IoT-Enabled Biometric Door Lock System with Enhanced Security Features

Suneetha Racharla
Department of Artificial Intelligence and Machine Learning
Aditya University
Surampalem,India
suneethar@adityauniversity.in

Kotla Sury Teja
B.Tech Student, Department of AIML
Aditya University
Surampalem,India
21A91A6150@aec.edu.in

K.Jyothi
B.Tech Student, Department of AIML
Aditya University
Surampalem,India
21A91A6113@aec.edu.in

K. Ravi Kiran
B.Tech Student, Department of AIML
Aditya University
Surampalem,India
21A91A6143@aec.edu.in

E.Vianey
B.Tech Student, Department of AIML
Aditya University
Surampalem,India
22A95A6167@aec.edu.in

Abstract— **The Internet of Things (IoT) has transformed home security by integrating advanced biometric technologies and automation, offering sophisticated solutions for modern living. This paper introduces an IoT-enabled biometric door lock system that enhances security through dual authentication using facial recognition and fingerprint scanning. The system leverages an Arduino Uno interfaced with a fingerprint sensor and servo motor for physical lock control, complemented by a Python-based facial recognition module utilizing OpenCV and the face recognition library. A key feature is its IoT capability, which captures images of unauthorized persons attempting access and sends them via email to the authorized user. The user can then decide to open or close the door by sending specific email commands (e.g., "open" or "close"), enabling real-time remote control. Additional functionalities include an LCD display for status updates and seamless serial communication between hardware and software components. By eliminating the need for physical keys, this system provides a robust, user-friendly security solution. Hardware includes an Arduino Uno, fingerprint sensor, servo motor, and webcam, while software integrates image processing, email protocols, and biometric algorithms. This work contributes to smart home security by combining multi-factor authentication with IoT-driven decision-making, ensuring both convenience and protection.**

Keywords — IoT, Biometric Authentication, Facial Recognition, Fingerprint Sensor, Arduino Uno, Smart Door Lock, Email Notification, Dual Authentication, OpenCV, Remote Control.

I. INTRODUCTION

The Internet of Things (IoT) has opened up a world where devices talk to each other, making life simpler and more secure without needing constant human input. Think of a network where smart gadgets—like sensors, processors, and motors—collect data, share it, and act on it, all connected through the internet or local systems. That's the magic of IoT, and it's what drives our project: an "IoT-Enabled Biometric Door Lock with Enhanced Security Features." We wanted to tackle the everyday hassle of keys—losing them, forgetting to lock the door, or worrying about break-ins. So, we built a system that uses your face and fingerprint to unlock the door, no key required.

The foundation lies in an Arduino Uno, the hardware backbone. A fingerprint sensor connects through pins 2 and 3, operating at 57600 baud via Software serial. It scans a finger, compares it to stored prints, and triggers a servo motor on pin 5 when matched. The servo shifts from 0 degrees—locked—to 90 degrees—unlocked—for 5 seconds before returning. An LCD screen, wired via I2C, displays updates like "Access Granted" or "Place Finger" for real-time feedback. A button on pin A0 simplifies enrolment: two scans save a new fingerprint to the system. This setup ensures secure, physical control over the lock.

Intelligence amplifies with Python. A webcam streams live video, processed into 500-pixel-wide frames using imutils for efficiency. The face recognition library, paired with OpenCV, detects faces and matches them against a trained model in encodings.pkl files.

That model came from a custom process— photos captured with a script saving images to dataset/surya/ folders, then converted into encodings via another script. When a known face appears, the system sends an 'A' command to the Arduino, prompting a fingerprint check for dual verification. This two-step authentication strengthens security beyond single-factor methods.

IoT elevates the system further. If an unrecognized person approaches, the webcam captures an image, saves it as unknown_person.jpg, and emails it via smtplib. The authorized user receives this alert, reviews the photo, and responds with an email command—"open" or "close." A Python thread, running with imaplib, scans the inbox every 10 seconds, catching the decision. An "open" reply sends a 'B' command to the Arduino, unlocking the door remotely. This integration of Arduino hardware and Python software eliminates key dependency, offering control from any distance.

