Smart Home Security with Facial Recognition and Motion Detection Using Internet of Things (IoT)

Ayushi Pandey
Student
LPCPS, Lucknow
ayushipandey26feb@gmail.com

Dr. Aarti Rani
Assistant Professor
LPCPS, Lucknow
aarti.singh18oct@gmail.com
ORCID: 0000-0002-8081-6821

Abstract-**Modern and reliable security solutions are desperately needed, as urban theft problems continue to rise. This study presents a Facial recognition-based smart home safety system and motion detection. Its goal is to increase urban safety by providing real-time monitoring and alerting capabilities. Existing security protocols are vulnerable to hackers and have various weaknesses. The suggested remedy for the security problem is based on facial recognition and detection and is grounded on the Internet of Things (IoT). The lens of the camera captures the face of a person. and compared to the database that was obtained. Anyone who isn't enumerated may be contracted admission to the through a mobile application by someone with permission on the premises. A photo of the person's face will be collected and sent to the relevant authorities via email if they enter without authorization or knowledge. If someone tries to enter without permission, an alarm will go off. Theft is still a major problem that causes both financial and emotional hardship, even with the implementation of numerous security measures. The concept of technology adding value to our everyday lives is combined with IoT. The idea of security and privacy is one important area where technology helps us. This article provides an overview of smart home security systems that employ face recognition and the Internet of Things to effectively and affordably secure our homes.**

Keywords- Smart Home Security, Facial Recognition, Motion Detection, Internet of Things, Biometrics, Face Detection, Face Recognition Algorithms, Real-Time Surveillance, Liveness Detection, Home Automation.

1. INTRODUCTION

For any household, crimes like theft and burglary are major worries. Installing smart home security systems that are accomplished by a solitary gadget can help individuals stop worrying all the time, especially at night. For security purposes, most people have cameras installed at each entry to their homes, allowing them to see who is coming in. Advanced home security systems may also recognise faces. Low-level visual features and geometrical feature points can be used to perform facial identification (Klobas et al., 2019). However, thieves can circumvent this by displaying the owner's or a household member's image.

A home security system that uses both speech recognition and face authentication is the subject of the invention. Using a live stream, this will authenticate each visitor to the residence twice and verify the information entered using the proprietor's database names. The inclusion of speech recognition ensures that users cannot simply access by displaying a photo of one of the identified members; rather, they must utter a specific passphrase that will be processed by the speech recognition system twice to verify their identity (Arif et al., 2020). Notifying the owner's device will make it simple for the current members to be verified and granted entry to the house. An alert will be issued to the owner with their photo if an anonymous being is found at any of the entrances. The user can give someone a one-time entry without adding them to the database, which would not grant them lifetime access, or they can add the individual to their database with a single click.

People have been required to wear masks whenever they gather since the start of the COVID-19 epidemic. Facial recognition algorithms had a hard time identifying the person wearing the mask. The study includes an examination of how the facial recognition system can identify an individual even while they are wearing a mask. The paper covers a range of facial recognition techniques that can be used with little attribute removal, with a particular highlighting on

facial recognition throughout the eye region. This study will be useful not just during COVID-19 but also in the event of a robber or burglar wearing a cover. Authorities can use the recognition system to find a criminal.

Being in their own homes will make the companions feel safer and become more tech-savvy with an efficient home safety system. This concept can be expanded to include a security system for establishments that need security, such as malls and banks [1].

2. OVERVIEW OF SMART HOME SECURITY

A smart home is furnished with internet connected gadgets that permit remote control of the appliances, environment controls, safety measures, and other aspects of the house from a mobile device. They can be configured with wireless or hardwired systems. Consumers now have easy access to a wide range of internet-connected home goods, including pet cams, smart thermostats, smart locks, smart entertainment speakers, outdoor security cameras, and video doorbells.

All of the gadgets within a Smart home can be accessed from a specific area and are connected together, such as a laptop, tablet, game console, or cell phone. Single home automation systems can be used to operate doors, TVs, thermostats, cameras, lighting, house monitors, and appliances like refrigerators. Users of the remote-control system can schedule tasks, activate devices, and keep an eye on outcomes from any location. Appliances in smart homes are capable of self-learning. They are capable to become familiar with the homeowner's schedule and settle in accordingly. When users utilize features that allow them to slightly regulate the temperature and lighting in their homes, they save energy.

