

# A Literature Survey on Smart Home Security

Arshi Khan<sup>1</sup>, Aasha Meena<sup>1</sup>, Aashiya Ansari<sup>1</sup>, Rozy Khan<sup>1</sup>, Suman Sen<sup>1</sup>, Komal Meghani<sup>1</sup>, Dr. Kalraiya<sup>2</sup>

<sup>1</sup> Research Scholar, Dept. Of ECE, SISTec Gandhi Nagar, Bhopal, Madhya Pradesh, India

<sup>2</sup> Associate Professor, Dept. Of ECE, SISTec Gandhi Nagar, Bhopal, Madhya Pradesh, India

## ABSTRACT

*The integration of facial recognition technology with machine learning has significantly advanced modern security systems. This paper reviews the current state of smart security systems that employ these technologies to automatically authenticate individuals, grant access to authorized personnel, and alert administrators by transmitting images of unauthorized individuals via cloud platforms. Various methodologies, system architectures, and the effectiveness of these integrated systems are discussed.*

**Keywords:** - Smart Security Systems, Facial Recognition, Machine Learning, Image Processing, Access Control.

## 1. INTRODUCTION

This research focuses on developing a smart home security system using face recognition technology with ESP32, FTDI module, and a camera. The system captures an image of the person at the door and checks it against a stored database. If the face matches, access is granted; otherwise, entry is denied[1]. This solution provides an efficient, low-cost, and intelligent method to enhance home security by allowing only authorized individuals to enter. This smart setup not only increases safety but also allows for remote monitoring and control, making it an ideal solution for modern homes.

Security has become a critical concern in both residential and commercial sectors due to the increasing instances of unauthorized access, theft, and cyber threats. Traditional security systems, such as locks, alarm systems, and CCTV cameras, have limitations in terms of active response, accuracy, and adaptability to dynamic threats. The need for more intelligent, responsive, and automated security systems has led to the development of smart security systems. Smart security systems are integrated frameworks that leverage emerging technologies such as facial recognition, machine learning, and cloud computing to enhance surveillance and access control. Facial recognition allows these systems to identify individuals based on unique facial features, making it a reliable biometric authentication method [2]. Machine learning enhances recognition accuracy by learning from data and adapting to new patterns over time [3]. Cloud computing supports these systems by enabling remote access, real-time notifications, and secure storage of image and log data [4].

These technologies work together to create an environment where access can be granted automatically to recognized individuals and denied to unauthorized ones. Additionally, the system can notify administrators and transmit the images of unidentified individuals to the cloud for further analysis or record-keeping. This automation minimizes human intervention, reduces response time, and increases security effectiveness [5].

This review aims to present an overview of the architecture, working principles, and key technologies behind such smart security systems. It also highlights real-world applications, benefits, and current challenges, along with prospects for future developments.

## 2. Challenges and Considerations

Despite advancements, several challenges persist:

- **Privacy Concerns:** Ensuring that facial recognition systems comply with legal and ethical standards to protect individual privacy.
- **Accuracy and Bias:** Addressing potential biases in recognition algorithms that may affect accuracy across different demographics.
- **Security of Data:** Protecting stored data from unauthorized access and cyber threats.
- **Environmental Factors:** Maintaining system performance under varying lighting conditions and angles of facial presentation

### 3. Related work

1. **Nguyen et al. – Smart Security System with Face Recognition[6]**
  - Describes a face recognition-based smart security system using image processing techniques.
  - Lacks cloud support and real-time remote monitoring.
2. **Shahrani et al. – Smart Building Security System with Face Recognition[7]**
  - Integrated intelligent face detection with cloud storage for monitoring.
  - Processing was not real-time and focused on batch uploads.
3. **Pulugu et al. – Machine Learning-Based Facial Recognition for Surveillance[8]**
  - Focused on video surveillance with facial recognition using ML models.
  - No access control mechanism (e.g., no door automation).
4. **Uddin et al. – Smart Home Security with Facial Authentication and Mobile App[9]**
  - Combines facial authentication with a mobile app for access control.
  - Better suited for individual use than multi-user institutional settings.
5. **Sharma and Dey – Door Unlock System Using Facial Recognition[10]**
  - Designed a low-latency indoor door access system using face detection.
  - Did not include cloud alerts or logging unauthorized users.

**6. Turk and Pentland – Eigenfaces for Recognition[11]**

One of the earliest approaches to facial recognition using PCA.

Still relevant as a baseline but limited in complex environments.

**7. Belhumeur et al. – Fisherfaces using LDA[12]**

- Improved classification performance over PCA-based methods.
- Effective in small-scale or controlled environments.

**8. Chen et al. – Cognitive Computing in Smart Surveillance[13]**

- Proposed edge-cloud hybrid architecture for faster decision-making.
- High performance, but system complexity increases.

**9. Singh et al. – Secure Cloud-Based Surveillance System[14]**

- Emphasized secure cloud storage for facial recognition systems.
- Lacked edge-based real-time control.

**10. Kumar and Devi – Facial Recognition for Attendance Systems[15]**

- Used facial recognition in office environments to automate attendance.
- Integrated with cloud database, but limited in multi-layered access.

