Review on Face authentication for door lock system using IOT

Puneeth R[1], Rathna Naik K M[1], Shashank S Gowda[1], Shreyas S[1]

Raghavendra Babu T M[2]

[1] Department of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

[2] Assistant Professor Dept. of CSE, P.E.S. College of Engineering, Mandya, Karnataka, India

ABSTRACT: The integration of IoT and AI in smart door lock systems has revolutionized home security by enabling advanced authentication methods such as face recognition, RFID, and temperature-based access control. These technologies enhance security through contactless operation, anomaly detection, and real-time monitoring, reducing vulnerabilities associated with traditional locking mechanisms. Various approaches, including ESP32-CAM-based systems, deep learning models, and Arduino-powered intrusion detection, have been explored to improve reliability and efficiency. With continuous advancements in sensor technology and machine learning, future smart door locks promise even greater accuracy and robustness in safeguarding residential and commercial spaces.

Key words: Facial Recognition, Raspberry Pi, IoT-Enabled Contactless Detection, Motion Detection, Smart Door Lock, Access Control Systems.

I. INTRODUCTION

Facial recognition-based doorbell and lock systems have emerged as a secure and convenient solution for modern access control. These systems utilize artificial intelligence, IoT, and deep learning techniques to authenticate individuals and enhance home security. Advanced models, such as those integrating OpenCV and Haar Cascade classifiers, detect and verify faces against a stored database, ensuring that only authorized individuals gain access. Some systems incorporate additional security features, such as temperature monitoring, to restrict entry if abnormal conditions are detected. Deep learning models, including logit-boosted CNNs, have further improved accuracy in face recognition and anomaly detection. IoT-based solutions leverage cloud storage and real-time mobile notifications, allowing homeowners to monitor visitors remotely. Raspberry Pi and ESP32-based implementations provide cost-effective and efficient alternatives, enabling smart locks to function without physical keys. Additionally, hybrid approaches integrating masked face recognition techniques ensure reliable authentication even when users wear face coverings. These innovations enhance security, convenience, and automation, making facial recognition-based door lock systems an essential component of smart home technology.

II. LITERATURE SURVEY

The author's Sachin Sharma, Mayank Sharma, Gopal Sharma, and Akash Bhasney have developed a multi-layered authentication method integrating facial recognition with healthmonitoring. Utilizing OpenCV and the Haar Cascade algorithm, it ensures only authorized individuals are granted access. If an abnormal temperature is detected, entry is denied to mitigate health risks and addresses the limitations of traditional access control methods by enhancing both security and safety, offering a comprehensive solution to modern security challenges across various environments [1]. As per Mohd Raza Moghul, Riddhesh Barve, Umesh Pal, Nadeem Shaikh, and Kavita Bani, an advanced home security solution has been developed that leverages IoT technology, motion detection, and real-time communication to provide secure remote monitoring of visitors. It eliminates the need for direct contact by integrating smart sensors, a Raspberry Pi-based control unit, and cloud-based communication [2]. According to Pooja Bende, Komal Taral, Tanvi Vadjikar, and

Jitendra Bakliwal, the system captures and analyzes a visitor's image using face detection algorithms in Python. The identified image is then sent to the owner's Android app via Wi-Fi for verification. Finally, the owner can accept or reject access through the app to control the door unlocking process [9]. In the words of Shweta Malve and Dr. S. S. Morade, when the doorbell is pressed, it captures the visitor's image and converts it to grayscale. The Haar-Cascade classifier then detects the face and checks it against a stored database. If a match is found, the visitor's name is announced otherwise, the image is stored. It enhances security by recognizing known visitors and updating the database with new ones [10].

