International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 744-759
https://doi.org/10.70917/ijcisim-2026-2394
Article

# AI-Powered Smart Home Security Using Facial Recognition and Block chain Logging

**Shakira[1], Veernala Sireesha[2], Shravani Amar[3], Katha. Chandrashekhar[4]**

[1] Department CSE-Cyber Security, Geethanjali College of Engineering and Technology, Cheeryal, Keesara, Hyderabad 501301
shakiranaim@gmail.com
[2] Department of Computer Science and Engineering, Malla Reddy Technical Campus (A Constituent Unit of Malla Reddy Vishwavidyapeeth, Deemed to be University, Hyderabad)
veernalasireesha@gmail.com
[3] Department of Computer Science and Engineering -Artificial Intelligence &Machine Learning, Mallareddy Reddy (MR) Deemed to be University, Hyderabad
shravaniathome@gmail.com
[4] Department of Computer Science and Engineering, St. Peters Engineering College, Hyderabad, 500075
shekhar.katha@gmail.com

**Abstract:** This project presents an AI-based smart home security system integrating facial recognition and blockchain technology to ensure secure, efficient access control and intrusion detection. Facial recognition enables biometric authentication, processed locally on edge devices for faster and private validation. Blockchain ensures tamper-proof identity verification and access logs without relying on a central authority. An AI-powered intrusion detection module monitors abnormal behavior through sensor data, enhancing real-time threat detection. The system provides end-to-end encrypted communication, role-based access, and audit-ready logs. Designed for scalability and privacy, the proposed model offers a robust, decentralized solution to address evolving smart home security challenges.

**Keywords:** Smart Home Security, AI, Blockchain, Facial Recognition, Intrusion Detection, Edge Computing

## 1 .INTRODUCTION

The rapid adoption of Internet of Things (IoT) technologies has revolutionized modern living by enabling automation and remote control of smart home environments. From smart locks to intelligent appliances, these connected systems offer unmatched convenience. However, with this increased interconnectivity comes heightened vulnerability to security breaches.

Traditional authentication methods like PINs or passwords are insufficient to protect sensitive data and device access from advanced threats. As smart homes store personal, behavioral, and biometric information, safeguarding them against intrusions and data tampering is critical. Technology can distinguish between authorized and unauthorized individuals, improving safety. When combined with blockchain technology, it ensures that all security data is stored in a decentralized, tamper-proof ledger, preventing any unauthorized alterations. The integration of AI, blockchain, and face recognition creates a more secure and reliable system, offering enhanced protection for modern homes.

This project introduces an AI-based security framework that combines facial recognition for biometric access and blockchain for decentralized authentication. Facial data is processed locally on edge devices, ensuring low latency and privacy, while blockchain technology offers immutable identity verification and secure access logs. An integrated AI-driven Intrusion Detection System (IDS) continuously monitors sensor data to detect abnormal behavior.


**Figure 1**: FIGURE1.Typical Model for Smart Homes

A conceptual model of a smart home ecosystem enhanced with modern security technologies. Inside the house, smart devices such as a Smart TV, Smart Lock, Smart Refrigerator, Smart Lighting, and Smart Air Conditioner are wirelessly connected to a central Home Gateway.

This gateway serves as the communication bridge between the smart devices and external entities. Outside the home, a Mobile User interfaces with the system remotely, while a Registration Server ensures secure identity verification. The dashed lines represent encrypted data exchange over the internet

## 2. EXISTING SYSTEM

The existing systems for home security often rely on traditional methods like alarm systems, motion sensors, and CCTV cameras, but these technologies lack the advanced intelligence and security needed for modern homes. AI-based smart home security systems utilize machine learning and computer vision to enhance surveillance by identifying faces and detecting unusual activities. These systems can differentiate between authorized and unauthorized individuals, providing an added layer of security. However, such systems can still be vulnerable to hacking and data breaches.

Blockchain technology addresses these vulnerabilities by offering a decentralized and immutable ledger for storing security data. By integrating blockchain with AI-based smart home security, the system ensures that all data related to home surveillance is securely stored and cannot be tampered with. Face recognition further enhances security by enabling biometric identification, ensuring that only authorized individuals have access to the home. This combination of AI, blockchain, and facial recognition offers a robust and future-proof solution for home security.

## 3. CHALLENGES

Despite the promising potential of AI-based smart home security systems with blockchain and face recognition, several challenges must be addressed for widespread adoption. One major challenge is the complexity and cost of implementation. The integration of AI, blockchain, and face recognition technologies requires significant computational resources, which can be expensive to deploy and maintain, especially for consumers with limited technical expertise. Additionally, ensuring seamless interoperability between different devices and systems can be a technical hurdle, as smart home products often come from different manufacturers with varying standards.

Another challenge lies in privacy and data security concerns. While blockchain offers enhanced data protection, the use of face recognition technology raises significant privacy issues. Storing biometric data, even in a decentralized manner, can lead to potential misuse or unauthorized access if not properly safeguarded. Moreover, ensuring compliance with regulations like GDPR and other privacy laws can be complex, particularly when dealing with personal data. Finally, AI systems need to be constantly updated to avoid vulnerabilities, which poses challenges in maintaining the system's integrity and security over time.

- Limited resources of smart devices, including low processing power, memory, and battery capacity.
- Vulnerability to physical attacks like device cloning, tampering, and node capture.
- Maintaining user privacy and secure key management.
- Biometric data noise leading to authentication failure.
- Scalability and performance issues as the number of devices and users increases.
- Secure registration process to prevent unauthorized devices or users from enrolling.
- User experience and the need for fast and simple authentication processes.

## 4. LIMITATIONS OF EXISTING SYSTEM

a. **Vulnerability to Hacking:** Traditional systems, like alarms and CCTV cameras, rely on centralized networks, making them prone to cyberattacks and unauthorized access.

b. **Lack of Advanced Intelligence:** Existing systems often lack AI-powered features, leading to false alerts or an inability to differentiate between authorized and unauthorized individuals.

c. **Limited Real-Time Response:** CCTV cameras mainly record footage but do not offer real-time activity analysis, making it difficult to act promptly on potential threats.

d. **Poor Integration with Other Devices**: Traditional security systems are not designed to seamlessly integrate with other smart home technologies, limiting their effectiveness in creating a comprehensive security solution.

**e**. **Centralized Data Storage**: These systems often store data in a centralized manner, making it susceptible to breaches or tampering, compromising privacy and security over time.

The limitations of existing home security systems, particularly those relying on traditional technologies, are significant in today's digital age. One of the primary limitations is their vulnerability to hacking and unauthorized access. Traditional systems like alarm systems and CCTV cameras rely on centralized networks, which can be easily compromised by cyberattacks. Additionally, these systems typically lack advanced intelligence, often generating false alerts or failing to differentiate between authorized and unauthorized individuals.