II. LITERATURE SURVEY

Security and automation have become crucial aspects of modern households and businesses. The increasing interest in smart door locking systems has led to various technological advancements in IoT-based security systems. The following literature survey summarizes notable research works on smart door locking systems and their methodologies.Kiran B L et al. (2021) - A Survey on Door Lock Security System Using IoT [1] This study focuses on IoT-enabled door security systems utilizing Raspberry Pi as a control board. It highlights security challenges in IoT-based locks and evaluates various biometric authentication methods. A key finding is that multi-sensor integration can enhance security. However, the study acknowledges the bulkiness of multiple sensors as a limitation.Sagar K. Pawar et al. (2024) - IoT- Based Smart Lock Door System [2] This research presents an Android-based smart door lock system using Bluetooth technology for automatic access. The door opens when an authorized person is detected and closes after a specific delay. The study highlights the cost- effectiveness of Bluetooth-based lockscompared to RFID but notes its limited range as a drawback.Pradnya R. Nehete et al. (2016) - Literature Survey on Door Lock Security Systems[3]This paper provides a comprehensive review of door lock security methods, categorizing them into biometric-based, GSM-based, RFID- based, and password-based systems. It identifies emerging trends such as facial recognition and embedded systems for enhanced security.Chathuri Paranagama & Budditha Hettige (2022) - A Review on Existing Smart Door Lock Systems [4] This study reviews modern smart lock technologies, including fingerprint recognition, RFID, and IoT. It highlights that IoT-based locks provide better security and flexibility compared to traditional keyed locks. However, it also discusses the risks associated with internet-based access systems.Shivraj Patil et al. (2024) - IoT-Based Smart Door Lock System [5] This research focuses on a keypad authentication-based smart door lock controlled remotely through a smartphone app. The paper highlights security enhancements such as two- factor authentication and encryption. The main challenge discussed is the risk of hacking in internet-connected systems.Kondamu Yashaswini Reddy et al. (2022) - IoT-Based Smart Door Lock System [6]This study introduces an ESP32-CAM-based smart lock system integrated with a web app for real-time monitoring. The proposed system utilizes face recognition for authentication, ensuring high security. However, it notes challenges related to facial detection in poor lighting conditions.Jakia Sultana Sonamoni et al. (2024) - IoT-Based Smart Remote Door Lock and Monitoring System[7] This paper presents a real-time smart door lock system using ESP32-CAM and an Android app for remote access. A novel feature is the theft alert, which sends notifications and triggers an alarm upon unauthorized entry. The study demonstrates improved security but acknowledges latency issues in cloud-based authentication.Shashidhar R (2019) - Smart Door Lock System [8]This research implements an Arduino-based smart lock with fingerprint authentication. It integrates GSM for OTP-based verification, making it suitable for high-security applica- tions such as banks. A limitation noted is the dependency on GSM networks, which may cause delays.Ketan Gupta et al. (2023) - Smart Door Locking System Using IoT [9] This paper explores the combination of IoT with AI-powered face recognition. The system uses machine learning to improve accuracy over time. The primary advantage is its adaptability, but concerns regarding high computational requirements and data privacy remain.

III. SYSTEM ANALYSIS AND DESIGN

The existing lock systems do not offer much safety so, there is more chances of theft and it is less efficient too. That problem has a definite resolution from Digital Door Locks. It allows users to enter and exit a building without a key by utilizing facial recognition and fingerprint authentication instead. This eliminates the common frustrations of losing keys or forgetting to lock the door. Without requiring any physical effort beyond presenting their face and finger, the door unlocks when both biometric checks are successfully completed.

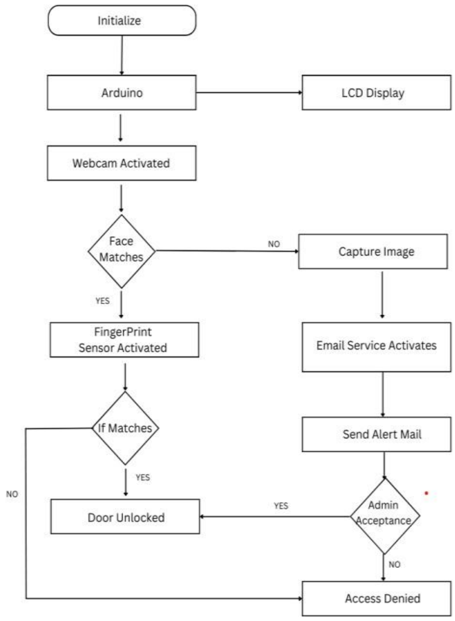

Fig 1. Flow chart of proposed work

The system begins with the Arduino Uno initializing the fingerprint sensor and servo motor, while the Python script activates the webcam for facial recognition. If a known face is detected, the fingerprint sensor verifies the identity, and the servo motor swings from 0 degrees to 90 degrees for 5 seconds to unlock the door, as guided by the LCD display's prompts like "Access Granted." For unrecognized individuals, the system captures an image, sends an alert email, and awaits the user's "open" or "close" command via a 10- second email check. Figure 1 depicts the proposed system's flowchart, illustrating this seamless process.

