

# A Raspberry Pi-Based Surveillance System (RASGUARDIAN)

Dr. RakshithK<sup>1</sup>, NirooparadhyaSR<sup>2</sup>, RuchithaKV<sup>3</sup>, VijayKumarKM<sup>4</sup>, BhavaniKS<sup>5</sup>

<sup>1</sup>Assistant professor, Dept of ECE

<sup>2, 3, 4, 5</sup>Dept of ECE

<sup>1, 2, 3, 4, 5</sup> Maharaja Institute of Technology Thandavapura, Mysore, Karnataka, India

**Abstract-** *These days, security is a problem in every way. So let's use modern technology to fix these problems. The project utilizes the Face Recognition Module to take pictures of people and compare them with database photographs that have been stored. The door will be unlocked by a solenoid lock if it corresponds with the authorized user. The demand is always growing for a facial recognition system that is quick, precise, and able to prevent unauthorized users from entering highly secured locations, identify intruders, and reduce human error.*

**Keywords-** Raspberry pi, Web camera, Solenoid lock, pi adaptor, Relay module.

## I. INTRODUCTION

Robust security solutions are more important than ever in the quickly changing technology landscape of today. Keys and access cards, two common forms of traditional access control, are becoming more and more susceptible to loss, copying, and misuse. Using biometric authentication, novel ways have gained traction in response to these issues, offering improved convenience and security. One of the most innovative of these is the Face Locked Door System, which uses face recognition technology to regulate access to areas that are secured. The Face Locked Door System is an example of how access control has changed from depending on tangible tokens to using biometric authentication. This technology authenticates users and only allows authorized workers access by taking pictures and analyzing their face features.

By doing away with the requirement for users to carry around actual keys or access cards, this procedure improves user experience and expedites the authentication process. Sophisticated hardware and software components work together to provide safe access at the heart of the Face Locked Door System. The hardware consists of high-resolution cameras that can take close-up pictures of people's faces, and the software uses sophisticated algorithms to examine face traits and compare them to a database that has already been registered. The quick and precise identification made possible by this smooth hardware and software integration practically eliminates unwanted access.

## II. CONTEXTUALISED WORK

**A. Structure of the System:** Numerous works suggest taking a face picture with a camera and then comparing it to a database of authorised individuals using facial recognition software. If a match is found, this opens the door.

**B.Partitioning of Hardware:** because it's inexpensive and simple to use, Raspberry Pi is a well-liked option.

**C.Algorithms for Face Recognition in :** Talk about diverse face detection and matching facial recognition methods, such as Principal Component Analysis (PCA) and Eigenfaces. In order to increase accuracy, more recent works probably investigate deep learning approaches.

**d. security things to know:** Certain security concerns are acknowledged in some works, such as liveness detection (confirming that the subject is real and not an image) and face data preservation.

**E. Door Lock System Based on Face Recognition (this one utilises Raspberry Pi):** Smart Door Lock System Using Facial Recognition Technology (This one talks about Eigenfaces and PCA)

Security considerations are mentioned in the door locking system using face recipient.

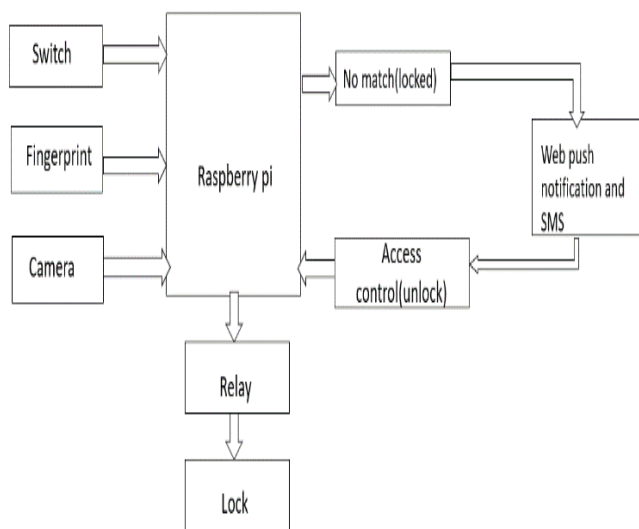
## III. ANALYSIS OF PROBLEM

Physical areas that are traditionally secured with traditional locks and keys are more vulnerable to security lapses. In order to tackle this problem, the project intends to create a Face-Locked Door System that strengthens the security of residential or business spaces and improves access management by utilizing facial recognition technology.