Based on the work of Onuike C. B., Amagba S. O., Ezekwem C. M., and Nwaji G. N., a cost- effective facial recognition system has been developed for security applications using a Raspberry Pi 3 and locally sourced materials. It integrates microcontrollers, sensors, and Python programming, featuring a display screen and a buzzer for user interaction. Developed using Dennis and Wixom's prototype methodology, it successfully distinguishes authorized individuals from unauthorized ones. Hardware improvements are suggested to enhance performance, while future enhancements include voice assistance, police database integration, and cloud storage for further optimization [5]. In accordance with the work of Asif Rahim, Yanru Zhong, Tariq Ahmad, Sadique Ahmad, Paweł Pławiak, and Mohamed Hammad, exploring the use of deep learning, particularly logit-boosted CNN models, for anomaly detection and face recognition in IoT-enabled smart homes. Six models integrating logistic regression (LR), gradient-boosting classifiers (GBCs), and convolutional neural networks (CNNs) were evaluated, with the LR-HGBC-CNN model achieving the highest accuracy in both tasks. Highlighting the potential of deep learning in enhancing smart home security and privacy while also addressing challenges related to generalizability, privacy-preserving techniques, and deployment. It calls for further research to overcome these limitations [6]. From the perspective of KH Teoh, RC Ismail, SZM Naziri, R. Hussin, MNM Isa, and MSSM Basir, it describes the process, including face detection with Haar Cascade classifiers and image processing through deep learning techniques. TensorFlow is utilized to train the classifier, enhancing recognition accuracy and highlighting the effectiveness of deep learning in improving face identification, with experimental results demonstrating the system's successful implementation [8]. Michal Kelemen, Ivan Virgala, Tatiana Kelemenová, Ľubica Miková, Peter Frankovský, Tomáš Lipták, and Milan Lorinc contend that ultrasonic sensors are used for non- contact distance measurement by transmitting and receiving sound waves. Sensors function by measuring the time of flight of an ultrasonic wave to a detected object. Since most materials

reflect sound waves, ultrasonic sensors are suitable for various applications. Unlike photoelectric sensors, they excel in detecting films, transparent objects, and liquids. Additionally, their performance is unaffected by target color or frequent color changes [13]. As discussed by Kurra Naga Sai, Dr. T.D. Sunil, and Dr. M.N. Eshwarappa, reviews mechanical, electronic, and smart lock security systems, analyzing their mechanisms, strengths, and vulnerabilities. It explores emerging trends such as biometric authentication and smart home integration for enhanced security. Additionally, it addresses potential risks, including hacking and unauthorized access, with the goal of improving the design and implementation of advanced access control solutions [3].

The analysis by Mohan Kumar, Irfan Ahamath M, and Gowtham R presents the development of an RFID-based door lock system using an Arduino microcontroller for keyless and secure access. It enhances security by eliminating traditional keys and enabling remote monitoring through smartphone applications. Future improvements include biometric authentication and IoT integration to further enhance smart home security [4]. As expressed in the work of Mohammed Emen, Tarek M. Mahamoud, Mostafa M. Ibrahim, and Tarek Abd El-Hafeez, a novel hybrid approach for masked face recognition is proposed. This approach integrates deep learning-based mask detection, landmark and oval face detection, and robust principal component analysis (RPCA). A pretrained SSD-MobileNetV2 model is used for mask detection, while RPCA separates occluded components to enhance recognition accuracy. Additionally, particle swarm optimization (PSO) fine-tunes KNN features and optimizes the number of nearest neighbors for classification. Experimental results demonstrate a 97% recognition accuracy, surpassing existing methods and highlights the advancements in masked face recognition and suggests further improvements for real-world applications [7]. In the words of Oladunjoye John Abiodun and Okwori Anthony Okpe, an IoT-based security system has been developed for smart homes. It utilizes an Arduino Uno microcontroller, ultrasonic sensors, and a GSM module to detect intrusions and send SMS alerts to homeowners, primarily for security purposes [11]. The analysis by Amuta E.O., Sobola G.O., Eseabasi O., Dike H.N., Matthew S., Agbetuyi A.F., and Wara S.T., primarily focuses on the design of a home security system based on PIR sensors and a fire detection system using LM35 temperature sensors. It presents the development of an integrated security and fire detection system utilizing Passive Infrared Receiver (PIR) sensors and LM35 temperature sensors, combined with an Arduino Uno microcontroller [14]. According to Yashaswi R, Abdulwahab Ahmed Mohamed Omer, Nikhil Reji, Muhammed Mishal, and Nagaraja P. S., on security whether data security or home security is a primary concern. With advancements in technology and the growing use of IoT, digital door locks have become increasingly common. Unlike traditional locks that require a physical key, digital locks utilize methods such as Radio-Frequency Identification (RFID), fingerprints, Face ID, PINs, and passwords. Various digital door lock solutions have already been developed using these technologies. To ensure home security, owners typically keep doors locked at all times. However, in a rush, they may forget to lock the door or be uncertain whether they have locked it. The author's present a smart Wi-Fi Door Cinch using the ESP32 CAM and the Blynk App, offering a convenient and efficient solution for remote door locking and monitoring [12].