**11. Arpaci et al. – Ethical Issues in Smart Systems[16]**

- Investigated privacy and ethical concerns in smart surveillance systems.
- Highlights the need for privacy compliance in system design.

**12. Buolamwini and Gebru – Gender Shades[17]**

- Analyzed algorithmic bias in facial recognition systems.
- Calls for diverse datasets to improve fairness.

#### 4. What Makes Our Project Different

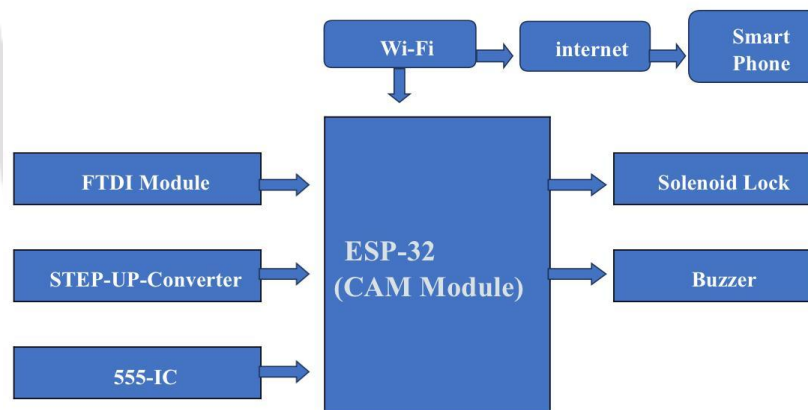
After reviewing all the existing work, we found that most projects focused on just one or two features. Some of them only used facial recognition without any real-time alerts or cloud access, while others stored data in the cloud but didn't actually control a door or send alerts when someone unauthorized tried to enter. A few older systems used traditional methods like PCA and LDA which don't work very well in real-world conditions, especially with poor lighting or different face angles.

**What makes our project stand out** is that it brings together **real-time facial recognition, automatic door control using a solenoid lock, and instant cloud-based alerts**—all in one system. When someone unauthorized is detected, the system takes their picture and immediately sends it to the admin through the cloud. Plus, it's **affordable, easy to set up**, and works well for homes, offices, or schools.

Moreover, it enhances security by **instantly capturing and sending the image of any unauthorized person to the admin via the cloud**, a feature rarely implemented in earlier models.

Additionally, the system is **designed to be scalable, cost-effective, and easy to deploy** in both home and institutional environments. These integrated features—**real-time decision-making at the edge, cloud alerting for unauthorized access, and practical automation using hardware components**—are not collectively present in any single prior work reviewed in this paper.

In short, our project combines the best parts of earlier systems and adds features they were missing, making it more complete and practical for everyday use.



#### 5. FUTURE WORK

To enhance security, future developments will focus on:

- **AI-Based Threat Analysis:** Implementing machine learning models to distinguish between real threats and false alarms.
- **Blockchain for Access Control:** Secure, decentralized authentication for better user access management.
- **Cloud Integration:** Storing event data for analytics and automated emergency responses.





## 6. ACKNOWLEDGEMENT



The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

## 7. CONCLUSION

Smart home security is an evolving field that requires continuous innovation. The proposed system integrates multiple security mechanisms with AI-driven threat detection and cloud connectivity, addressing key limitations of existing solutions. Future research should focus on improving response accuracy and enhancing user control capabilities to create a truly intelligent security system.

## 7. REFERENCES

- [1] Dokic K., Martinovic M., & Radisic B. (2020). Neural networks with ESP32 - Are two heads faster than one? *Conference on Data Science and Machine Learning Applications (CDMA 2020)*. DOI: 10.1109/CDMA47397.2020.00030.
- [2] T. Nguyen, B. Lakshmanan, and W. Sheng, "A Smart Security System with Face Recognition," arXiv preprint arXiv:1812.09127, 2018.
- [3] D. Pulugu et al., "Machine Learning-Based Facial Recognition for Video Surveillance Systems," *ICTACT Journal on Image and Video Processing*, vol. 14, no. 2, pp. 3149–3154, 2023.
- [4] S. Shahrani et al., "A Smart Building Security System with Intelligent Face Detection and Recognition," *IOP Conference Series: Materials Science and Engineering*, vol. 1176, no. 1, p. 012030, 2021.
- [5] K. M. M. Uddin et al., "Smart Home Security Using Facial Authentication and Mobile Application," *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 2, pp. 40–50, 2022.
- [6]  [Paper Link \(arXiv\)](#)
- [7]  [Paper Link \(IOP Science\)](#)
- [8]  [Paper Link](#)
- [9]  [Paper Link](#)

- [10]  [Paper Link \(ResearchGate\)](#)
- [11]  [Paper Link \(ResearchGate\)](#)
- [12]  [Paper Link \(ResearchGate\)](#)
- [13]  [IEEE Xplore Link](#)
- [14]  [Paper Link \(IJRASET\)](#)
- [15]  [Paper Link \(ResearchGate\)](#)
- [16]  [ScienceDirect Link](#)
- [17]  [Paper Link \(MIT Media Lab\)](#)