When the homeowner is not at home, convinced home computerization systems alert them if they sense any gesture. If they see any risky conditions, others can notify the forces or fire service. A system of physical objects that can pleat and transfer microelectronic data is known as the internet of things. Once associated, services like smart doorbells, smart appliances, and smart security systems are integrated into this technology [2].

3. FACIAL RECOGNITION TECHNOLOGY

A biometric technique baptized facial recognition uses a person's facial features to identify them.. People capture face images, which are then processed automatically by the recognition equipment. The document introduces related research on face recognition from numerous angles. The study discusses the stages of facial recognition development as well as the technology involved. We introduce real-world facial recognition research, as well as generic evaluation standards and databases. We present an innovative idea of facial recognition. Face recognition has emerged as the next improvement trend, with numerous possible applications.

Visual model recognition includes facial recognition as a sub problem. Beings always use their eyes to understand visual information and classify patterns in images. The intellect acknowledges these facts as noteworthy concepts. A computer's image or video is a multi-pixel media. The gadget should classify the concept that a convinced data point signifies. This is a fundamental organization matter in the gratitude of visual models. In the portion of the data that all apparatus interprets as the face, face recognition involves recognizing the person to whom the face belongs. This is a problem with the subdivision.

In its broadest sense, facial recognition mentions to the technologies that are employed to develop a facial recognition system. It comprises preprocessing images, face detection, face positioning, and exclusivity recognition, among other things. All of the faces in a single image are recognized by the face detection approach. Here, the whole image is scanned to determine whether the chosen area represents a face. The face direct system may produce output in a variety of shapes, including squares and rectangles. In the face detection coordinate system, the face point is the organized location of the facial feature. Actual positioning technologies that are now in use are fundamentally integrated into the deep learning framework. Algorithms for face positioning require a lot less calculation time than those for face identification [3].

4. UNDERSTANDING MOTION DETECTION SYSTEMS

Motion sensors have revolutionized several industries and better-quality our ease and safety, making them an indispensable part of our daily lives. These gadgets, which sense movement and interpret it into valuable information, enable automation, energy proficiency, and welfare valuations. The advances in motion sensor technology, their essential concepts, and their many applications in a diversity of trades, including home automation and healthcare, are covered in this article. Motion sensors are electronic devices that recognize changes in the activity or spot of their

environment. They use an assortment of technologies, including optical, microwave, ultrasonic, and infrared. Infrared motion sensors can detect variations in heat patterns, whereas ultrasonic sensors use sound waves to gauge movement and distance. To sense movement, microwave sensors lead out microwave pulses and monitor the signals they receive. Optical sensors employ light to detect motion by bouncing a light beam [4].

By providing intelligent and automated systems that adapt to human presence and movement, motion sensor sensors have transformed a number of industries and applications. These gadgets leverage a variety of different technologies to identify and evaluate motion, producing useful information for a variety of uses, including automation, entertainment, security, and healthcare. This study attempts to investigate the technology, applications, and difficulties of motion sensor devices in order to highlight their significance and possible future advancements. In today's world, motion sensor technology is vital since it changes how we interact with our environment. These gadgets enable a diversity of tasks, such as recording physical motion in fitness programs or turning on lights when someone arrives at a room, by sensing and interpreting motion.

4.1 Types 0f Motion Detection

The marketplace is occupied with numerous categories of motion sensors. PIR, ultrasonic, microwave, tomographic, and shared types are scarce of them.

i. Passive Infrared Sensor

All animals with heated blood emit infrared radiation. A small layer of pyro electric film is used in passive infrared sensors, which react to infrared light by producing electricity. When this electrical surge occurs, this sensor will sound the housebreaker alarm. These sensors are long-lasting, reasonable, and energy efficient. Alarm systems for indoor spaces normally use these sensors.

ii. Ultrasonic Sensor

There are two types of ultrasonic sensors: active and passive. The latter are designed to detect certain sounds, such as glass breaking or metal hitting metal. Notwithstanding their high sensitivity, these sensors are often overpriced and prone to false alarms. Vigorous ones generate sound waves, or ultrasonic wave bursts, and then measure how well they bounce off moving objects. Since these sound waves are audible to animals like cats, dogs, and fish, an active ultrasonic alarm could frighten them.