III. METHODOLOGY

This section presents the methodologies employed in various motion and presence detection technologies used in smart home security and automation systems. These methodologies integrate sensor-based detection, IoT networks, Arduino, Raspberry Pi, and digital image processing to enhance security and access control. Each technology has its advantages and limitations, along with specific technological gaps that highlight areas requiring further research and improvement.

Author	Methodology	Advantages	Disadvantages
Oladunjoye John Abiodun et al. (2024) [11]	**Ultrasonic Sensors:** Detects intrusions by measuring sound wave reflections	High accuracy in detecting motion, works in darkness	Prone to false alarms from environmental noise
Amuta E.O et al. (2025) [14]	**Passive Infrared (PIR) Sensors:** Detects human motion by sensing infrared radiation from warm objects	Low power consumption, cost-effective	Cannot detect static objects, affected by environmental conditions
Pooja Bende et al. (2021) [9]	**Camera-Based Detection:** Uses digital image processing for facial recognition	Provides detailed visual data, enables facial recognition	High processing power required, privacy concerns
Mohd Raza Moghul et al. (2024) [2]	**IoT-Enabled Contactless Detection:** Integrates multiple sensors with internet connectivity	Remote access, real-time monitoring	Requires a stable internet connection, potential cybersecurity risks
Shweta Malve et al. (2021) [10]	**Facial Recognition:** Machine learning-based object detection using Haar Cascade and LBPH methods	High security, contactless authentication	Performance affected by lighting and image quality
Mohan Kumar A et al. (2024) [4]	**Servo Motors:** Provides precise movement for locking mechanisms	Reliable and allows controlled movement	Requires calibration, can wear out over time

Sachin Sharma et al. (2024) [1]	**Solenoid Locks:** Uses electromagnetism for secure locking	Strong locking mechanism, fast response time	Requires continuous power, can overheat
Mohd Raza Moghul et al. (2024) [2]	**Accessibility Features:** Provides voice alerts and automation for individuals with disabilities	Improves usability for disabled individuals	Can be expensive to implement, requires technical knowledge

Table 1: A brief description of methodologies used.

The survey provides various motion and presence detection technologies used in smart home security and automation systems, focusing on sensor-based detection integrated with Arduino, Raspberry Pi, IoT networks, and digital image processing. Ultrasonic sensors detect intrusions by measuring sound wave reflections, often paired with Arduino and GSM modules for real-time alert transmission. Passive Infrared (PIR) sensors identify human motion by sensing infrared radiation emitted by warm objects, triggering alarms or notifications. Camera-based detection, leveraging Raspberry Pi and digital image processing, enables facial recognition for identifying individuals at entry points. Additionally, IoT-enabled contactless detection integrates multiple sensors with internet connectivity, allowing remote monitoring and real-time alerts.

Facial recognition technology plays a crucial role in smart security applications, particularly in IoT-enabled door locks and monitoring systems. Most implementations utilize Raspberry Pi as the core processing unit, interfacing with Pi cameras for image acquisition and OpenCV for real-time face detection and recognition. The Haar Cascade algorithm, a machine learning-based object detection method, employs rectangular features and cascading classifiers for rapid face detection, while the Local Binary Pattern Histogram (LBPH) method encodes texture patterns into histograms, ensuring accurate and reliable recognition even under varying lighting conditions.

Electronic locks further enhance security by providing keyless entry, programmed access control, and integration with access control systems. They authenticate users via keypads, RFID readers, and biometric scanners, eliminating physical keys, while smart locks incorporate internet connectivity through Wi-Fi, Bluetooth, or other protocols for remote access and mobile app integration. However, electronic locks require regular maintenance due to battery reliance and may be vulnerable to hacking. Servo motors and solenoid locks play a vital role in these mechanisms, with servo motors enabling precise movement control and solenoid locks using electromagnetism for secure and efficient access control. Moreover, these systems prioritize accessibility by offering voice alerts and automation features for individuals with disabilities. IoT integration further enhances convenience, allowing homeowners to receive notifications and visitor images via mobile applications, granting or denying access remotely.