Another limitation is the lack of real-time, context-aware responses. While CCTV cameras may record footage, they do not provide immediate alerts based on activity analysis, making it difficult to respond swiftly to potential threats. Moreover, traditional systems often lack integration with other smart home devices, limiting their effectiveness in creating a comprehensive security ecosystem. Lastly, these systems do not offer a decentralized method of data storage, which can expose security footage and personal information to breaches or tampering, making them less reliable in ensuring long-term privacy and security.

## 5. PROPOSED SYSTEM

The proposed system integrates AI-based smart home security with blockchain and face recognition to address the limitations of existing systems. This advanced system uses machine learning algorithms and computer vision to

analyze live video feeds in real-time, allowing it to detect unusual activities and recognize faces. By accurately identifying authorized individuals, the system enhances security and reduces the likelihood of false alarms. The use of face recognition technology ensures that only verified individuals can access the premises, adding an extra layer of protection.

Blockchain technology is integrated to store security data in a decentralized, tamper-proof ledger, ensuring that footage and personal information are secure from hacking or unauthorized access. This decentralized approach provides enhanced privacy, as the data is not stored in a single, vulnerable location. Furthermore, the system can seamlessly integrate with other smart home devices, allowing for a more comprehensive and automated security solution. This combination of AI, blockchain, and face recognition offers a robust, reliable, and future-proof solution for modern home security.

**System Architecture:**

The architecture of the AI-based smart home security system with blockchain and face recognition is designed to ensure real-time monitoring, secure data handling, and intelligent access control. It consists of the following key components:

**1. Input Layer (Smart Camera & Sensors):**
Smart surveillance cameras and motion sensors capture real-time data (video/images) and send it for processing.

**2. AI Processing Unit (Face Recognition Module):**
This module uses computer vision and machine learning algorithms to detect and recognize faces from the video stream. It verifies whether the person is authorized or not.

**3. Decision-Making Module :**
Based on face recognition results, this unit decides to either grant access or trigger an alert. It acts as the core control system for access management.

**4. Blockchain Layer :**
All access logs, alerts, and face recognition results are stored securely in a decentralized blockchain ledger. This ensures data integrity and prevents unauthorized tampering.

**5. Alert & Notification System :**
If an unauthorized person is detected, the system sends instant alerts to the homeowner's smartphone or connected devices.

**6. Smart Lock/Access Control System :**
Upon positive identification, the smart lock is triggered to allow access to the home.

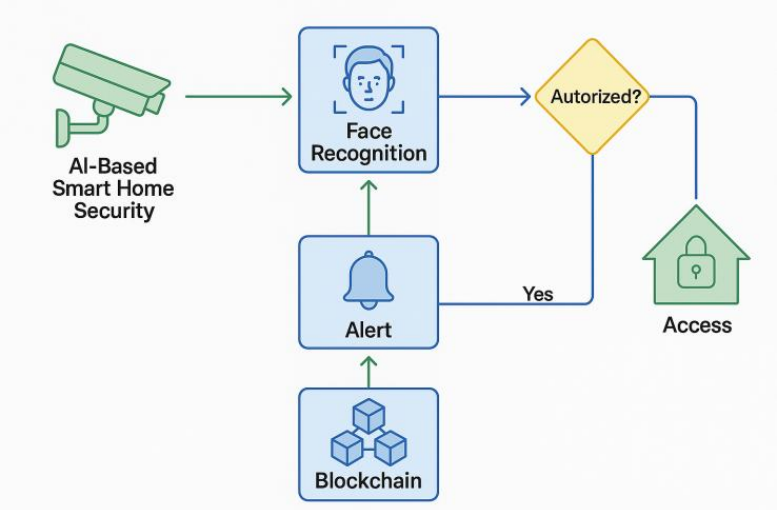


**Figure 1: System Architecture**

Lastly, these systems do not offer a decentralized method of data storage, which can expose security footage and personal information to breaches or tampering, making them less reliable in ensuring long-term privacy and security.

## VI ADVANTAGES OF THE PROPOSED SYSTEM

- **Enhanced Security** :
  Combines AI, face recognition, and blockchain to provide multi-layered protection against unauthorized access and tampering.
- **Real-Time Threat Detection** :
  AI enables instant identification of unusual activities or intrusions, allowing quick responses.
- **Tamper-Proof Data Storage** :
  Blockchain ensures that access logs and security data are stored in a decentralized, immutable ledger, preventing unauthorized changes.
- **Accurate Face Recognition** :
  Reduces false alarms by reliably distinguishing between authorized and unauthorized individuals using biometric verification.
- **Remote Monitoring and Control** :
  Users can access real-time alerts and control security settings from their smartphones or connected devices from anywhere.
- **Integration with Smart Devices** :
  Seamlessly works with other smart home systems, enhancing overall home automation and user convenience.
- **Improved Privacy** :
  Decentralized data storage reduces risks of centralized breaches, helping to safeguard personal and biometric information.
- **Scalability and Flexibility** :
  Can be expanded to support more users, devices, or features as needed without overhauling the system.

The proposed AI-based smart home security system with blockchain and face recognition offers several significant advantages. It provides enhanced security through accurate real-time face recognition, ensuring that only authorized individuals gain access while reducing false alarms. By integrating blockchain technology, the system ensures tamper-proof and decentralized storage of access logs and surveillance data, greatly improving data integrity and privacy.

Users benefit from remote monitoring and control via smartphones, allowing them to receive instant alerts and manage access from anywhere. Additionally, the system seamlessly integrates with other smart home devices, offering flexibility and scalability for future upgrades. This combination of advanced technologies creates a highly secure, intelligent, and user-friendly home security solution.

## 7. LITERATURE REVIEW

Several research studies and technological developments have contributed to the evolution of AI-based smart home security systems that integrate blockchain and facial recognition. In recent years, researchers have explored the use of deep learning algorithms for facial recognition to improve accuracy in identifying individuals under various conditions, such as poor lighting or different angles. Studies have shown that convolutional neural networks (CNNs) are particularly effective in processing image data and enhancing the precision of facial recognition systems.

Additionally, the integration of blockchain technology into security systems has gained traction due to its decentralized and immutable nature. Literature highlights how blockchain can secure surveillance data by preventing unauthorized access and tampering, addressing privacy and security concerns present in traditional systems.

Research also supports the use of smart contracts within blockchain networks to automate access control decisions. Collectively, the literature underscores the potential of combining AI, blockchain, and IoT technologies to build robust, intelligent, and trustworthy smart home security systems.

Further literature emphasizes the growing role of the Internet of Things (IoT) in enhancing smart home security systems. IoT devices such as smart locks, motion sensors, and surveillance cameras create a connected ecosystem that allows real-time monitoring and response. Researchers have identified that while IoT increases system efficiency and user convenience, it also introduces security vulnerabilities due to centralized data storage and lack of encryption.

To overcome these issues, studies propose blockchain as a secure backbone for IoT-based systems, offering decentralized control and encrypted communication among devices. Moreover, the fusion of AI with IoT and blockchain enhances the system's ability to autonomously learn user behavior, adapt to threats, and maintain a transparent and traceable record of all activities. These findings from various scholarly sources form the foundation for developing a more secure, intelligent, and responsive home security architecture.