## IV. RECOMMENDED METHODS

There are several important steps in the face-locked door system's technique. To identify security requirements and user access levels, a thorough requirement collection process is the first step. Subsequently, extensive investigation and

evaluation are carried out to investigate appropriate facial recognition technologies, hardware elements, and software structures. The next step is to design the system architecture, including the parts, interfaces, and workflows. Hardware selection and configuration entail making the right device choices and setting them up in accordance with the system architecture. Software development comprises building a safe database to store biometric data and developing algorithms for door control, user authentication, and facial recognition. Accuracy, dependability, and security of the system are guaranteed under a variety of scenarios through integration and testing. For optimal use, configuration settings and user training are provided in addition to deployment at the designated location. The approach is then completed by continuing training, documentation, monitoring, and maintenance, which guarantee the system's continued optimization and operation. The successful deployment of a reliable and effective face-locked door system is ensured by this methodical approach.



**Fig1:Blockdiagram**

## V. DESIGN OF HARDWARE

A face-locked door system's hardware design includes carefully choosing and setting up each component to guarantee dependable operation and software integration. An outline of the hardware design factors is provided below:

**1. Camera:** Select a high-resolution camera that can take crisp pictures of people's faces. Take into account elements like field of view, performance in low light, and software compatibility for facial recognition.

**2. Raspberry Pi:** Decide on a Raspberry Pi to serve as the system's core processing unit. Make sure it has enough

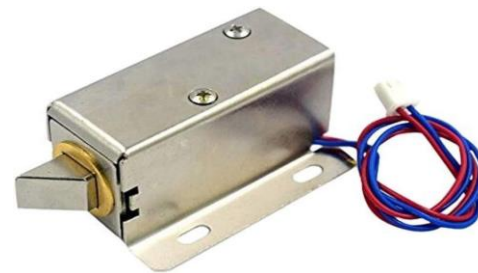
memory, processing power, and input/output interfaces to handle facial recognition software, interface with hardware accessories, and operate the door lock.



**Fig 2: Raspberry Pi**

## 3. LOCKING DEVICE:

Choose the locking mechanism type that best suits the security needs and door compatibility of your space. Electromagnetic locks, motorised deadbolts, and electric strikes are available options. A good microcontroller integration and electronic control of the locking mechanism are important considerations.



**Fig 3: Solenoid lock**

**4.Relay:** To connect the microcontroller and the locking mechanism, use a relay. Select a relay that can manage the locking mechanism's load by having the right voltage and current ratings. Achieve adequate isolation to prevent voltage spikes from harming the microcontroller.

**5.Power source:** To ensure that all of the system's components receive steady power, choose a dependable power source. Think about things like the amount of voltage needed, the current that can be used, and backup power alternatives in case of power interruptions.

**6. Enclosure:** Select an appropriate enclosure to keep the hardware parts safe from the elements, including moisture,

dust, and tampering. Make sure the enclosure has enough ventilation and access points for maintenance and wiring.

**7.Switches and Sensors:** Take into account incorporating switches or sensors to allow for manual override or to determine whether someone is in close proximity to the door. Motion sensors, push-button switches, and door position sensors are a few examples of this.

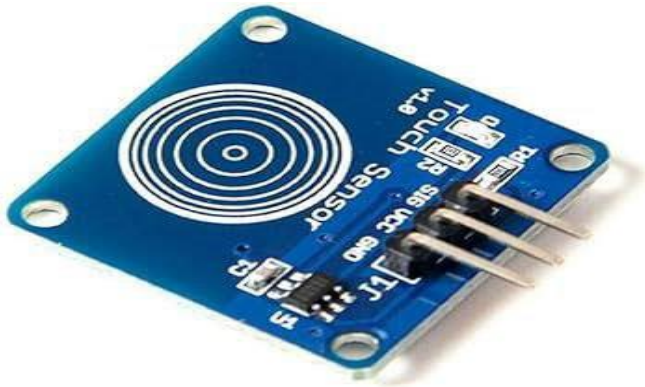


Fig 4: Vibration Sensor

**8.Wiring and Connections:** To guarantee correct operation and ease of maintenance, plan and lay the wiring connections between the components.

## VI. SOFTWARE ARCHITECTURE

A face-locked door system's software design entails arranging and structuring the software's component parts in order to Here is an outline of the software design considerations for effectively controlling access based on facial recognition:

**1. Modular Architecture:** To facilitate scalability, flexibility, and maintainability, design the software with a modular architecture. It should be divided into separate modules or layers that are responsible for tasks like facial detection, recognition, database management, access control, and user interface.

**2. Facial Recognition Algorithm:** Use a reliable algorithm for facial recognition to identify people based on their facial features. You should choose or develop an algorithm that is accurate, efficient, and able to handle variations in lighting, pose, and facial expressions.

**3. Database administration:** Construct a database administration system to house and handle authorized users' biometric information, such as their facial scans and the corresponding access rights. Ascertain the database's scalability, security, and speed of update and retrieval.