Despite significant advancements in smart security and automation, several technological gaps remain. Ultrasonic and PIR sensors suffer from false positives due to environmental noise or

non-human movement, reducing reliability. Facial recognition algorithms often experience accuracy issues in poor lighting conditions, with aging faces, or when individuals wear masks, necessitating more advanced AI-driven recognition techniques. IoT-based security systems face cybersecurity vulnerabilities, as they rely on cloud storage and wireless networks that can be susceptible to hacking. Electronic locks, servo motors, and solenoid locks require continuous power supply and frequent maintenance, making them prone to battery depletion or mechanical failure. Additionally, while IoT integration improves convenience, many smart home security systems lack AI-driven adaptive accessibility features, limiting their usability for individuals with disabilities. Addressing these gaps through AI-driven improvements, energy-efficient designs, and enhanced security protocols will be crucial for the next generation of smart security systems.

IV. CONCLUSION

The literature survey highlights the advancements in smart home security systems, emphasizing the integration of IoT, facial recognition, and various sensor-based detection technologies. The reviewed studies demonstrate that Raspberry Pi, Arduino, and deep learning-based image processing significantly enhance security by enabling real-time monitoring and authentication. Ultrasonic and PIR sensors provide reliable motion detection, while electronic and smart locks offer keyless access control, improving convenience and safety. Despite these advancements, challenges such as hacking vulnerabilities, power dependencies, and environmental factors affecting recognition accuracy remain. Future research should focus on improving security algorithms, enhancing system efficiency, and integrating cloud-based storage and AI-driven decision-making for more adaptive and robust security solutions.

V. REFERENCES

[1] Sachin Sharma1, Mayank Sharma2, Gopal Sharma3, Akash Bhasney4, “IoT-Enabled Smart Door Lock System Using Temperature Sensor” (2024).

[2] Mohd Raza Moghul, Riddhesh Barve, Umesh Pal, Nadeem Shaikh, Kavita Bani, “Contactless IOT Doorbell & Security System” (2024).

[3] Kurra Naga Sai, Dr. TD Sunil and Dr. MN Eshwarappa, “A comprehensive review of door lock security systems” (2024).

[4] Mohan Kumar A.1*, Irfan Ahamath M.2 & Gowtham R, “Revolutionizing Home Security: A Comprehensive Overview of an Advanced RFID Door Lock System for Keyless Access and Smart Home Protection” (2024).

[5] Onuike, C. B., Amagba, S. O., Ezekwem, C. M. & Nwaji, G. N, “Design and Development of a Prototype Security Door Using Facial Recognition System” (2024).

[6] Asif Rahim 1, Yanru Zhong 2, Tariq Ahmad 3, Sadique Ahmad 4, Paweł Pławiak and Mohamed Hammad, “Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models” (2023).

[7] Mohammed Eman 1, Tarek M. Mahmoud 2, 3, Mostafa M. Ibrahim 4 and Tarek Abd El-Hafeez 2, “Innovative Hybrid Approach for Masked Face Recognition Using Pretrained Mask Detection and Segmentation, Robust PCA, and KNN Classifier” (2023).

[8] KH Teoh2, RC Ismail1,2, SZM Naziri2, R Hussin2, MNM Isa2 and MSSM Basir, "Face Recognition and Identification using Deep Learning Approach" (2020).
[9] Pooja Bende, Komal Taral, Tanvi Vadjikar, Jitendra Bakliwal, "Contactless Door Unlock System" (2021).
[10] Shweta Malve, Dr. S. S. Morade, "Face Recognition Technology based Smart Doorbell System using Python's OpenCV library" (2021).
[11] Oladunjoye John Abiodun and Okwori Anthony Okpe, "Smart Home Security using Arduino-based Internet of Things (IoTs) Intrusion detection System" (2024).
[12] Yashaswi R1, Abdulwahab Ahmed Mohamed Omer2, Nikhil Reji3, Muhammed Mishal4, Nagaraja P S5, "SMART DOOR LOCK SYSTEMUSING ESP32 CAM IOT BASED" (2024).
[13] Michal Kelemen1*, Ivan Virgala1, Tatiana Kelemenová2, Ľubica Miková1, Peter Frankovský1, Tomáš Lipták1, Milan Lörinc, "Distance Measurement via Using of Ultrasonic Sensor" (2015).
[14] Amuta E.O.1, Sobola G.O.1, Eseabasi O.1, Dike H. N.2, Matthew S.3, Agbetuyi A.F.1, Wara S. T. 4, "Motion Detection System Using Passive Infrared Technology" (2025).