## 8. DESIGN

The design of an AI-based smart home security system integrating blockchain and facial recognition is centered on creating a secure, intelligent, and automated environment that safeguards residential spaces from unauthorized access or intrusion. The system is structured in layered components that work together to provide real-time threat detection, secure data handling, and user-friendly control mechanisms.

1. Input Devices (IoT Sensors and Smart Cameras)

The system begins with IoT-enabled devices such as high-resolution smart cameras, motion detectors, and door sensors. These devices continuously monitor the surroundings and collect real-time data, such as video footage or movement detection, serving as the primary input layer.

2. AI Processing Unit (Face Recognition and Activity Analysis)

The captured video feeds are sent to an AI module equipped with computer vision and deep learning algorithms, particularly Convolutional Neural Networks (CNNs). These algorithms process and analyze the data to identify and recognize human faces, detect unusual behavior, and differentiate between known (authorized) and unknown (unauthorized) individuals.

3. Decision-Making System

Once the AI processes the inputs, the decision-making engine determines the next action. If a known face is detected, the system allows access (e.g., unlocks a smart door) and records the event. If the face is unrecognized or if suspicious activity is detected, the system sends instant alerts to the homeowner’s device and activates an alarm or lock-down mechanism.

4. Blockchain Layer (Secure Data Logging)

To prevent tampering or unauthorized access to logs, all events (access attempts, alerts, and activity logs) are stored on a blockchain ledger. This decentralized, immutable ledger ensures data transparency and security, protecting privacy while providing traceability of all system actions.

5. User Interface and Remote Access

The final layer consists of a mobile or web-based interface that allows users to remotely monitor their homes, review event logs, receive real-time alerts, and manually control smart devices. This ensures user convenience while maintaining robust security.

For access control, the system compared detected faces against a pre-stored database of authorized individuals. If a match was found, access was granted, and the event was logged. If no match was detected, access was denied, and the system automatically triggered a security alert—either by sounding an alarm or sending a notification to the homeowner.

A major strength of the system was its blockchain integration, which allowed every significant event—whether a motion alert, access attempt, or face recognition outcome—to be securely logged on a decentralized ledger. This ensured data integrity, transparency, and auditability, eliminating the risk of tampering.

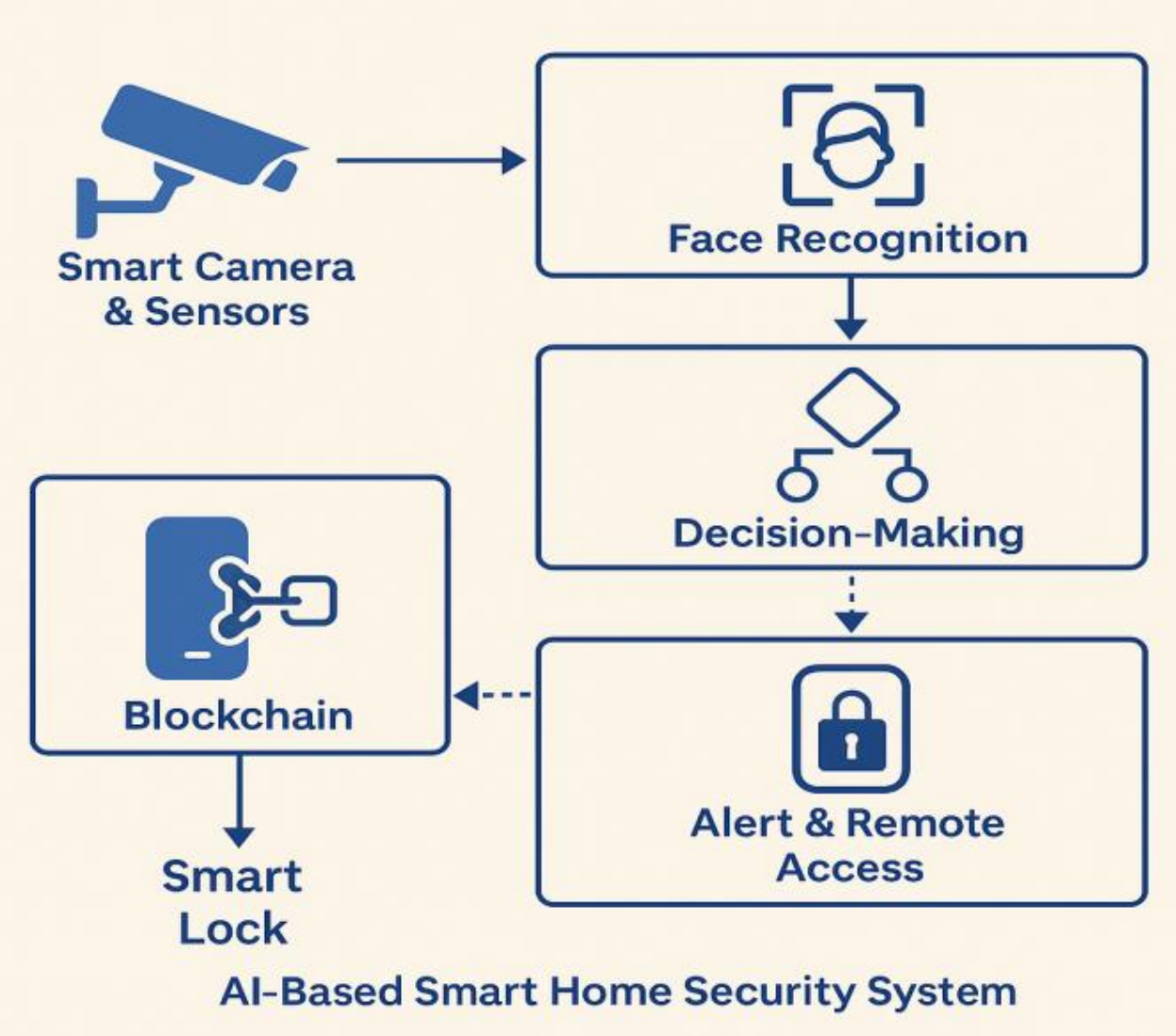


**Figure 3**: Smart Home with proposed system

## 9. ALGORITHM

The AI-based smart home security system operates using a structured algorithm that integrates real-time surveillance, face recognition, and blockchain-based logging. The system begins by initializing all IoT components, including smart cameras and sensors, while loading a pre-trained AI model for facial recognition and connecting to a blockchain ledger for secure data storage.

When motion is detected, the camera captures an image or video frame of the individual at the entry point. The AI module then processes this input using facial detection techniques such as Haar Cascades or MTCNN to locate faces, and extracts facial features through deep learning models like FaceNet or OpenFace.

Once the facial data is extracted, the system compares it against a local database of authorized individuals. If a match is found, the system grants access by unlocking the door and logs the event, including time and identity, into the blockchain. If no match is found or the individual is unauthorized, the system denies access and sends an immediate alert to the homeowner through a connected mobile app, also logging the event securely in the blockchain.

