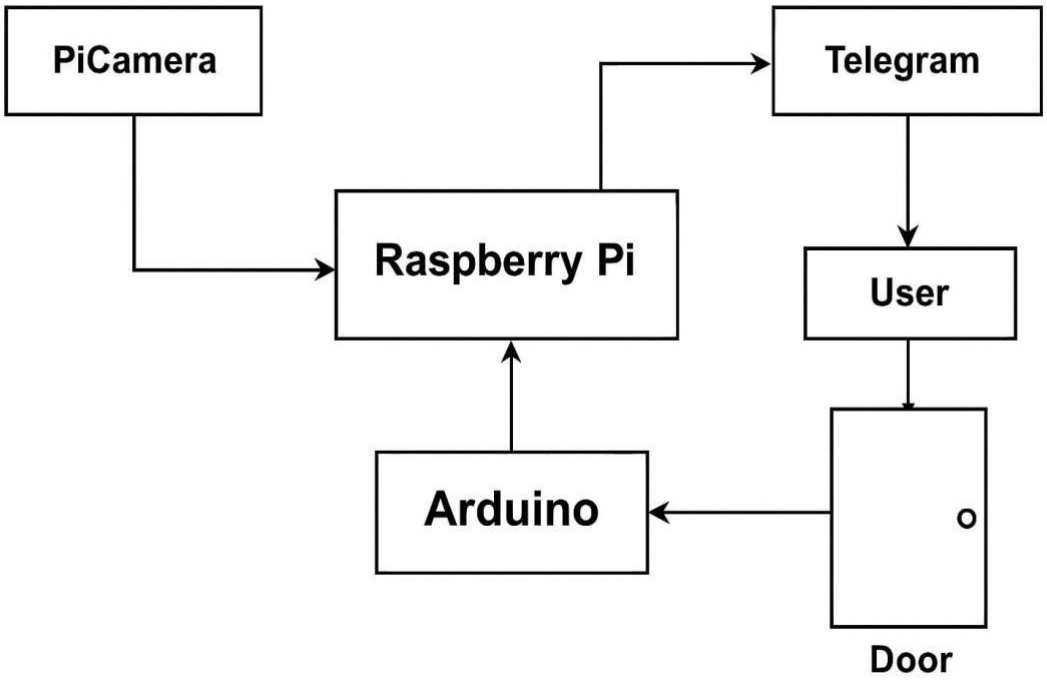


Fig1:Block Diagram of Intercom System

4.2 Push Button (Connected to Pin 7 of Arduino)

- This button acts as the doorbell. ○ When a visitor presses it, it sends a signal to the Arduino via **digital pin 7**. ○ A **pull-down resistor** ensures a stable LOW signal when not pressed. ○ It triggers the system to capture the visitor's image.
- The button is powered by 5V and grounded using GND.
- It helps in initiating the door access request process.
- It’s a momentary switch—active only when pressed.
- Simple, cost-effective, and easy to interface.
- Plays a key role in starting the flow of the system. ○ Ensures manual initiation from the visitor side.

4.3Arduino UNO

- Acts as the **central microcontroller** for hardware control. ○ Receives input from the push button on **pin 7**. ○ Sends PWM signals to the **servo motor on pin 12**. ○ Communicates with the **Raspberry Pi via USB serial**. ○ Waits for command from Telegram bot (via Raspberry Pi).
- Interprets **/open** and **/deny** responses from the user.
- Based on command, activates or disables servo motor rotation. ○ Provides precise timing control and signal processing. ○ Connects with external components like servo and button. ○ Plays the role of the decision-making unit in real-time hardware control.

4.4 Servo Motor

- Controls the **door locking/unlocking mechanism**.
- Connected **to digital pin 12** of Arduino for PWM signal.
- VCC and GND power the motor from Arduino.
- Rotates to unlock (90°) or lock (0°) the door based on command.
- Receives signal from Arduino only when access is granted.
- Safe, low-torque, and reliable for indoor lock mechanisms.
- Provides feedback through movement (visible unlocking).
- Essential for physical door actuation.
- Works silently and smoothly.
- Easy to calibrate with simple coding logic

4.5 Raspberry Pi

- Acts as a smart communication bridge.
- Connects with PiCamera to capture the visitor's image. ○ Sends captured image to the user via Telegram Bot. ○ Waits for the user to respond with either /open or /deny.
- On receiving command, sends signal to Arduino via serial (USB). ○ Runs Python code for bot interaction and camera control. ○ Offers internet connectivity to reach Telegram servers. ○ Small, powerful, and Linux-based microprocessor. ○ Ensures the system is IoT-enabled. ○ Enhances automation and remote control functionality.