**4.User Interface:** Create a user interface with controls for system configuration, user administration, and access tracking that are easy to understand. A feature like access logs, system health indicators, and real-time feedback on access attempts should be considered.

**5. Integration with Hardware:** Adjust the programme to work with the system's hardware, including the camera, microcontroller, relay, and locking mechanism. To facilitate smooth connection between the hardware and software components, develop drivers and communication protocols.

**6. Error Handling and Logging:** Put strong error handling procedures in place to deal with exceptions, mistakes, and unforeseen circumstances politely. For troubleshooting and auditing purposes, log pertinent data, including warnings, system problems, and access attempts.

**7. Security measures:** Use security measures to prevent unauthorized access or tampering with sensitive data, such as biometric data and access logs. To guarantee data integrity and confidentiality, put access controls, authentication methods, and encryption into place.

**8. Validation and Testing:** To ensure the software's security, dependability, and functionality, thoroughly test and validate it. To find and address any flaws or vulnerabilities, run system, integration, and unit tests.

## VII. RESULT

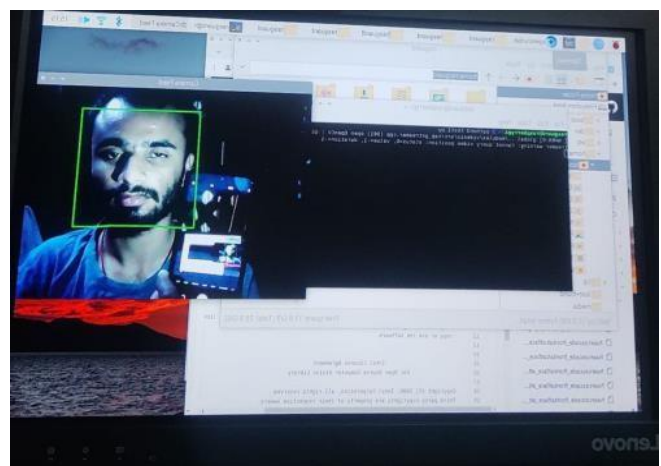


Fig4:Image identification

## VIII. CONCLUSIONS

A face-locked door system uses facial recognition technology to restrict entry to secured areas in a simple and safe manner. The technology effectively recognises authorised users and allows them admittance while blocking unauthorised

users by taking pictures of and evaluating their faces. This method removes the need for tangible tokens like keys or access cards and improves security by lowering the possibility of unwanted access. Face-locked door systems can also be scaled to meet changes in the number of users or access points, and they provide real-time monitoring and auditing capabilities. Because they offer contactless access and may be integrated with current security infrastructure, they are appropriate for a range of applications where convenience, hygiene, and security are critical considerations. Installing a face-locked door system is, all things considered, a major improvement in access control.

C. Kolluru, A. G. V, S. P. S, K. R. D, and A. S. Kumar, 2023, 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10307437.

## REFERENCES

- [1] [1] M. B. H., J. S., K. D. M, L. C. Govindapillai, and J. C. J. R., "Face Recognition Door Lock System Using Raspberry Pi," 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 1645-1648, doi: 10.1109/ICACCS54159.2022.9785217.
- [2] "Pose and Illumination Invariant Face Recognition for Automation of Door Lock System," Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1105-1108, doi: 10.1109/ICICCT.2018.8473103, A. Purushothaman and S. Palaniswamy A.
- [3] "Face Recognition Door Lock System Using Raspberry Pi," The Third International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2023, pp. 218-221, doi: 10.1109/ICSCCC58608.2023.10176434, T.G. Reddy, S. C. Sai, B. P. Kumar, R. T. Venkatesh, K. Sathwik, and K. Singh.
- [4] David A. Wangean, S. Setyawan, F. I. Maulana, G. Pangestu, and C. Huda, "Development of Real-Time Face Recognition for Smart Door Lock Security System using Haar Cascade and OpenCV LBPH Face Recognizer," 2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE), Jakarta, Indonesia, 2023, pp. 506-510, doi: 10.1109/ICCoSITE57641.2023.10127753.
- [5] M.A. Azhari Halim, M. F. I. Othman, A. Z. Z. Abidin, E. Hamid, N. Harum, and W. M. Shah, "Face Recognition-based Door Locking System with Two-Factor Authentication Using OpenCV," Sixth International Conference on Informatics and Computing (ICIC), Jakarta, Indonesia, 2021, pp. 1–7, doi: 10.1109/ICIC54025.2021.9632928.
- [6] "Development of Face Recognition-Based Smart Door Lock System with Remote Servo Control Authentication,"