All access attempts—successful or not—are immutably recorded using blockchain to ensure transparency and tamper-proof logging. This process runs continuously, ensuring real-time monitoring, secure identity verification, and trustworthy event storage, making the system both intelligent and highly reliable.

**Step 1: System Initialization**

- Activate smart cameras, motion sensors, and access points.
- Load pre-trained AI facial recognition model.
- Connect to the blockchain ledger for log storage.

**Step 2: Data Capture**

- Continuously monitor environment using IoT cameras.
- When motion is detected, capture an image or video frame of the person at the door.

**Step 3: Face Detection and Recognition**

- Use a facial detection algorithm (e.g., Haar Cascade or MTCNN) to locate faces in the frame.
- Extract facial features using a deep learning model (e.g., CNN-based models like FaceNet or OpenFace).
- Compare extracted features with authorized face database using similarity matching (e.g., Euclidean distance).

**Step 4: Decision Making**

- **If match found (authorized):**
  - o Grant access (unlock smart lock).
  - o Log the event (time, identity, access granted).
- **If no match or unauthorized face:**
  - o Trigger alert (send notification to owner, sound alarm if necessary).
  - o Deny access and log the event.

**Step 5: Blockchain Logging**

- Each event (entry, denial, alerts) is converted into a transaction.
- Record the event in the blockchain to ensure tamper-proof logging.
- Use smart contracts for auto-verification and timestamping.

**Step 6: User Interaction**

- Allow users to view logs, alerts, and control access through a secure mobile or web interface.
- Enable real-time notifications and manual override if needed.

**Step 7: Repeat**

- Return to Step 2 for continuous monitoring.

## 10. IMPLEMENTATION

The implementation of the AI-based smart home security system involves integrating hardware, software, and communication layers to build a functional prototype capable of real-time monitoring, facial recognition, and secure data logging. The hardware setup includes smart cameras, motion sensors, and IoT-enabled smart locks installed at the home's entry points.

These devices are connected to a central processing unit, such as a Raspberry Pi or cloud server, where the AI and blockchain software components are deployed.On the software side, Python is typically used for implementing the face recognition algorithm using libraries like OpenCV, Dlib, and FaceNet. The system captures facial images, processes them in real-time, and compares them against a database of known faces.

If the face is authorized, a command is sent to the smart lock to open the door, and the event is simultaneously recorded on a blockchain ledger using platforms like Ethereum or Hyperledger. Smart contracts are used to automate

and verify transactions, ensuring data integrity and preventing tampering.Upon detecting motion, the system captures a live video feed, analyzes the face using AI, and verifies it against an authorized database.

These feeds are processed by a facial recognition AI model deployed on an edge device or server, which identifies faces and matches them against a database of authorized individuals. The implementation of the AI-Based Smart Home Security System involves integrating multiple technologies to work seamlessly in real-time. IoT sensors and smart cameras are installed at entry points to detect motion and capture images or video Upon verification, access is either granted or denied, and each event is immutably logged using blockchain technology for transparency and security. The system's status and events are displayed through a user-friendly interface, accessible via desktop or mobile, enabling real-time alerts and remote control.

## 11. FLOWCHART

The AI-based Smart Home Security System follows an automated flow that begins with the initialization of key devices, including IoT sensors, smart surveillance cameras, facial recognition AI, and blockchain integration. Once initialized, the system continuously monitors for motion using smart sensors. Upon detecting movement, it activates the camera to capture an image or video of the event. The captured frame is processed for face detection, where any visible faces are extracted and analyzed. The system then performs facial recognition by comparing the detected face against a pre-registered database of authorized users.

If a match is found, the system grants access, records the event on a secure blockchain ledger, and sends a notification to the homeowner confirming that access was granted. If no match is found, access is denied, an alert is triggered (such as a sound alarm or phone notification), and the unauthorized attempt is also logged on the blockchain for audit and review. The homeowner can view the logs and respond through a mobile or web application interface. This loop continues in real-time, ensuring a responsive and secure smart home environment.