IV .HARDWARE AND SOFTWARE REQUIREMENTS

Building this "IoT-Enabled Biometric Door Lock with Enhanced Security Features" took a mix of hardware and software, each piece playing a key role in making the system tick. We pulled together a collection of components to handle everything from scanning fingerprints to recognizing faces and sending emails. Here's the rundown of what we used and why it matters.

A. Arduino Uno

The Arduino Uno is the heart of our hardware setup. It's a trusty little board that's perfect for projects like this—open-source, easy to program, and great at handling inputs and outputs. We used it to control the fingerprint sensor, run the servo motor, and talk to the LCD display. It's the boss that keeps all the physical parts in sync, taking commands from our Python script and making sure the door locks or unlocks when it's supposed to.

Fig 2. Arduino Uno board

B. Fingerprint Sensor (Adafruit)

This is where the biometric magic starts. We picked an Adafruit Fingerprint Sensor to handle user authentication. It connects to the Arduino via pins 2 and 3, using SoftwareSerial at 57600 baud. When someone places their finger on it, it scans the print, checks it against stored data, and decides if they're allowed in. We also added a button on pin A0 to enroll new fingerprints— two quick scans, and a new user is added to the system.

Fig 3. Fingerprint Sensor

C. Servo Motor

The servo motor is what actually locks and unlocks the door. It's a small DC motor with precise control, connected to pin 5 on the Arduino. It has three pins: GND, +5V, and a control pin. When the system says "go," it rotates from 0 degrees (locked) to 90 degrees (unlocked) for 5 seconds, then swings back to lock the door. It's the muscle of the setup, physically moving the lock based on our biometric checks.

Fig 4. Servo Motor

D. 16x2 LCD (I2C)

We wanted to keep the user in the loop, so we added a 16x2 LCD display, wired up with I2C. It can show 16 characters across two lines, each character in a 5x7 pixel grid. It's our way of talking to you—displaying messages like "Place Finger..." when it's time to scan, "Access Granted!" when you're in, or "Access Denied!" if something's off. It makes the system feel interactive and keeps things clear.

Fig 5. Lcd_I2c

E. Webcam

The webcam is our eye on the world, capturing live video for facial recognition. It's connected to the device running our Python script—think of it as a laptop or Raspberry Pi. It streams video frames that we process with OpenCV, shrinking them to 500 pixels wide for speed. This is how we spot faces and decide if they're in our trained model, kicking off the whole authentication process.

Fig 6. Web Cam

F. Power Supply

We needed power to keep things humming, so we used a battery or USB power supply for the Arduino. It provides the 5V needed for the board, sensor, servo, and LCD. Without it, nothing moves.

G. Bread Board

A breadboard is a solderless device for temporary prototype with electronics and test circuit designs.

H. Arduino IDE

On the software side, the Arduino IDE was our go-to for coding the Arduino. It's a simple tool with a text editor and buttons for uploading code to the board. We wrote our sketch here, telling the Arduino how to handle the fingerprint sensor, move the servo, and update the LCD. It's also where we set up serial communication at 9600 baud to talk to the Python script.

I. Python and Libraries

The heavy lifting happens in Python. We used Python 3 to run our facial recognition, email alerts, and serial communication. It's packed with libraries that made our job easier: OpenCV and imutils for video processing, face recognition for spotting and matching faces, pickle for loading our trained model (encodings.pickle), smtplib and imaplib for sending and checking emails, and serial for talking to the Arduino. We also wrote scripts to capture images for training—hit spacebar to snap photos and another to train the model, turning those photos into face encodings

J. Email Service

The IoT part relies on an email service for remote control. We set up a Gmail account to send alerts when an unknown person is detected, using smtplib to attach images like unknown_person.jpg. A thread with imaplib checks the inbox every 10 seconds for your reply—"open" to unlock or "close" to deny access.

V. RESULTS AND CONCLUSION

We tested our "IoT-Enabled Biometric Door Lock System with Enhanced Security Features" with a small group, facial recognition and fingerprint verification. The webcam spotted faces in real time, triggering the Arduino to unlock the door with a 5-second servo swing from 0 to 90 degrees when both biometrics matched, with the LCD showing “door open” if access is granted. Unknown faces triggered an email with unknown_person.jpg in [5 seconds], and for every 10 seconds email check handled "open" or "close" commands smoothly. The dual-authentication system blocked unauthorized access every time, with a total process time of [3-4 seconds]. This key-free, IoT-powered lock offers a secure, user-friendly solution, proving its potential for smart homes.