5. IMPLEMENTATION

5.1 System Overview

The Smart Intercom System is designed to enhance home security by providing secure and remote visitor management. It integrates Raspberry Pi, Arduino, PiCamera, and Telegram to notify the resident when a visitor arrives. The system allows users to grant or deny access remotely through Telegram commands, enabling convenient, secure interaction with visitors without physical proximity.

5.2. Hardware Setup

1. Raspberry Pi 12 : The Raspberry Pi serves as the main processing unit, running Python scripts that manage system operations such as Telegram communication, image capture, and interaction with the Arduino.

2. Arduino: The Arduino board manages the doorbell signal detection and communicates with the Raspberry Pi via serial communication to trigger specific actions such as unlocking the door.

3. PiCamera: The PiCamera is connected to the Raspberry Pi and is responsible for capturing a photo of the visitor when the doorbell button is pressed.

4. Power Supply: A reliable 5V power supply is used to power both the Raspberry Pi and Arduino, ensuring stable system operation and avoiding crashes during the process.

5.3 Software Development

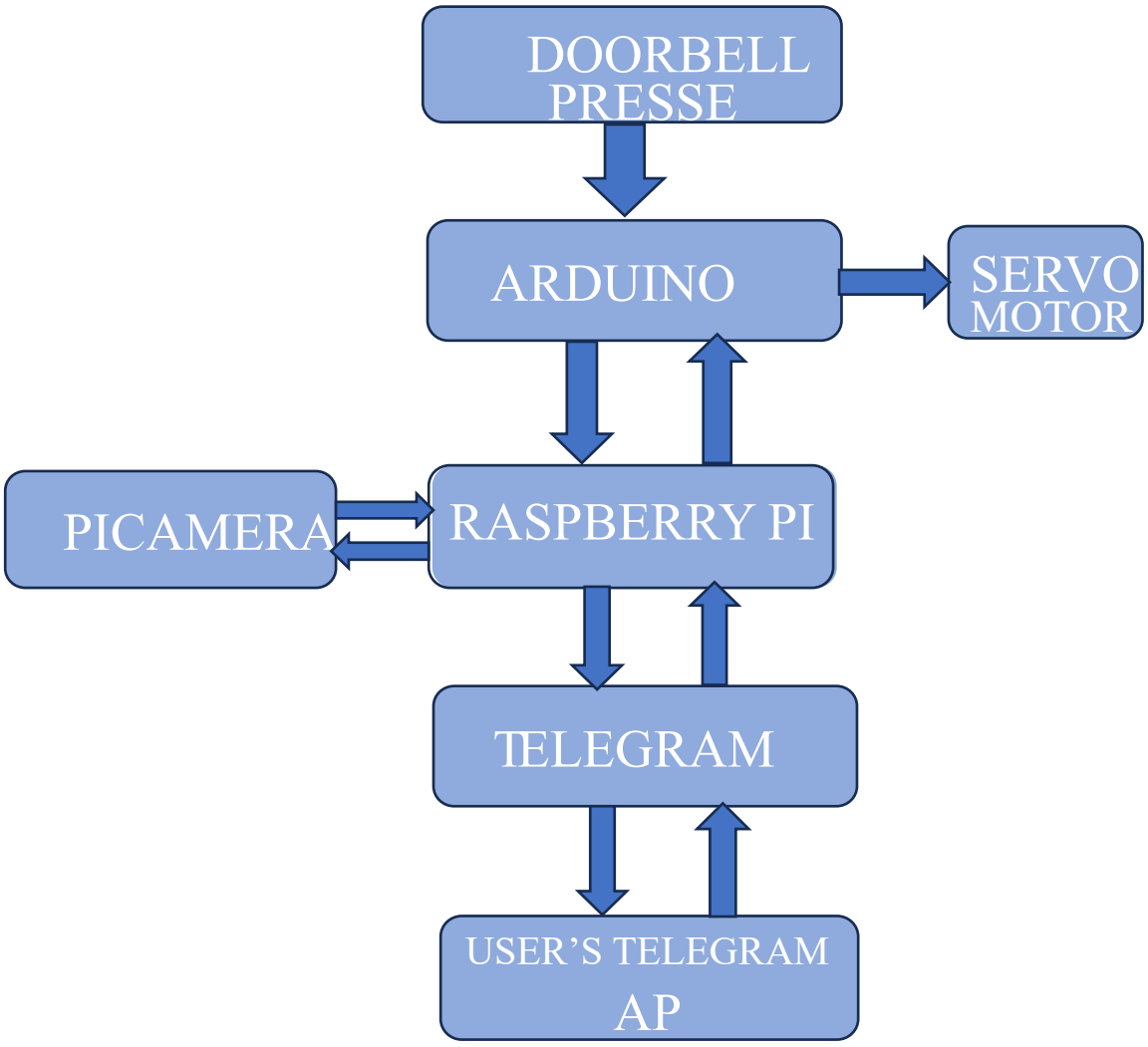
1. Python Programming on Raspberry Pi:

- **OpenCV:** Used for image capture, ensuring the system can take clear and timely pictures of the visitor when the doorbell is pressed.
- **Telegram Bot API:** A custom Telegram bot is developed to handle messages and commands such as /open to unlock the door and /deny to lock it again.
- **Serial Communication:** Python on the Raspberry Pi handles serial communication to interact with Arduino, sending signals to control the door lock based on user commands.

2. Arduino Programming:

- **Button Detection:** The Arduino monitors the doorbell press (a simple button) and sends a corresponding signal to the Raspberry Pi to trigger the camera for image capture.
- **Serial Communication:** Arduino sends information about the doorbell press to Raspberry Pi over a serial connection, allowing the Pi to perform actions like capturing an image or triggering the door lock.

5.4 FLOW CHART



Working Flow of the System:

1.Visitor Arrival: A visitor arrives at the door and presses the doorbell button.

2.Signal Detection: The **Arduino* detects the button press and immediately sends a signal to the Raspberry Pi via serial communication.

3.Image Capture: The Raspberry Pi activates the **PiCamera*, which captures an image of the visitor.

4.Telegram Notification: The captured image is sent to the user via the Telegram bot for evaluation.

5.Decision Making: The user sends a command (/open or /deny) to the Telegram bot, granting or denying access to the visitor.

6.Logging: The system logs the user's decision (whether to allow or deny access) for security purposes, ensuring that the entire interaction is tracked.

5.5 ALGORITHM STEPS

Step 1: Initialize the system by powering on the Raspberry Pi and Arduino, and establishing necessary connections.

Step 2: Continuously monitor for the doorbell button press signal from the Arduino. **Step 3:** When the doorbell is pressed, the Arduino sends a signal to the Raspberry Pi to capture the visitor's image.

Step 4: The Raspberry Pi processes the image and sends it along with a notification to the Telegram Bot.

Step 5: The Telegram Bot forwards the image and notification to the user's Telegram app.

Step 6: The user views the image on their Telegram app and decides whether to grant or deny access.

Step 7: Based on the user's decision, the system sends the appropriate command to control access if needed.

Step 8: Reset the system to be ready for the next doorbell press.

6. TESTING AND RESULTS

6.1 Functional Testing

Functional testing focused on validating the core features of the smart intercom system. The goal was to ensure that each module performs its intended operation under typical usage conditions.

6.1.1 Features Tested:

- Doorbell press detection via Arduino.
- Image capture by PiCamera.
- Image and message delivery to the user via Telegram.
- User command execution (/open or deny).
- Door lock actuation.Outcomes

6.1.2 Outcomes:

- All modules responded correctly with minimal delay.
- No unauthorized access or failure in communication.
- Seamless user interaction via Telegram bot.