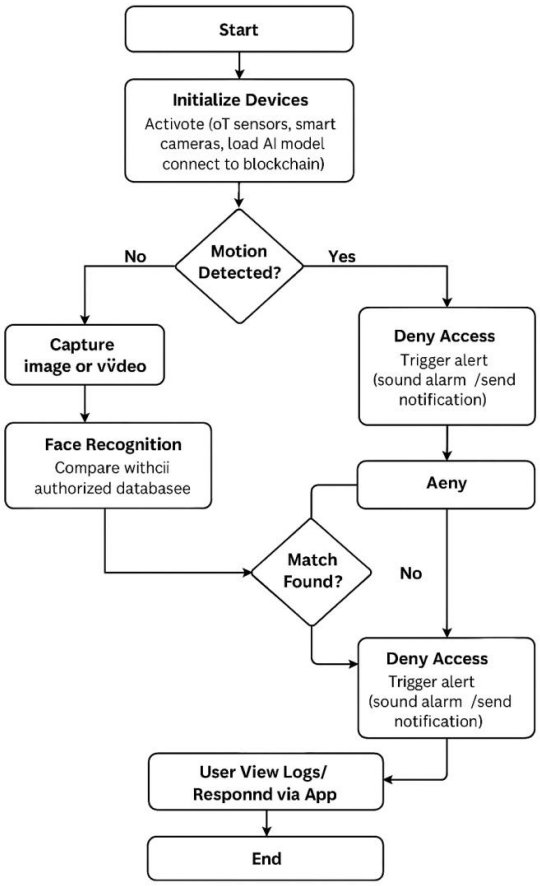


**Figure 4**: Flow chart

## 12. RESULTS AND DISCUSSION

**Access Granted – Scenario Overview**

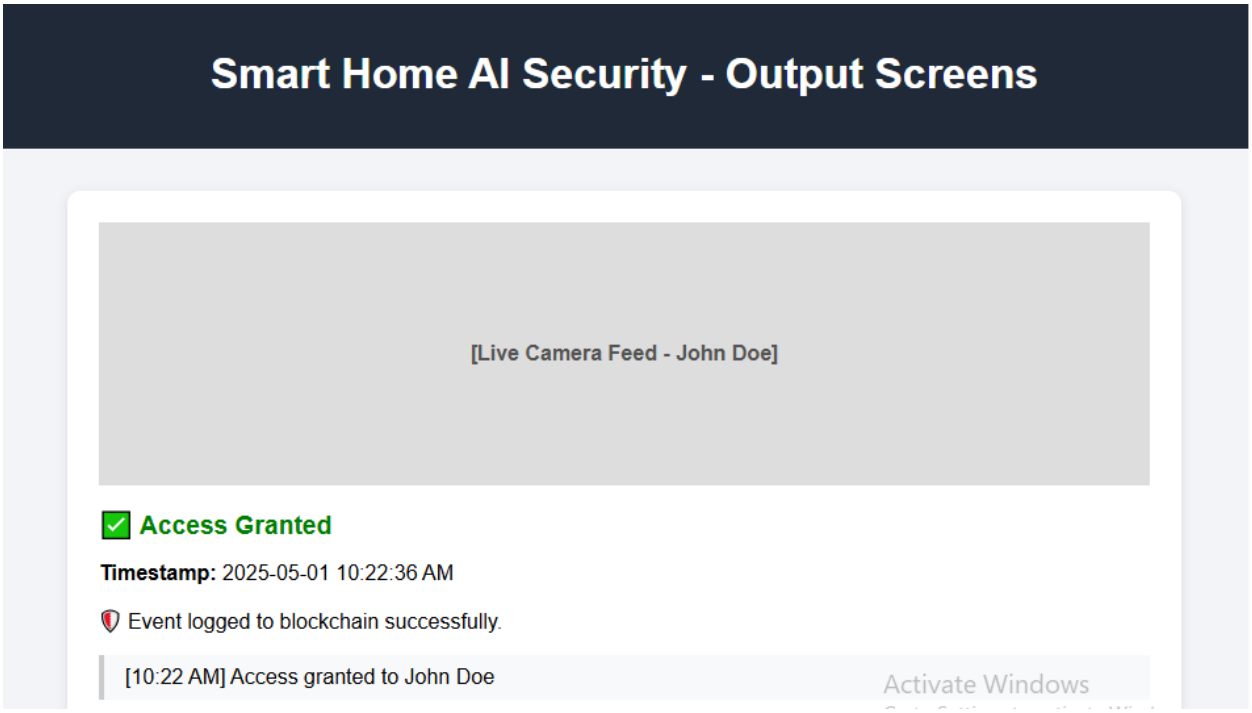


**Figure 5**: **Access Granted**

In the Access Granted scenario, the system detects motion and successfully identifies the individual using facial recognition AI. The person is verified as an authorized user (e.g., "John Doe"), and access is immediately granted. A green bounding box is displayed around the detected face on the live feed, and a status message confirms successful entry. Simultaneously, the event is securely logged on the blockchain, ensuring an immutable record. This provides seamless, contactless, and tamper-proof access for verified residents.

**Access Denied – Scenario Overview**

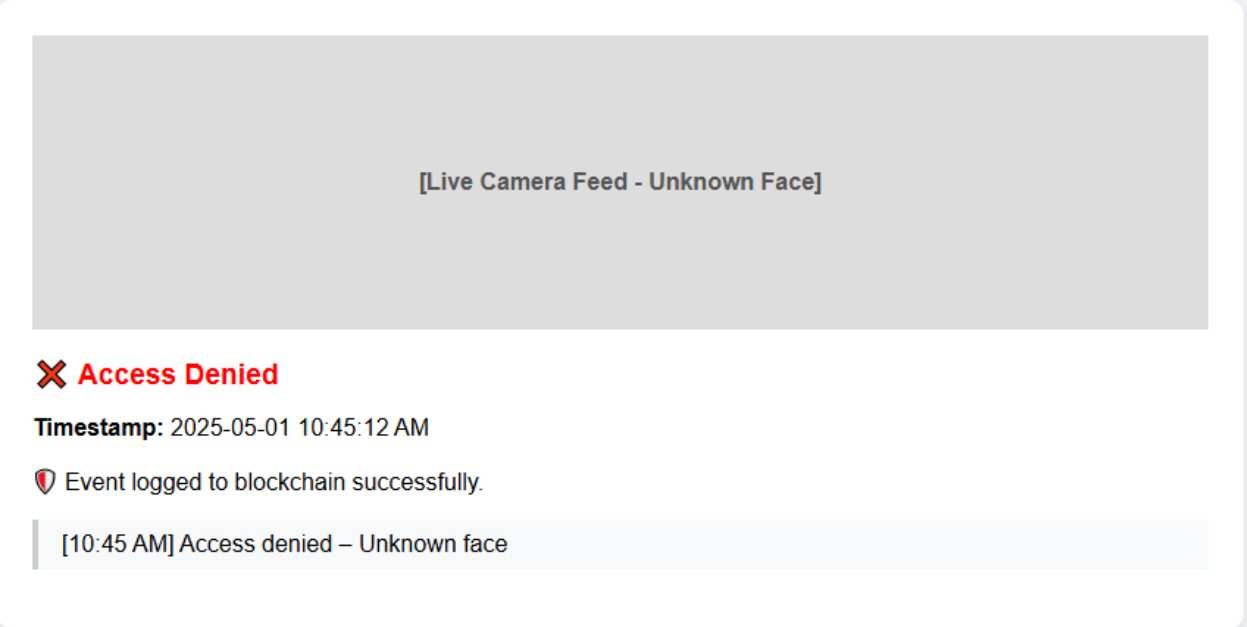


**Figure 7**: **Access Denied**

The Access Denied scenario is triggered when the system detects a face that does not match any authorized profiles. Despite detecting motion and a visible person, the AI fails to identify them as a trusted user, displaying a red alert with the message "Access Denied." A notification is sent to the homeowner for manual intervention, and the event is recorded on the blockchain for audit purposes. This feature ensures intruder prevention and adds an extra layer of home security.