iii. Microwave Sensor

These sensors generate pulses of microwaves and then measure how many of them reflect off of things to determine whether or not they are moving. Despite their high sensitivity, microwave sensors can occasionally detect moving items outside of their target range by detecting non-metallic objects. Because of its high power consumption, these sensors are frequently made to cycle ON and OFF. Knowing the cycles makes it possible to get past them. Using microwave sensors, electronic guard dogs operate.

iv. Tomographic Sensor

These sensors produce radio waves and perceive any turbulence to those waves. They are frequently positioned to generate a radio wave web that conceals wide regions and have the capability to see through buildings and objects. Due to their high cost, these sensors are typically found in storage facilities, warehouses, and other settings requiring a commercial degree of protection.

v. Collective types of Motion Sensors

To reduce false alerts, several motion detector types comprise many sensors. Though, only when both types notice motion do dual sensors become lively. For specimen, because it uses less energy, a dual microwave or PIR sensor will primarily be set to passive infrared. The microwave division will activate when the passive infrared sensor trips, and if the other sensors trip as well, the alarm will ring. This cooperative type is outstanding at disregarding false alarms, but it increases the likelihood of omitting the actual ones. [5].

4.2 Using Motion Detectors in Combination with Security Systems

The way surveillance systems work has been completely transformed by the addition of motion detectors to security cameras. They recover camera recitals in subsequent ways:

- Movement-Triggered Video Recording: Security cameras that have motion detectors installed only start recording when motion is detected, eliminating superfluous footage and saves storage space.
- Warnings & Alerts in Real Time: Users are instantaneously notified when motion is detected, allowing them to respond immediately to any threats.
- Conservation of Energy: Wireless cameras with sensors that detect motion have longer battery lives since they don't use power until movement is detected.
  Smart Integration: A lot of contemporary motion detector surveillance equipment may be seamlessly coupled with point-of-sale systems, allowing events to be coordinated.

When combined, these physiognomies increase the helpfulness of motion detecting video security systems and lessen the essential for ongoing manual monitoring. [6].

5. ADVANTAGES OF FACIAL RECOGNITION IN SECURITY

Using unique facial features, a biometric facial recognition system authenticates or identifies individuals. This technique gained prominence in the early 1990s when governmental organizations such as the Defense Advanced Research Projects Agency, and the National Institute of Standardization and technique exhibited facial recognition programs. These early efforts highlight the promise of facial recognition technology, predominantly for security and recognition. Despite being initially developed for military, government, and business applications, face recognition began gaining traction in the residential market in the 2010s. [7].

Some of the *reasons for* facial recognition is being widely integrated into several products today.

- **Enhanced Security**
  Because facial recognition accurately confirms identities, it offers a high level of security. Because face features are distinct and hard to copy, unauthorized access is more difficult than with passwords or PINs, which are easily forgotten or stolen. Additionally, passkeys for passwordless and anti-phishing authentication are frequently accessed by facial recognition. Shoulder surfing attacks, which have increased in frequency in recent years, are also reduced by using biometrics like facial recognition.

- **Convenient**
  Customers mostly appreciate facial recognition technology's convenience, even though it is safe. Verification and access procedures are streamlined by facial recognition. Without carrying physical keys or having to memorize passwords, users may quickly unlock devices, approve payments, or enter secure locations. Going back to using passwords or PINs can seem antiquated and inconvenient to someone who is used to utilizing facial recognition to access their smartphone or user account.

- **Speed**
  Wait times for activities like finishing purchases, checking in at the airport, and logging onto gadgets are shortened via quick facial recognition procedures. Because facial recognition doesn't require the user to do anything during verification, it looks natural when correctly integrated into a system. Because facial recognition doesn't require human input, more customers find it even easier than fingerprint scanning.

- **Contactless Operations Improve Hygiene**
  Contactless communication is made possible by facial recognition, which improves convenience and hygiene. For example, people can enter a protected building without coming into contact with any physical surface. This improves environmental health by lowering the chance of bacteria and viruses spreading. For diseases like COVID-19, which are primarily transmitted through touch, having identifying technologies can be essential.