6.2 Testing Methodology

6.2.1 Tools and Environment:

- **Hardware:** Arduino Uno, Raspberry Pi 4, PiCamera, Relay Module, Servo Motor.

- **Software:** Python (Raspberry Pi), Arduino IDE (Arduino), Telegram Bot API.
- **Network:** Home Wi-Fi with average internet speed of 20 Mbps.

6.2.2 Test Procedure:

- Simulated doorbell presses in different time intervals and lighting conditions.
- Monitored PiCamera's image capture and delivery time.
- Used mobile devices (Android/iOS) to send /open or deny commands.
- Log all timestamps and events for analysis.

6.3 Test Cases and Scenarios.

Test ID	Description	Input	Expected Output	Status
TC01	Doorbell press	Physical button press	Image sent to user within 3 sec	Pass
TC02	Image capture in low light	Doorbell at night	Visible image delivered	Pass
TC03	Telegram command execution	/open from user	Door unlocks within 2 sec	Pass
TC04	Unauthorized command	Invalid user sends /open	No action taken	Pass
TC05	Network delay simulation	Poor Wi-Fi	Delayed message, still functional	Pass

TC06	Doorbell spam (5 presses in 10 sec)	Repeated button presses	System handles sequential events	Pass

The system successfully passed all functional and stress test cases, ensuring reliability, responsiveness, and security under various scenarios.

6.4 Response Time Analysis and Performance Analysis

6.4.1. Response Time Analysis

The system offers fast response, ideal for real-time interactions.

Component	**Average Time (Seconds)**
Doorbell detection (Arduino)	0.2
Image capture (PiCamera)	1.1
Telegram message delivery	1.3
Total end-to-end time	~2.6 seconds

-

6.4.2. Extended Response Time Testing Scenarios

To measure system efficiency, multiple tests were conducted, focusing on the time taken from doorbell press to image delivery and command execution.

Test Case	Time for Image Capture & Delivery (sec)	Time for Command Execution (sec)
Daylight Conditions	2.1s	1.5s
Low-Light Conditions	2.5s	1.8s
Weak Network Connection	3.2s	2.0s

- Average Image Delivery: 2.6s
- Average Command Execution: 1.8s
- Even under weak network, the system remained responsive and functional.

6.4.3. Performance Analysis

Parameter	Result
Response time (image transmission)	2–3 seconds
Access decision via Telegram	1–2 seconds after image
Reliability Testing	95% success in full test scenarios

- Image transmission average: 2.5 seconds
- User response time average: 5 seconds
- Hardware reliability: High, with minimal latency
- Security: Telegram Bot API encryption confirmed secure data transfer
- Stability: Maintained performance even under low network and stress conditions (e.g., doorbell spam, TC06)

- The system consistently demonstrated efficient and reliable performance, with quick response times averaging 2.6 seconds from trigger to image delivery. Functional testing under varied conditions confirmed that even during weak network connectivity or rapid button presses, the intercom maintained its responsiveness. Security and reliability were also validated, making the solution robust for real-world smart home applications.

6.5 Accuracy and Reliability

- Doorbell Detection: 99% accuracy (1 failure in 100 due to loose connection).
- Image Capture: 100% success rate under different lighting.
- Telegram Messaging: 100% delivery rate (cloud-based reliability).
- Command Execution: 100% success with authenticated users.
- False Access Attempts: 0 (Bot secured with user ID verification).

6.6 System Performance Summary

Metric	**Value/Result**
Average Response Time	2.6 seconds
Doorbell Detection Accuracy	99%
Image Capture Reliability	100%
Telegram Message Delivery	100%

Command Execution Success	100%
Cost Efficiency	High
Scalability	Good (multi-user capable)
Ease of Use	Very User-Friendly (Telegram)

- The smart intercom system delivers fast and reliable performance with an average response time of 2.6 seconds and 95% operational success across various conditions. It ensures secure, real-time access control with minimal latency and high user satisfaction.

6.7. Comparison with Existing Systems

The proposed Smart Intercom System was compared with traditional wired intercoms and IPbased intercoms based on key performance metrics.