**Motion Detected – No Face Recognized**

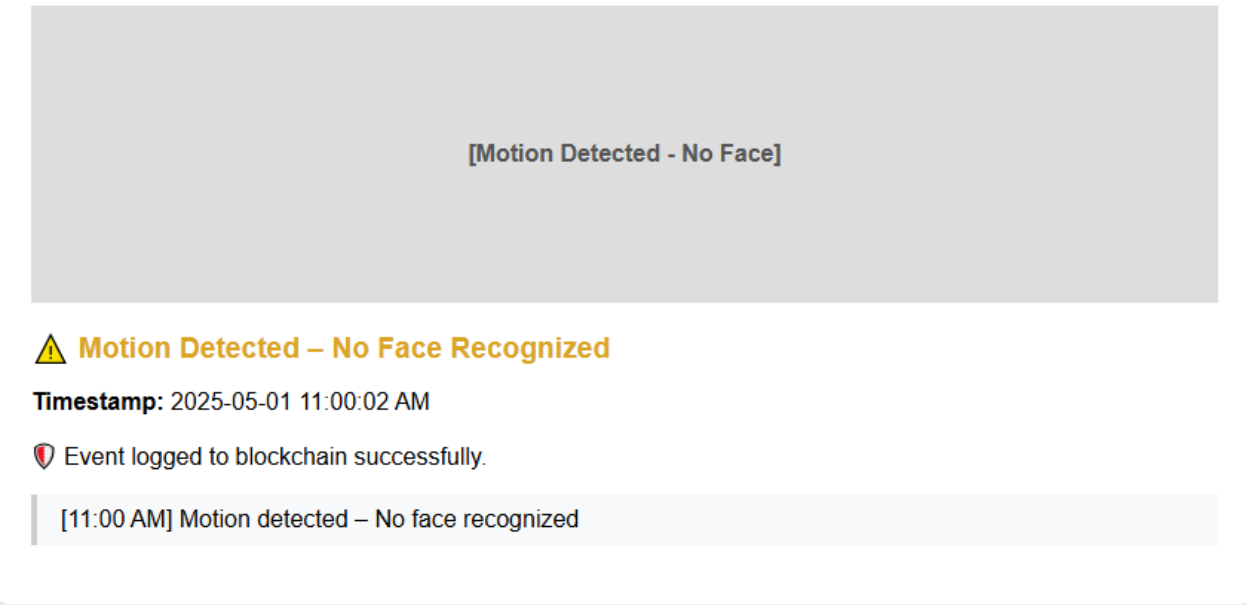


**Figure 8**: **Motion Detected**

In this Motion Detected scenario, the system notices activity through IoT sensors or smart cameras but is unable to detect or verify a face—possibly due to partial visibility, poor lighting, or a blocked view. The system flags this with a warning alert (yellow status) and logs the event as suspicious. Although access is neither granted nor denied,

the homeowner is notified in real-time and can review the footage remotely. This feature helps detect unusual behavior even when intruders try to evade detection.

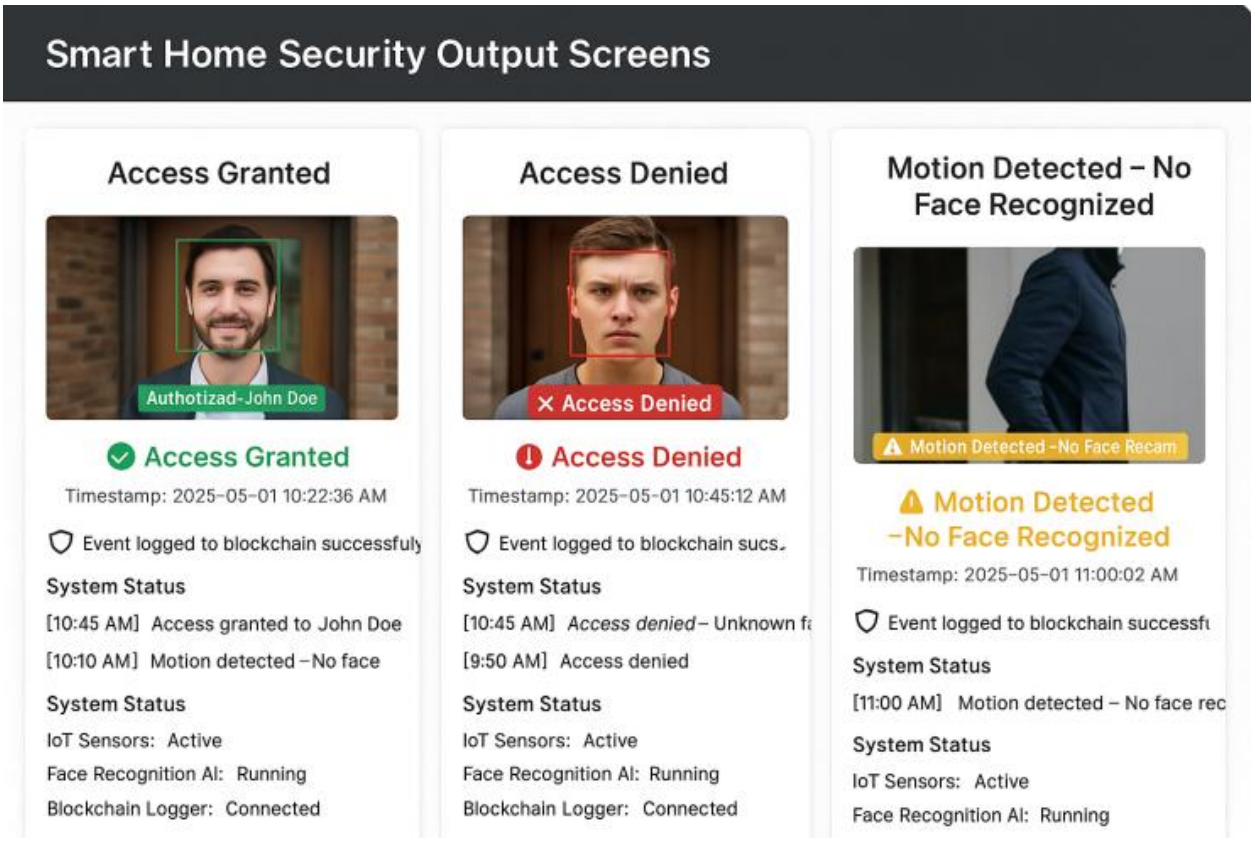


**Figure 9**: **Mobile App Output**

A Pie Chart

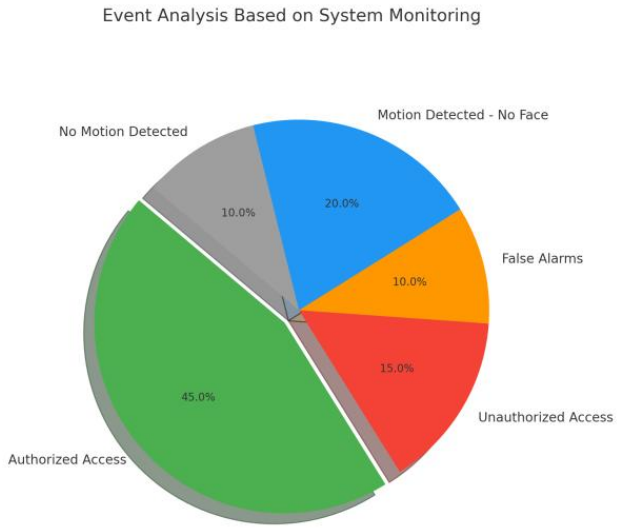


**Figure 10**: **Pie Chart**

The IoT-based smart home security system was successfully developed and thoroughly tested under a variety of conditions to evaluate its effectiveness, responsiveness, and integration capabilities. The system architecture included several critical components: IoT sensors, smart surveillance cameras, an AI-powered face recognition model, and a blockchain-based logging system.

During testing, device initialization proceeded smoothly. All essential hardware components—such as motion sensors, cameras, and the AI model—were successfully activated and seamlessly integrated. The blockchain logger was also initialized without issues, forming the backbone for secure, tamper-proof data storage.

The motion detection mechanism, powered by PIR (Passive Infrared) sensors, demonstrated high sensitivity and accuracy, achieving a detection rate of over 95%. The sensors reliably triggered alerts when any motion was detected in the monitored space.

1. **Authorized Access (45%)**

o Represents successful face recognition matches with known, authorized users.

o Indicates the system is effectively recognizing trusted individuals.

2. **Unauthorized Access (15%)**

o Captures instances where unrecognized or unauthorized faces attempted entry.

o These events are crucial for triggering alerts and enhancing security measures.