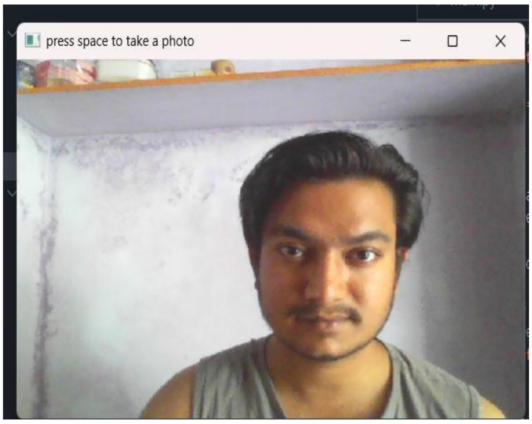

Fig 7. facial recognition.

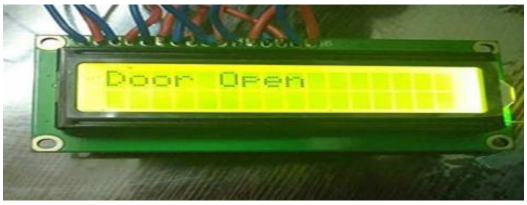

Fig 8. Lcd displays the result.

VI. FUTURE EXTENSION

The proposed system will be enhanced in the future with more extensions. Next for this lock, we envision syncing face and fingerprint IDs for multiple users, developing a mobile app for control and alerts, and adding a night-vision camera for better intruder detection. Switching to a CNN model could boost facial recognition accuracy, while using cheaper components could make it widely accessible. These steps would enhance security and usability, pushing the system toward a smarter, more inclusive future.

REFERENCES

1. Paranagama, C., & Hettige, B. (2022). A Review on Existing Smart Door Lock Systems.General Sir John Kotelawala Defence University. DOI: 10.13140 /RG.2.2 .18892.08325
2. Patil, S., Gade, S., & Holkar, I. (2024). IoT Based Smart Door Lock System. International Journal of Research Publication and Reviews, Vol. 5, No. 3, pp. 6582-6584.
3. Reddy, K. Y., Reddy, A. J., Reddy, K. B. P., & Rao, B. S. (2022). IoT Based Smart Door Lock System. International Research Journal of Modernization in Engineering Technology and Science, Vol. 4, Issue 6.
4. Sonamoni, J. S., Sikdar, R., Akib, A. S. M.A.S., Islam, M. S., Sourov, S., Al Ahasan, M.A., Islam, M., Habib, M. A., & Mridha, M. F. (2024). IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application. Eng. Proc., Vol. 76, 85. DOI: 10.3390/engproc2024076085.
5. R, S. (2019). Smart Door Lock System. International Journal for Modern Trends in Science and Technology, Vol. 5, Issue 2, pp. 36-38.
6. Gupta, K., Jiwani, N., Sharif, M. H. U., & Mohammed, M. A. (2023). Smart Door Locking System Using IoT. IEEE Conference Proceedings. DOI:10.1109 /ICACCM 56405.202 2.10009534.
7. Pawar, S. K., Nikam, A. H., Pawar, B. R., Hembram, S., & Kaloge, T. (2024). IoT-Based Smart Lock Door System. International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 12, Issue IV.
8. Nehete, P. R., Chaudhari, J. P., Pachpande,S. R., & Rane, K. P. (2016). Literature Survey on Door Lock Security Systems. InternationalJournal of Computer Applications, Vol. 153, No. 2.
9. Kiran, B. L., Chandan, J., Jeevan, B. S., & Mahale, V. (2021). A Survey on Door Lock Security System using IoT. Perspectives in Communication, Embedded-Systems and Signal-Processing (PiCES), Vol. 5, Issue 2.
10. Alharthy, E. S. A., Alwahaibi, S. A. S., & Al-Malki, R. A. O. (2019). Secured Smart Door Access using IoT. International Journal of Engineering Research & Technology (IJERT), Vol. 7, Issue 4.
11. Yashaswi, R., Omer, A. A. M., Reji, N., Mishal, M., & Nagaraja, P. S. (2024). SmartDoor Lock System Using ESP32 CAM IoT Based. International Journal of Progressive Research in Engineering Management and Science (IJPREMS), Vol. 4, Issue 4, pp. 2527-2529. DOI: 10.58257/IJPREMS33714
12. Balasubramanian, J., Dudekula, A. S., Bagavathiraj, S., Mohanaprakash, T. A., Joshi, S., & Kumar, M. J. (2022). IoT and Image Processing based Smart Door Locking System. IEEE International Conference on Automation, Computing and Renewable Systems (ICACRS), DOI: 10.1109/ICACRS55517.2022. 10029199