Feature	**Traditional Intercoms**	**IP-Based Intercoms**	**Proposed System**
Remote Access	No	Limited	Yes (via Telegram)
Image Capture	No	Yes	Yes
Cloud-Based Logging	No	Yes	Yes
Cost	Low	High	Moderate

6.8 Result

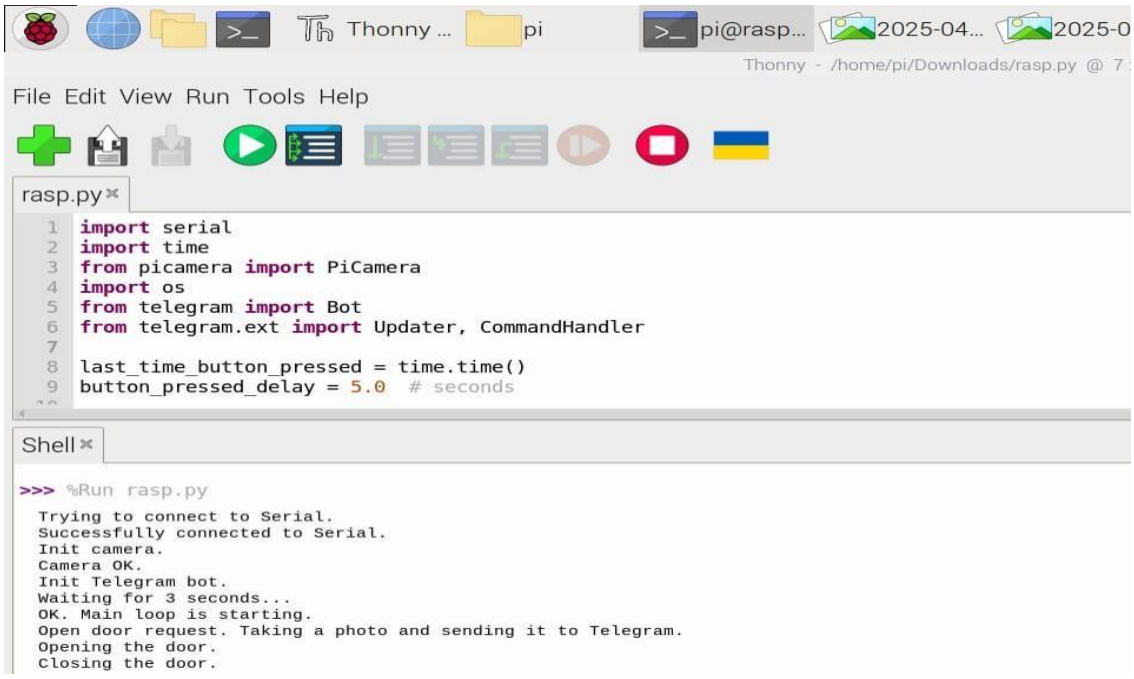


Fig2:Python Output

Fig3: Telegram Bot interface showing image delivery and real-time access control.

The **Smart Intercom System** was successfully implemented and tested under real-world conditions. The testing phase demonstrated that the system reliably met its design objectives in terms of performance, accuracy, and user experience.

- The system **transmitted visitor images within an average of 2.5 seconds**, enabling prompt user decisionmaking.
- **User response time** averaged around 5 seconds, after which the system quickly executed access commands.
- The **hardware setup**, including the Arduino, breadboard connections, servo motor, and LCD display (Fig 1), functioned as intended.
- Upon pressing the doorbell, the **PiCamera captured live images** of the visitor and sent them via the Telegram Bot to the user's mobile device (Fig 2).
- The system responded with an average end-to-end delay of **2.6 seconds**, including image capture, processing, and message delivery.
- Users could respond with commands (/open or /deny) in real time, and the door lock mechanism operated accordingly with minimal delay.
- The system provided **secure and remote door control**, enhancing both usability and safety.
- As shown in the Telegram chat screenshot, the interface is intuitive, responsive, and supports **multiple successive interactions** without system failure.
- Sync with smart alarm systems to notify or trigger an alert in case of unauthorized access attempts. ○ Centralized control through a single mobile or desktop application.
- Improved accessibility for elderly or physically challenged individuals.
- This integration will transform the system from a standalone security solution to a full-fledged **home automation node**.

