Artificial Intelligence-Driven Smart Home Control with Face Recognition System

[1]Dr. Y. Chitti Babu,[2]Kamparaju Sindhura,[3]Bussa Santhi,[4]Buddi Swapna

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

This project presents an AI-driven smart home control system integrated with face recognition technology. The system enhances home security and automation by identifying authorized users. It ensures convenience, safety, and intelligent decision-making through artificial intelligence. The system uses camera-based monitoring and computer vision techniques to identify authorized users and grant or deny access accordingly. Unauthorized access attempts are restricted, improving overall home safety. Traditional home security systems rely on physical keys. passwords, or access cards, which can be lost, stolen, duplicated, or misused, leading to security vulnerabilities. These systems also lack intelligent user identification and real-time monitoring of unauthorized access. There is a need for a secure, contactless, and cost-effective smart home access control system that can accurately identify individuals and restrict entry to authorized users only.

KEYWORDS: Artificial Intelligence (AI), Face Recognition, Computer Vision, Deep Learning, Face Authentication, Real-Time Detection, Image Processing.

INTRODUCTION

Smart homes aim to automate household functions such as lighting, security, and appliances. With advancements in Artificial Intelligence and Computer Vision, face recognition has become a reliable biometric authentication method. This project combines smart home automation with AI-based face recognition to improve security and user's home safety. The proposed system not only improves security but also adds an

additional layer of intelligence by enabling personalized automation.

LITERATURE SURVEY

Smart home systems have gained significant attention in recent years due to rapid advancements in information and communication technologies. A smart home is generally defined as a residential environment that integrates sensing, communication, and intelligent control technologies to enhance comfort, security, energy efficiency, and quality of life. The core concept of smart homes revolves around automation and intelligent decision-making using real-time data collected from various devices.

RELATED WORK

Several researchers have contributed to the development of smart home systems with the aim of improving comfort, energy efficiency, security, and automation. Initial related work in domain focused on basic home automation systems where household appliances were controlled manually or through simple rule-based mechanisms. These systems relied on wired communication and predefined schedules, offering limited flexibility and intelligence.

EXISTING SYSTEM

The existing smart home systems mostly depend on manual switches, mobile applications, passwords, or PIN-based access. Users must actively operate these systems to control lights, fans, and other appliances. Security is commonly provided through keys or numeric codes, which can be lost, shared, or easily guessed. These methods do not offer strong protection against unauthorized access. Automation in current systems is very limited and follows fixed rules. There is no intelligent mechanism to automatically verify a person's identity. Continuous monitoring is often missing in traditional setups. Any breach may go unnoticed until manual checking is done. Overall, the existing system lacks advanced security, intelligence, and reliable automation.

PROPOSED SYSTEM

The proposed system implements AI-driven face recognition for secure user authentication in a smart home environment. It continuously monitors the entry area using a camera to detect and recognize faces in real time. Access is granted only to authorized users, while unauthorized individuals are blocked. This approach significantly

enhances home security and helps prevent theft and unauthorized entry. The system eliminates the need for physical keys, cards, or PINs, making access completely contactless. A webcam is used for face capture, reducing additional hardware costs. Authorized user data is securely stored in a database for reliable verification.

SYSTEM ARCHITECTURE

The architecture of the AI-driven smart home control system consists of a webcam, face recognition module, user database, access control unit, and smart door system. The webcam captures real-time facial images of the user and sends them to the face recognition module.

The face recognition module processes the image and compares it with stored facial data in the user database. Based on the authentication result, the access control unit decides whether to grant or deny access. If the user is authorized, the system unlocks the door; otherwise, access is denied and an alert is generated. This architecture ensures secure, contactless, and real-time access control for smart homes.

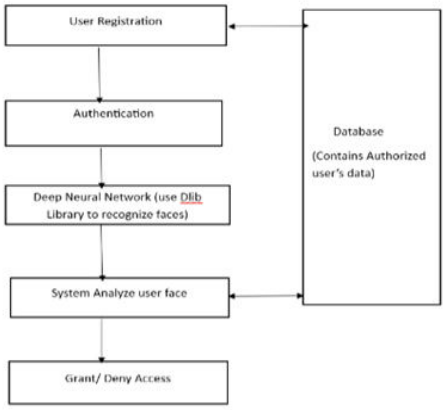

Fig 1: System Architecture

METHODLOGY DESCRIPTION

The methodology of the smart home system is designed to provide intelligent automation, monitoring, and control of household appliances using modern communication and computing technologies. The system follows a structured approach that includes data acquisition, communication, processing, decision-making, and actuation.

RESULTS AND DISCUSSION

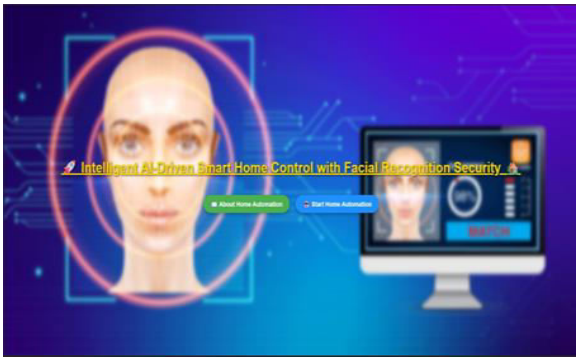

Fig2: Home page of Facial Recognition

The home page of the facial recognition system serves as the main interface through which users interact with the application. It is designed to be simple, user-friendly, and secure, providing quick access to the core functionalities of the system.

