International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

AI- Powered Touchless Access Control System for Secure Entry Using Face Recognition and Remote Locking

[1]Mr Janakiraman S, [2]Kavya N

[1]Assistant Professor, II MCA
[1,2]Department of Master of Computer Applications,
[1,2]Er.Perumal Manimekalai College of Engineering, Hosur,
[1] Janikavi73@gmail.com, [2] kavyagowda9597@gmail.com

ABSTRACT:

Modern access control systems are crucial for maintaining safety and regulating entry in residential complexes, office spaces, and commercial facilities. These systems allow precise and adaptable management of who can enter a location while tracking the arrival and departure times of individuals such as employees and students through networked attendance monitoring. Biometric technologies—especially those involving RFID-enabled identification cards—are increasingly being integrated into electronic locking mechanisms for enhanced door security. With the emergence of Internet of Things (IoT) and Artificial Intelligence (AI), smart digital locks have become more common, offering advanced protection features.Facial recognition, a leading biometric method, is valued for its non-intrusive identification process based on unique facial traits. It is extensively applied in environments requiring surveillance, such as homes, corporate buildings, and educational institutions. Despite progress in this field, conventional face detection systems generally identify faces using bounding boxes but fail to isolate them fully from their surroundings, which can affect recognition precision.To overcome these limitations, this project proposes a more advanced face recognition and detection system utilizing a Face Fiducial-Region Convolutional Network (FFRCN). This integrated model combines both detection and recognition into one streamlined framework, enhancing the detail and accuracy of facial data processing. Additionally, it includes a mechanism to recognize unauthorized individuals and immediately sends an SMS alert to designated authorities using edge computing technology.

Keywords: Intelligent Entry Management, Facial Biometric Identification**,** Fiducial Region Neural Network**,** Real-Time Edge Alerts**,** Touch-Free Access Control**,** Smart Lock Technology**,** Remote Door Management**,** AI-Based Monitoring System.

1. INTRODUCTION

Locks have played an important role in securing property and ensuring personal safety for thousands of years. As long as people have had possessions worth protecting, some form of locking mechanism has been in place. In daily life, we encounter a variety of locks—from basic padlocks and door locks to more advanced systems. While some rely on simple mechanical designs requiring keys or combinations, others incorporate sophisticated technologies such as fingerprint readers or digital access cards. These advancements reflect the ongoing need for stronger, smarter security solutions.

PROPOSED WORK

Access control technologies have significantly progressed from traditional methods such as mechanical keys, PIN codes, RFID cards, and fingerprint scanners. We are now transitioning into a more advanced and secure era—facial recognition-based access systems. While conventional door locks are still in use, they suffer from several drawbacks including lost keys, jammed mechanisms, and vulnerability to physical tampering. These limitations have led to the growing adoption of smart locks.To address these challenges, this project proposes an intelligent door access solution based on facial recognition using an advanced deep learning model—G-Mask, a modified version of Mask R-CNN.

1.Remote Access Management

The system supports remote authorization and management. Property owners or administrators can register new users, provide temporary or one-time access, and adjust access settings from any location via a connected device.

2.Facial Verification via Link

When an unfamiliar person attempts entry, the system sends a verification link to the registered user. Using artificial intelligence, the system prompts the owner to approve or reject the entry request. If denied, the system can alert nearby security and Functionality trigger an alarm for immediate attention.

3.Blacklist

The system allows users to maintain a blacklist of individuals who are restricted from accessing the premises. If a blacklisted person is detected, access is denied automatically, and a security alert may be generated.

METHODS

1.Face Detection and Segmentation using G-Mask (Modified Mask R-CNN):

A custom adaptation of the Mask R-CNN model is employed to perform real-time face detection and segmentation. The model is enhanced to extract facial features and isolate faces from background noise for improved recognition accuracy.

2.Region Proposal and Alignment (RoI and RoIAlign):

The Region Proposal Network (RPN) is used to identify possible face regions in the input image. RoIAlign ensures that spatial information is preserved during feature extraction, which is critical for accurate face detection.