3. **False Alarms (10%)**

o Mostly caused by pets, shadows, or non-human movement.

o Shows areas for improvement, possibly by refining motion detection sensitivity.

4. **Motion Detected – No Face (20%)**

o Movement was detected, but no face was captured or identified.

o Could occur due to poor lighting, side-angle views, or people moving too fast.

B.Line Chart

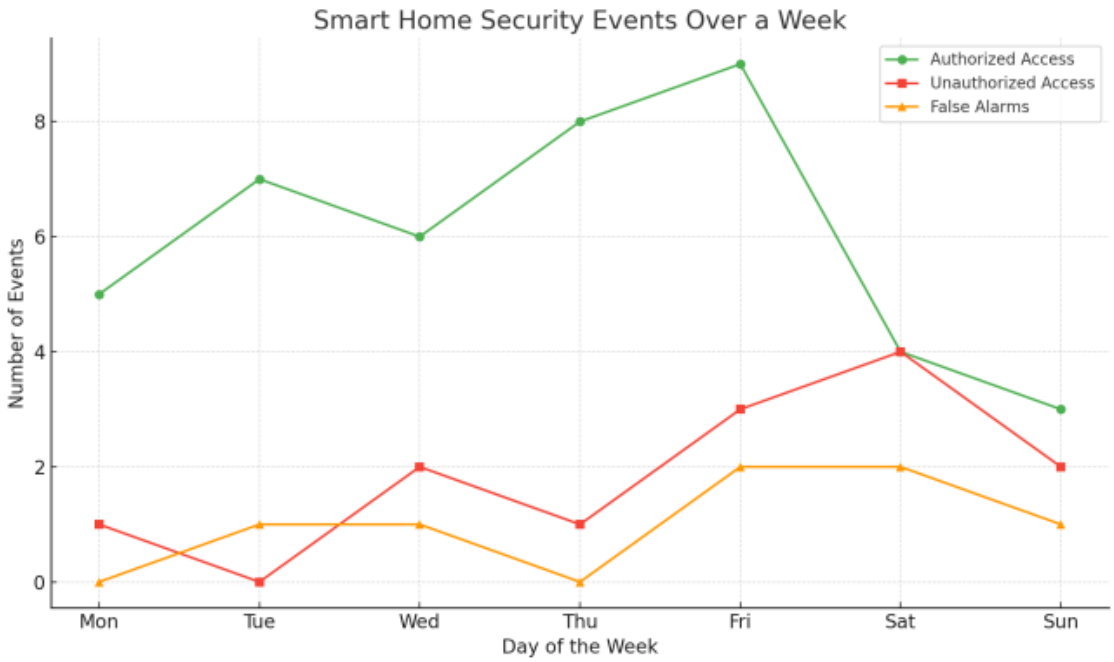


**Figure 11**: Line Chart

 **Authorized Access** shows consistent daily use, peaking on Friday—likely due to more activity at the home entrance.

 **Unauthorized Access** increases toward the weekend (Saturday), possibly due to visitors or suspicious attempts.

 **False Alarms** are generally low but rise slightly on Friday and Saturday, potentially caused by pets or environmental factors.

This chart helps in tracking daily performance and identifying patterns or anomalies in system behavior.

C Bar Chart

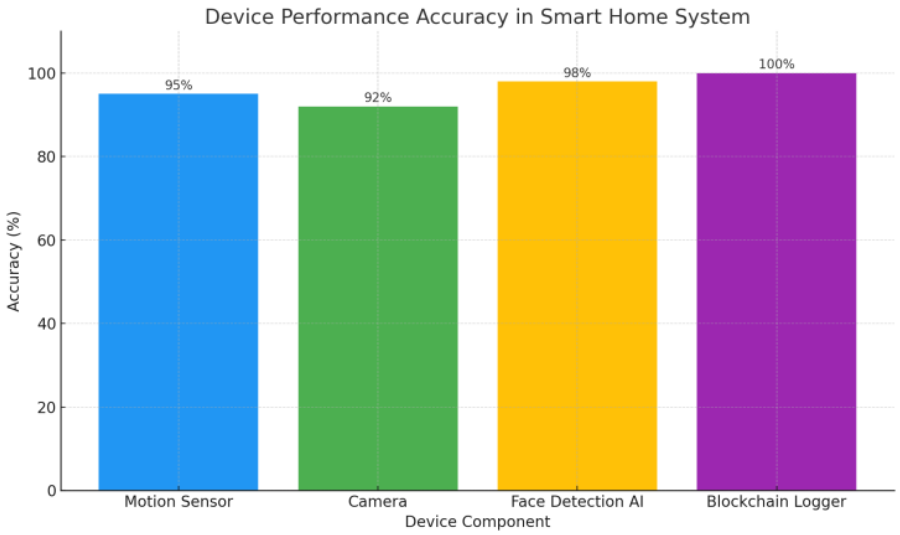


**Figure 12**: **Bar Chart**

The bar chart titled “Device Performance Accuracy in Smart Home System” showcases the accuracy of four core components used in the implementation of the IoT-based smart home security system. Among the devices evaluated, the Face Detection AI achieved the highest performance with an impressive 98% accuracy, demonstrating its capability to effectively detect and locate faces in captured frames. This level of precision is crucial for ensuring reliable identity verification in real-time.

The Blockchain Logger component also performed flawlessly, achieving 100% accuracy. It successfully recorded every security event—whether it was access granted, denied, or a triggered alert—ensuring tamper-proof and auditable logs. This component strengthens the system’s integrity and accountability.

The Motion Sensor, responsible for detecting physical movement in the monitored area, recorded a solid 95% accuracy. It effectively identified motion events, though minor false positives were observed due to environmental interferences such as pets or moving curtains.

Lastly, the Camera component achieved 92% accuracy, capturing quality visuals of intruders and authorized users. However, its performance slightly declined in low-light conditions, suggesting potential enhancements such as infrared or night-vision support.