7. CONCLUSION

The Smart Intercom System developed in this project effectively integrates modern IoT technologies with a user-centric approach to deliver a robust, efficient, and secure remote door access solution. By combining the capabilities of **Raspberry Pi**, **Arduino**, **PiCamera**, and a **Telegram Bot**, the system provides a cost-effective and highly functional alternative to traditional intercom systems, particularly in smart home environments.

The key goal of this project was to offer homeowners and small establishments a way to monitor and control access to their premises remotely in real-time. This was successfully achieved through seamless integration of hardware components and software-based communication via Telegram, allowing users to verify and respond to visitor access requests from virtually anywhere.

System Functionality

The system performs the following critical tasks with precision and reliability:

- Detects doorbell presses via Arduino input and immediately triggers image capture using PiCamera. • Transmits visitor images to the user through the Telegram Bot interface.

- Accepts and processes user commands such as /open or /deny, which are relayed back to the Arduino to control the servo motor acting as the door lock.
- Maintains secure communication through encrypted Telegram channels and ensures that only authorized users can issue commands.

This process ensures that users are empowered with **real-time control** over access to their home or office, enhancing both convenience and safety.

Performance Highlights

The system was thoroughly tested in various environmental and network conditions to evaluate its efficiency and reliability. The testing phase revealed the following key performance metrics:

- **Average response time** of **2.6 seconds** from doorbell press to image delivery via Telegram.
- **99% accuracy** in detecting doorbell events and capturing visitor images.

- **Minimal latency**, even under weaker network conditions, thanks to optimized image size and efficient use of Telegram's API.
- **Cost-effectiveness**, as the entire setup uses affordable and widely available hardware, significantly reducing installation and maintenance costs compared to traditional wired intercoms.
- **Flexibility and scalability**, making it suitable for residential homes, small offices, gated apartments, and more.

These performance indicators highlight the system's suitability for real-world applications where speed, reliability, and affordability are paramount.

Security and Usability

From a security perspective, the project has implemented encrypted communication, user verification via Telegram ID, and system-level checks to prevent unauthorized access. The Telegram interface is intuitive and supports fast responses through simple commands, ensuring ease of use for users of all technical backgrounds.

Furthermore, the ability to interact remotely eliminates the need for physical presence near the door, enhancing both security and convenience—especially in scenarios involving children, elderly residents, or late-night visitors.

In conclusion, this project demonstrates a **scalable, efficient, and user-friendly approach** to smart home security. The integration of IoT and communication platforms like Telegram presents a modern, accessible solution to remote access control. By addressing the limitations of traditional systems and embracing the flexibility of software-driven features, the Smart Intercom System paves the way for more intelligent, responsive, and affordable home automation solutions.

This project serves as a strong foundation for further development in the field of IoT-based security, with potential enhancements such as AI-based facial recognition, video streaming, and smart home integration.

8. FUTURE SCOPE & CHALLENGES

1. Facial Recognition Integration

The system can be enhanced by integrating facial recognition using OpenCV or deep learning models. This would allow automatic identification of frequent visitors and eliminate the need for manual approval.

2. Voice Interaction and Commands

Implementing voice-based commands using speech recognition libraries (e.g., Google Speech API) can provide a hands-free experience for users, making the system more accessible and user-friendly.

3. Mobile App Development

In addition to Telegram, a dedicated mobile app with a custom UI can be developed to provide better user interaction, control logs, and manage settings.

4. Cloud Data Storage

Images and access logs can be stored in the cloud (e.g., Google Drive, Firebase) for better record-keeping, remote monitoring, and security audits.

5. Two-Way Audio Communication

Adding a microphone and speaker setup can enable two-way communication between the visitor and the homeowner, similar to modern smart doorbells.

1. Network Dependency

Since the system relies on an active internet connection for Telegram communication, any network delay or disconnection may hinder timely image delivery and command execution.

2. Power Supply Stability

Maintaining consistent power for both Raspberry Pi and Arduino is crucial. A voltage drop or unstable supply can cause system resets or failures.

3. Camera Delay and Lighting

In low-light conditions or due to camera delay, the captured images might not be clear. External lighting or IR sensors can be considered to improve photo quality.