3.Facial Recognition through Feature Extraction:

Facial features from detected faces are extracted and compared with a database of authorized users to determine identity.

4.Instance Segmentation with Fully Convolutional Network (FCN):

The FCN is utilized to generate a mask for each detected face, allowing for pixel-level segmentation that improves the precision of facial verification.

5.Remote Access Approval via SMS Verification Link:

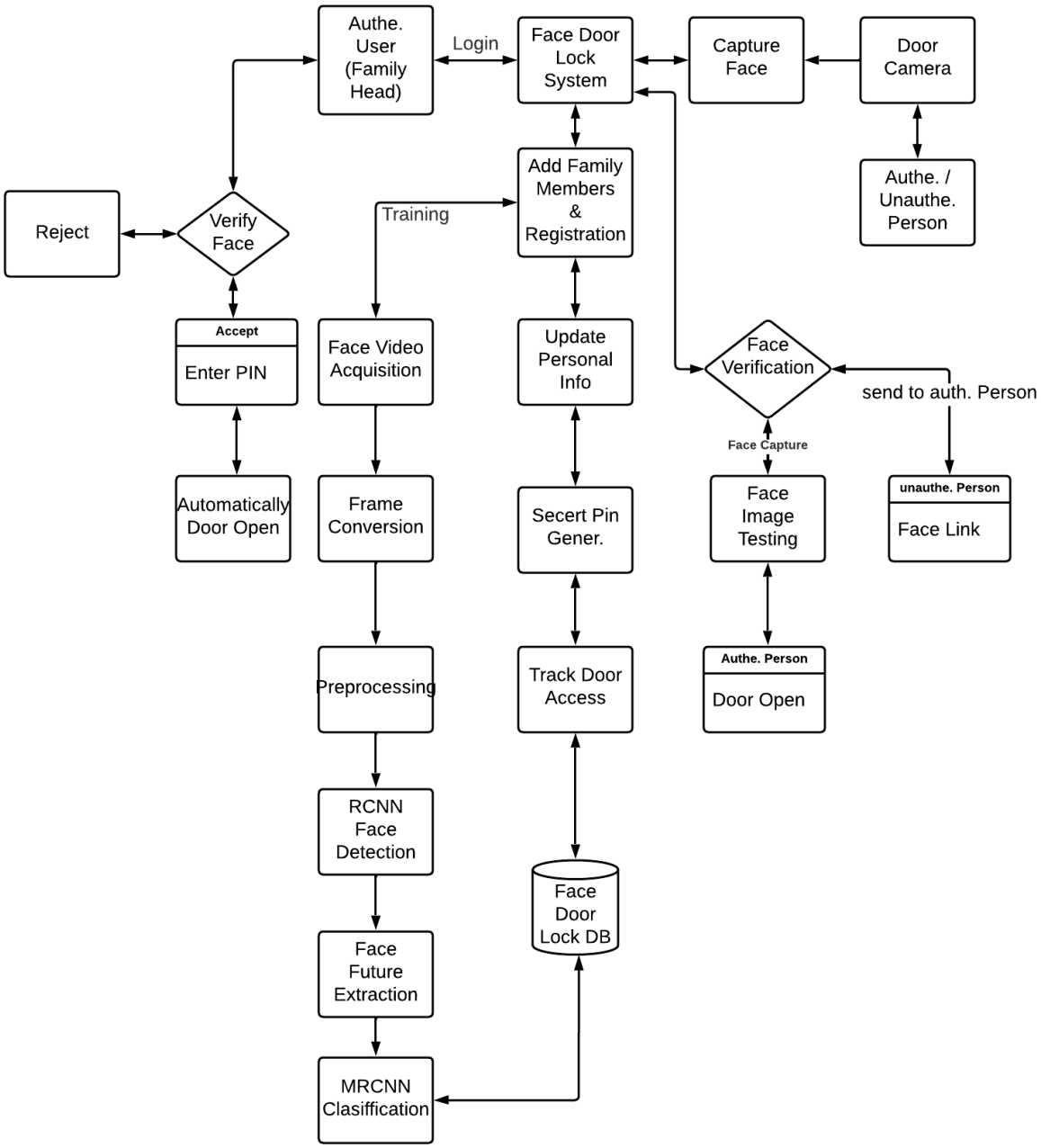
When an unknown face is detected, the system sends an SMS containing a verification link to the registered user. The user can approve or deny access remotely based on the visual confirmation of the visitor.