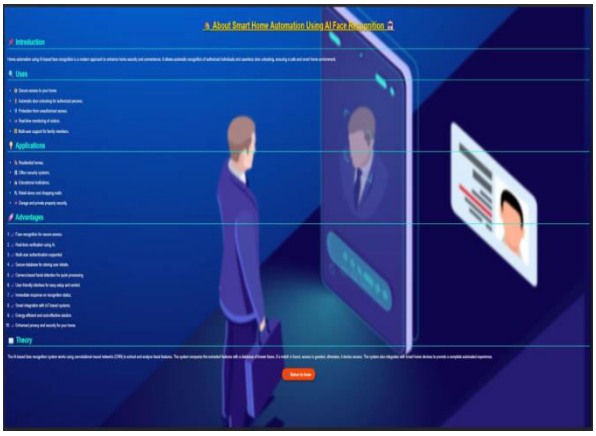

Fig 3: About Module

The home page using **AI-based Face Recognition** acts as the primary entry point of the system, enabling secure and intelligent user authentication. It is designed to provide real-time face detection and recognition using artificial intelligence and deep learning techniques.

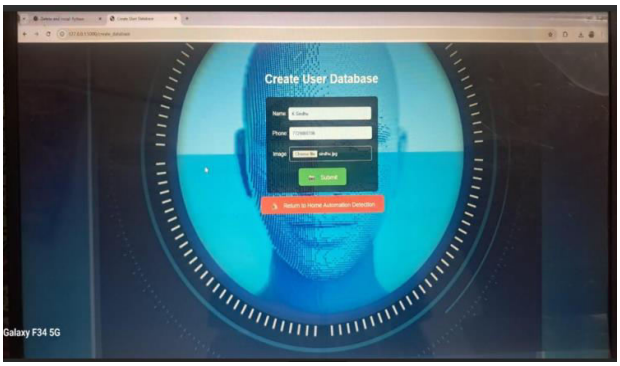

Fig 4: Register Page

The **Create User Database** module is a crucial component of an AI-based face recognition system. This module is responsible for registering new users and storing their facial data securely for future identification and authentication.

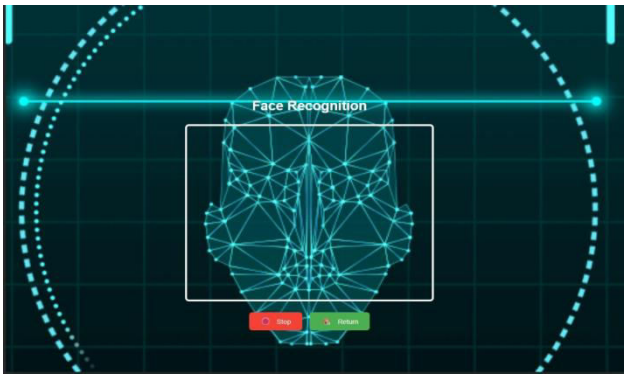

Fig 5: Face Recognition

The **Face Recognition** module is the core component of the AI-based system, responsible for identifying or verifying individuals by analyzing facial features. This module operates by comparing real-time facial data with stored information in the user database to determine identity.

CONCLUSION

The AI-driven smart home control system with face recognition enhances protection and safety by allowing access only to authorized users. By preventing unauthorized entry and automating home operations, the system ensures a secure, reliable, and intelligent living environment.

FUTURE SCOPE

The proposed AI-driven smart home control system can be further enhanced by integrating

advanced deep learning models to improve face recognition accuracy under varying lighting and pose conditions. Multi-factor authentication such as combining face recognition with voice or mobile-based verification can be added for higher security. The system can be extended to support cloud storage and mobile applications for remote monitoring and control. Integration with IoT devices like smart lights, alarms, and surveillance cameras can provide complete home automation. Additionally, real-time alert systems using SMS or mobile notifications can be improved to enhance response to unauthorized access.

REFERENCES

[1]Harini, P. (2019). GESTURE CONTROLLED GLOVES FOR GAMING AND POWER POINT PRESENTATION
CONTROL. *GESTURE*, *6*(12).

[2] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM Computing Surveys.

[3] Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. IEEE CVPR.

[4] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Face Net: A unified embedding for face recognition. IEEE CVPR.

[5] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). Deep Face: Closing the gap to human-level performance. IEEE CVPR.

[6] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. BMVC.

[7] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems.

[8] Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). Biometric systems: Technology, design and performance evaluation. Springer.

[8] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometric systems. IBM Systems Journal.

[10] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Biometric Anti-Spoofing. Springer.

[11] Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. IEEE Transactions on Information Forensics and Security.

[12] Li, S. Z., & Jain, A. (2011). Handbook of Face Recognition. Springer.

[13] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric anti-spoofing methods: A survey in face recognition. IEEE Access.

[14] Erdogmus, N., & Marcel, S. (2014). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. IEEE Biometrics Special Interest Group.

[15] Pinto, A., Pedrini, H., Schwartz, W. R., & Rocha, A. (2012). Face spoofing detection

through visual codebooks of spectral temporal cubes. IEEE Transactions on Image Processing.

[16] Patel, K., Han, H., & Jain, A. K. (2016). Secure face unlock: Spoof detection on smartphones. IEEE Transactions on Information Forensics and Security.

[17] Yang, J., Lei, Z., Liao, S., & Li, S. Z. (2014). Learn convolutional neural network for face anti-spoofing. IEEE Transactions on Information Forensics and Security.

[18] Boulkenafet, Z., Komulainen, J., & Hadid, A. (2016). Face anti-spoofing based on color texture analysis. IEEE International Conference on Image Processing.

[19] Atoum, Y., Liu, Y., Jourabloo, A., & Liu, X. (2017). Face anti-spoofing using patch and depth-based CNNs. IEEE International Joint Conference on Biometrics.

[20] Chingovska, I., Anjos, A., & Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoofing. BIOSIG Conference.