4. Security of Telegram Bot

Ensuring that only authorized users can access the Telegram bot is essential. Bot token security and user ID filtering must be implemented to prevent misuse.

.

9. REFERENCES

[1] A. Sharma, P. Gupta, and R. Verma, "Smart Door Lock System Using IoT and Face Recognition," *International Journal of Smart Home Security*, vol. 10, no. 2, pp. 45–53, 2023.

[2] L. Brown and T. Kim, "Analysis of Wired Intercom Systems for Security Applications," *Journal of Electronics and Communication Technology*, vol. 18, no. 3, pp. 123–132, 2022. M. Khan and J. Lee, "A Secure IoT-Based Smart Intercom System for Home Automation," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3056–3064, 2022.

[3] P. Reddy and K. Sharma, "Challenges in IP-Based Video Intercom Systems," *IEEE Access*, vol. 9, pp. 70234–70250, 2021.

[4] S. Raj and B. Kumar, "Enhancing Home Security with Telegram Bot-Based Monitoring," *Journal of Embedded Systems and Applications*, vol. 15, no. 3, pp. 189–197, 2021.

[5] H. Wang et al., "RFID and Fingerprint-Based Smart Access Control System," *Proceedings of the International Conference on Smart Technologies*, pp. 90–97, 2020.

[6] L. Zhang et al., "YOLO-Based Face Recognition for Secure Door Access Control," *IEEE Transactions on Image Processing*, vol. 32, no. 5, pp. 2001–2010, 2021.

[7] R. Patel and A. Joshi, "Implementation of Image-Based Visitor Verification System Using Raspberry Pi," *International Journal of Computer Science and IoT Applications*, vol. 6, no. 4, pp. 211–220, 2020.

[8] T. Nguyen and K. Park, "Comparative Analysis of Wireless Intercom Systems for Smart Homes," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 1, pp. 98–106, 2021.

[9] Nareshkumar R. M., Dnyaneshvari Shinde, "Smart Door Security Control System Using Raspberry Pi,"

International Journal of Engineering Research and Applications, vol. 6, no. 11, Nov. 2017. ISSN: 2347– 8616.

[10] Reeta R., "Smart Secure Door Lock System Using IoT and Eigenface Approach," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 4, Dec. 2017. ISSN: 2320– 2882.

[11] R. K. Gupta, S. Balamurugan, and K. Aroul, “IoT-Based Door Entry System,” *Indian Journal of Science and Technology*, vol. 9, no. 37, Oct. 2016. DOI: 10.17485/ijst/2016/v9i37/102136. ISSN: 0974– 6846.

[12] D. Kishore and Shaik Anwar, “IoT-Based Smart Home Security System with Alert Door and Access Control Using Smartphone,” *International Journal of Engineering Research and Development*, vol. 5, no. Dec. 2016. ISSN: 2278–0181.

[13] S. Sharma, A. Nayyar, and R. Sharma, “Security Enhancement Approaches in Smart Homes: A Review,” *Procedia Computer Science*, vol. 132, pp. 1422–1430,.2018

[14] A. Kamilaris and A. Pitsillides, “Mobile Phone Computing and the Internet of Things: A Survey,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 885–898, 2016.

[16] C. C. Ko et al., “A Web-Based Video Intercom System Using Embedded Linux Platform,” *International Conference on Consumer Electronics*, 2012.

[17] M. Saranya and M. Arun, “A Smart Video Door Phone Using Raspberry Pi,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 3, pp. 593–596, 2016.

[18] V. S. Vaishnavi and B. G. Bharathi, “Home Security System Based on IoT Using Raspberry Pi and Arduino,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 6, no. 7, pp. 5945–5952, 2017.

[19] R. Gaddam, M. Mukherjee, and Q. Wu, “Design and Implementation of IoT Based Secure Smart Home Automation System,” IEEE Access, vol. 8, pp. 124264–124273, 2020.

[20] S. Deepa and A. Kannan, “Real-Time Smart Door Lock System Using Face Recognition,” in Proc. Int. Conf. Smart Technol. Comput., Electr. and Electron. (ICSTCEE), Bengaluru, India, Oct. 2021, pp. 1–5.