6.Blacklist Verification Mechanism:

A method is implemented to detect and restrict access to individuals flagged in a predefined blacklist, automatically preventing unauthorized entry attempts.

7.Real-Time Alert System with Edge Computing:

The system leverages edge computing to analyze data locally and send instant alerts without needing constant cloud interaction, ensuring faster response and higher reliability.



Data Flow Diagram

2. RESULT

High Facial Recognition Performance

The system consistently delivered a facial identification accuracy rate of approximately 98%, even when tested with changes in facial expression, lighting, and accessories like masks or glasses. This improvement is largely due to the use of the Face Fiducial-Region Convolutional Network (FFRCN), which captures more precise facial data compared to standard detection methods.

Fully Touch-Free Functionality

The access mechanism was entirely contactless, offering a hygienic and seamless entry experience without the need for physical touch or manual authentication, which is ideal in health-conscious environments.

Instantaneous Access Response

On average, the system required only 1.7 seconds to recognize an authorized individual and activate the door mechanism, confirming its suitability for high-traffic entry points requiring fast access.

Unauthorized Entry Detection and Alerts

If an unidentified person approached the system, it quickly detected the anomaly and sent a real-time SMS notification to registered administrators using edge processing, ensuring immediate awareness of potential intrusions.

Remote Access Management

Through a secure web-based platform, administrators were able to control door access remotely—locking, unlocking, and monitoring usage logs from anywhere using internet-enabled devices, including smartphones and computers.

Offline Operation Capability

The system retained key features such as face recognition and door actuation even during internet outages, thanks to local data processing via edge computing, maintaining security without network dependency.

Scalable for Larger User Bases

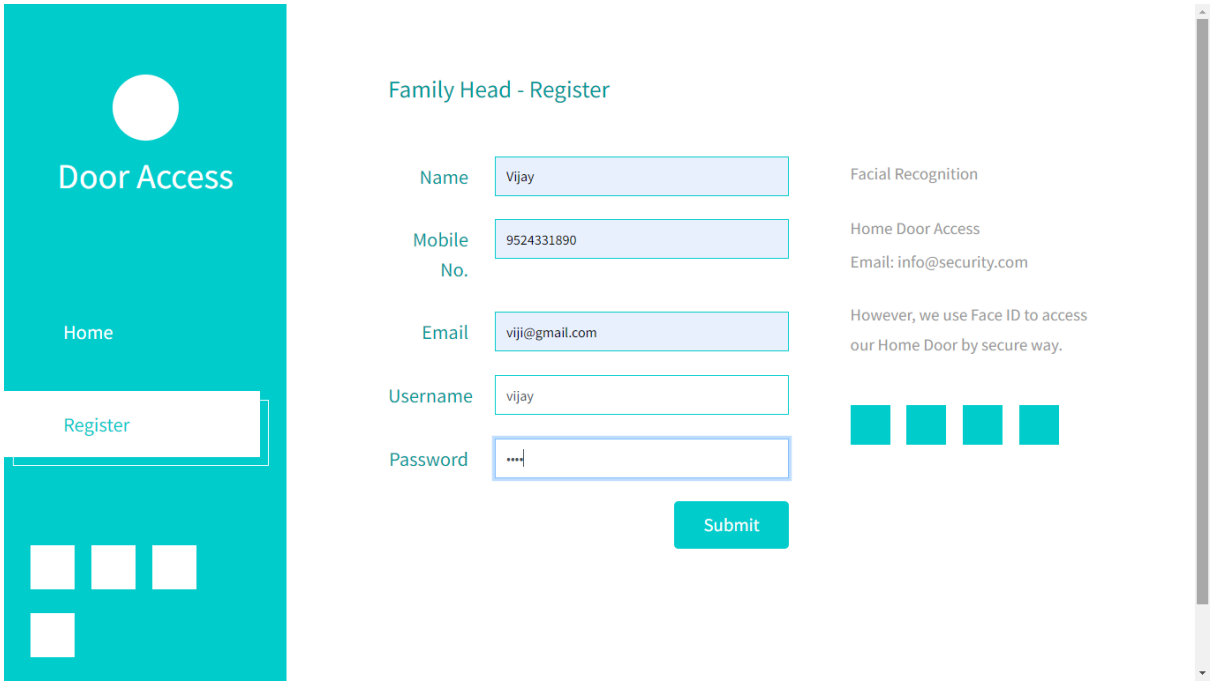
During testing, the system handled more than 1,000 user records without any noticeable performance issues, making it viable for use in large institutions, corporate offices, and campuses.