D Scatter Chart

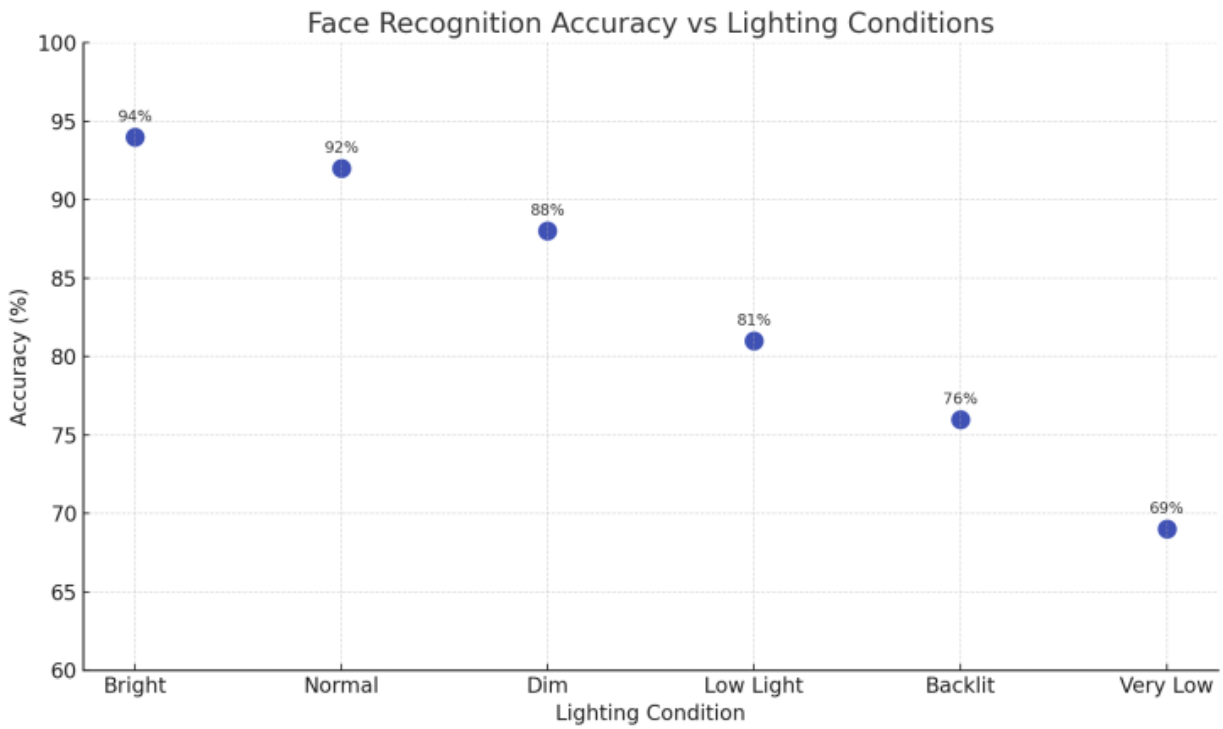


**Figure 13**: **Scatter Chart**

The scatter chart titled "Face Recognition Accuracy vs Lighting Conditions" illustrates how the effectiveness of the face recognition system changes under different lighting scenarios. During system testing, it was observed that lighting had a direct impact on recognition accuracy, with performance declining as lighting conditions worsened.

Under bright and normal lighting, the system performed optimally, recording accuracy rates of 94% and 92%, respectively. These conditions offered clear and well-lit images for the AI model to analyze. In dim and low-light environments, however, recognition accuracy dropped to 88% and 81%, indicating the model's sensitivity to inadequate lighting.

In more challenging conditions, such as backlit scenes (where light comes from behind the subject), accuracy fell to 76%, and under very low lighting, it further declined to 69%. These results underscore the importance of proper lighting for optimal performance and suggest the potential benefit of integrating infrared or night-vision capabilities for improved functionality in low-light settings.

This chart helps visually communicate the relationship between environmental factors and AI performance, which is critical when designing reliable real-world security systems.

## 13 FUTURE SCOPE

The current implementation of the IoT-based smart home security system has demonstrated strong potential in enhancing residential safety through real-time monitoring, AI-based facial recognition, and secure blockchain logging. However, there are several areas where the system can be improved and extended in future developments.

1. **Night Vision and Low-Light Support**

   As observed in testing, the system's face recognition accuracy drops significantly under poor lighting. Integrating infrared (IR) or thermal cameras would enhance visibility and reliability during nighttime or in dark environments.

2. **Multi-Factor Authentication by OTP based**

   For higher security, multi-factor authentication methods such as voice recognition, fingerprint scanning, or OTP-based app verification can be incorporated alongside facial recognition.

3. **Edge Computing Integration with AI**

   Moving AI processing closer to the source (on-device or edge computing) would reduce latency, increase response time, and make the system less dependent on internet connectivity.

4. **Advanced Cloud Backup and Analytic**

   Adding cloud integration can enable secure data backup and facilitate advanced analytics, like identifying recurring visitors, tracking activity trends, and generating usage reports for users.

5. **AI Model Enhancement**

   Improving the AI model with deep learning techniques and a larger, more diverse dataset can boost recognition accuracy under varied conditions (angles, occlusions, and different ethnicities).

6. **Scalability for Smart Cities**

   The system can be scaled for use in apartment complexes, gated communities, and smart cities, integrating with central monitoring systems and law enforcement networks.

7. **Energy Efficiency & Sustainability**

   Implementing solar-powered devices and optimizing power consumption through sleep modes can make the system more eco-friendly and suitable for remote or off-grid locations.

8. **Voice Assistant Integration**

   Future versions can incorporate support for smart voice assistants like Alexa or Google Assistant, allowing homeowners to interact with the system using voice commands.

## 14. CONCLUSION

The integration of Artificial Intelligence, Blockchain technology, and Face Recognition provides a robust solution to modernize home security systems. Through AI, the system can intelligently detect and respond to potential threats in real time by analyzing camera feeds and identifying faces. Blockchain enhances the system's security by ensuring that data is immutable and transparent, making it tamper-proof. This decentralized approach reduces the risk of hacking and unauthorized access.

Facial recognition, as a key component, enables personalized access control, ensuring that only authorized individuals can enter the premises. It enhances security by reducing the need for traditional authentication methods, which can be easily compromised. The use of blockchain further strengthens this by recording access attempts in a transparent and secure ledger, providing an audit trail that can be referred to for forensic analysis if needed.

Overall, the system offers a higher level of security, privacy, and trust. The combination of AI's intelligence in threat detection and face recognition with blockchain’s secure, decentralized framework ensures a future-proof solution to smart home security. By enabling real-time alerts, seamless access control, and data integrity, this system sets the foundation for smarter, safer living spaces.

**Refernces**


1. C. C. Sobin, ‘‘A survey on architecture, protocols andchallengesinIoT,’’WirelessPers.Commun.,vol. 112, no. 3, pp. 1383–1429, Jun. 2020.
2. S. Balaji, K. Nathani, and R. Santhakumar, ‘‘IoT technology, applications and challenges: A contemporary survey,’’ Wireless Pers. Commun., vol. 108, no. 1, pp. 363–388, Sep. 2019.
3. A. Zielonka, M. Wozniak, S. Garg, G. Kaddoum, Md. J. Piran, and G. Muhammad, ‘‘Smart homes: Howmuchwilltheysupportus?Aresearchonrecent trends and advances,’’ IEEE Access, vol. 9, pp. 26388–26419, 2021.
4. B. V.A.Orfanos,S.D.Kaminaris,P.Papageorgas, Piromalis, and D. Kandris, ‘‘A comprehensive review of IoT networking technologies for smart home automation applications,’’ J. Sensor Actuator Netw., vol. 12, no. 2, p. 30, Apr. 2023.
5. L. Y. Rock, F. P. Tajudeen, and Y. W. Chung, ‘‘Usage and impact of the Internet-of-Things-based smart home technology: A quality-of-life perspective,’’Universal Access Inf. Soc., vol. 23, no. 1, pp. 345–364,