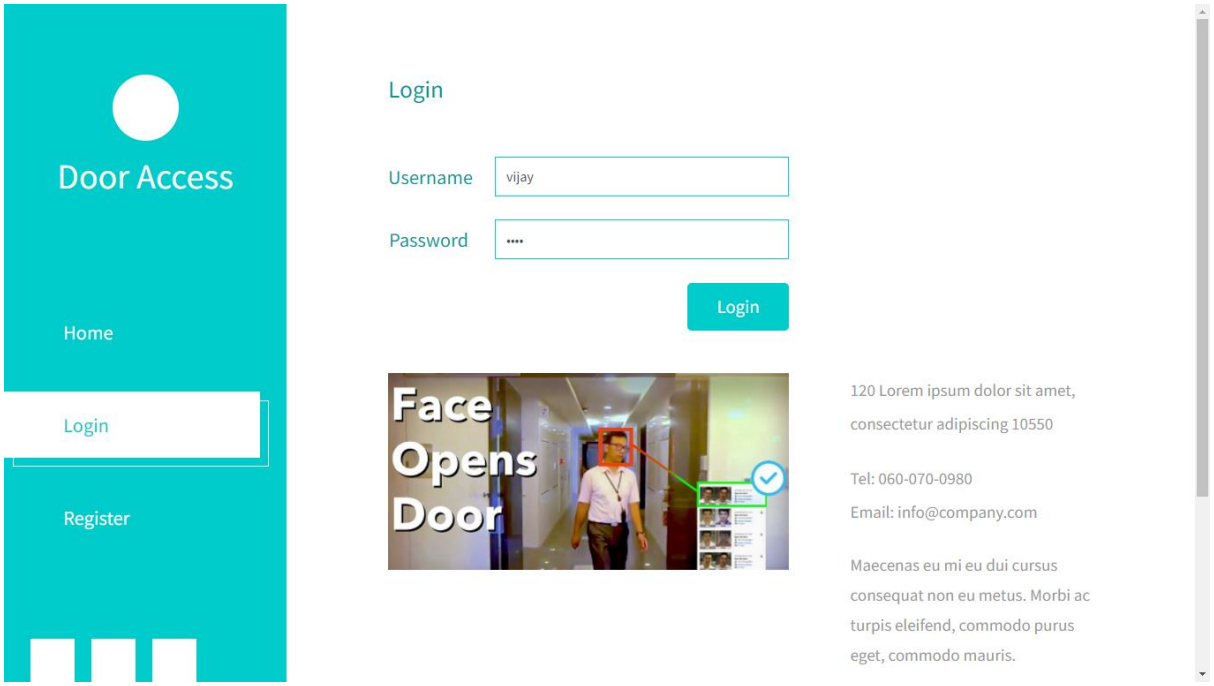
Strong Data Security Measures

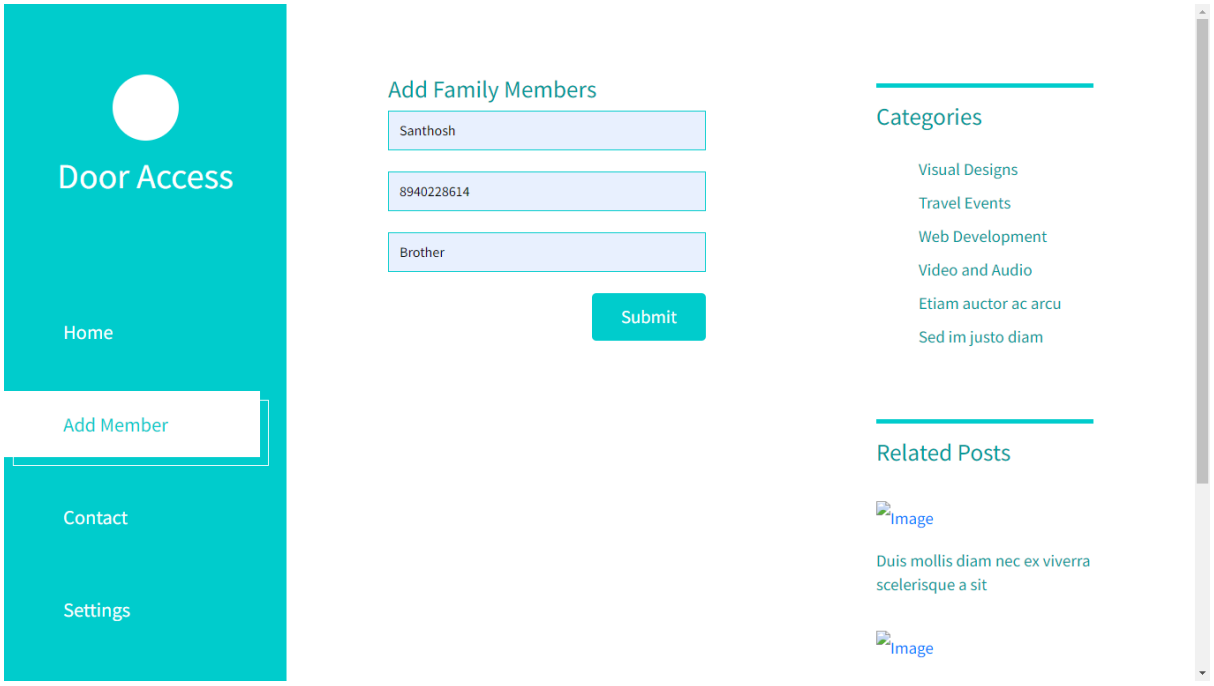
Facial images and access data were encrypted and stored securely, ensuring compliance with data privacy regulations. Only verified users could access system configurations and sensitive records.

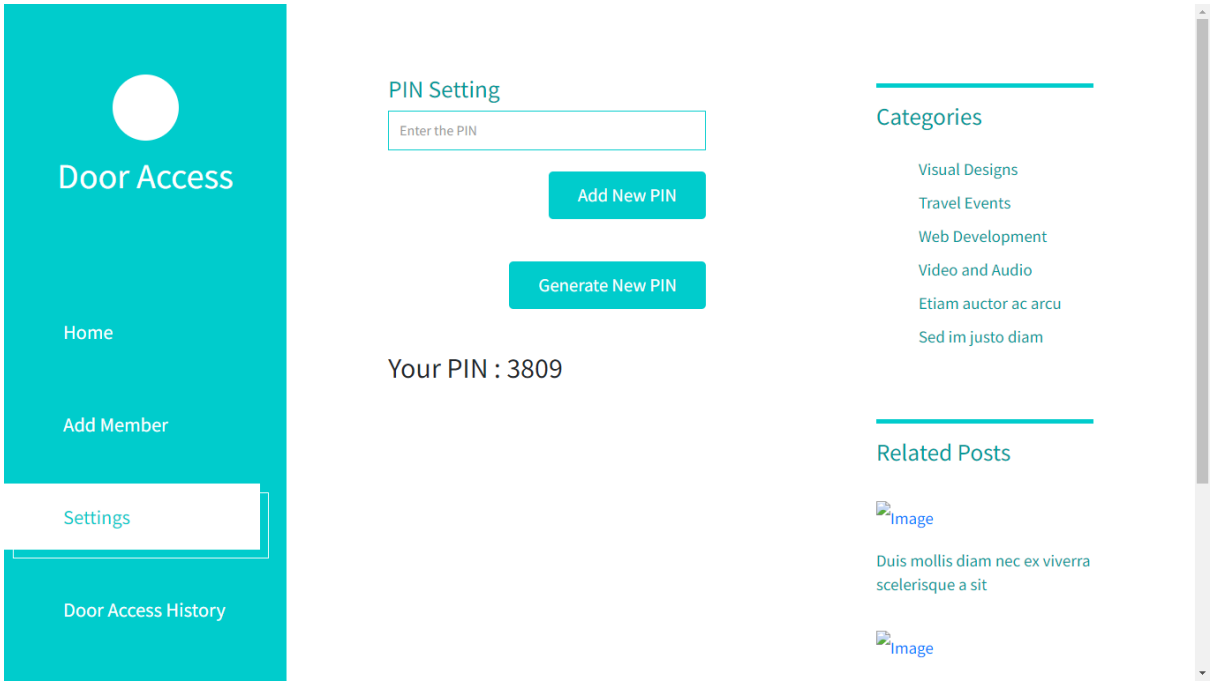
Low Energy Consumption

The components and processing methods used in the system were optimized for energy efficiency, enabling deployment in locations with limited or backup power sources.


Door Access
Home
Register
Family Head - Register
Name
Vijay
Mobile No.
9524331890
Email
viji@gmail.com
Username
vijay
Password
Submit
Facial Recognition
Home Door Access
Email: info@security.com
However, we use Face ID to access our Home Door by secure way.


Door Access
Home
Login
Register
Login
Username
vijay
Password
Login
Face Opens Door
120 Lorem ipsum dolor sit amet, consectetur adipiscing 10550
Tel: 060-070-0980
Email: info@company.com
Maecenas eu mi eu dui cursus consequat non eu metus. Morbi ac turpis eleifend, commodo purus eget, commodo mauris.





3. CONCLUTION

This study introduces an innovative approach to enhancing smart home security through advanced biometric authentication methods. The system incorporates models for both facial and voice recognition to verify user identities. Facial authentication utilizes a Mask-Region Convolutional Neural Network combined with FaceNet, leveraging one-shot learning techniques to analyze user images. Recognition is performed by extracting key facial features and calculating the minimum distance metric to determine if the individual matches a registered profile or is unknown. Importantly, the model is designed to accurately identify users whether they are wearing masks or not, provided that critical facial regions such as the eyes

and nose remain visible. The integrated system achieves an overall accuracy of 82.71%, demonstrating promising performance for securing smart home environments.

4. ACKNOWLEDGMENT

The authors declare that they have no reports of acknowledgments for this

REFERENCES

1. He, K., Gkioxari, G., Dollár, P., & Girshick, R. (2017). Mask R-CNN. Proceedings of the IEEE International Conference on Computer Vision (ICCV),2961–2969.
2. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 815–823.
3. Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks. IEEE Signal ProcessingLetters,23(10),1499–1503.
4. Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXivpreprintarXiv:1804.02767.
5. EdgeX Foundry. (n.d.). An Open Platform for Edge Computing. https://www.edgexfoundry.org/
6. OpenCV. (n.d.). Open Source Computer Vision Library. https://opencv.org/
7. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.