- **Fraud Anticipation**
  By using distinctive facial traits for detection verification, facial recognition improves fraud prevention. Even if they are twins, it is challenging for someone to effectively impersonate another person because everyone has unique facial features. Because only the certified person can act, this system protects against unauthorized access and transactions. The risk of phishing is further reduced because facial recognition removes the need for passwords, making it impossible for hackers to obtain or utilize fictitious identities.

6. CHALLENGES & LIMITATIONS OF FACIAL RECOGNITION

Facial recognition technology has fast become essential to our daily lives, powering everything from access control systems to law enforcement investigations. However, its widespread use has also highlighted a number of technical, ethical, and cultural problems.

Challenges to Prevent Fraud and Misuse:

Privacy & Surveillance
Unauthorized mass surveillance may be made possible by facial recognition technology. It permits tracking of people without their knowledge when used in public places by corporations or government organizations, endangering civil liberties and privacy. For instance, with no oversight, the London Metropolitan Police has increased their use of live facial recognition, scanning millions of people annually in public areas.

Bias & Misidentification
Marginalized populations are more likely to be misidentified by facial recognition technologies. When utilised by law enforcement, accuracy declines for women, older folks, children, and people of colour, resulting in erroneous arrests and false positives.

Data Security & Misuse
Once saved, facial data becomes extremely sensitive since, unlike passwords, it cannot be updated. It can be used for fraud, identity theft, or illegal spying if it is compromised. The hazards of misuse are increased by inadequate oversight of facial recognition services.

Technical Limitations in Real-World Conditions
In uncontrolled conditions, accuracy frequently decreases. System reliability is decreased by low-resolution photos, stance changes, occlusions such masks or glasses, and poor illumination. Applications for law enforcement, access control, and identity verification are all compromised by this [8].

Ethical & Societal Issues
The extensive use of computerized facial recognition raises important ethical concerns about justice, transparency, and trust. Public outcry is exacerbated by unauthorized installations, and unchecked expansion could normalize monitoring and threaten fundamental liberties [8].

7. FUTURE TRENDS IN SMART HOME SECURITY

Smart home technology is totally changing how homeowners live, work, and take care of their houses. These cutting-edge innovations, which vary from enhanced security to energy efficiency, are becoming essential elements that genuinely raise the value of your home rather than only being practical extras.

According to Fortune Business Insights, the global smart home market was projected to be worth $80 billion in 2022 and is expected to reach $338 billion by 2030. This rise shows how crucial it is becoming to use smart home products to enhance the effectiveness, worth, and beauty of your home. As more and more homes embrace smart technology, customers are looking for ways to link their homes. However, there are so many alternatives available that it can be difficult to know where to start and which one best fits your needs.

As advances in technology make automation simpler, stronger, and more accessible than ever, the market for smart homes has reached a tipping point in 2025. By then, there will be 69.91 million smart homes in the US, according to Statista research. This is meant for people who wish to make their houses more convenient and efficient [9].

Below are the top smart home trends to incorporate in your home:

Universal Device Connectivity-
The promise of universal interoperability with smart homes has finally been fulfilled via the Matter protocol. This ground-breaking standard enables smooth device interoperability among hundreds of manufacturers, including Apple, Google, and Amazon. Because Matter is an open standard for smart home technologies, your gadget can be used with any ecosystem that has earned the Matter certification. Your devices will operate smoothly and dependably thanks to this open-source protocol. This implies that your Amazon Alexa security system and Apple HomeKit lights can now

speak with your Google Nest thermostat directly. You no longer have to worry about incompatibilities when selecting the best gadget from each category. Because they provide flexibility and long-term viability, homes with Matter-compatible systems are more appealing to purchasers, which may increase their sale price.

AI-Powered Predictive Home Automation-
Without requiring manual programming, sophisticated artificial intelligence home automation systems automatically adapt your home environment based on your daily activities. Artificial intelligence (AI)-powered devices analyses your behavior patterns and make wise decisions, in contrast to conventional smart homes that need a lot of setup and scheduling they can predict your needs based on weather trends and calendar activities, as well as when you usually return home and what temperature you prefer at different periods of the day. From humid summers to unpredictable winters, AI systems excel at efficiently managing heating and cooling in a range of seasonal weather conditions.

Advanced Energy Management & Solar Integration-
Energy-efficient smart home technology regulates, optimizes, and tracks energy use throughout your home with a comprehensive system that includes solar panels, battery storage, and even electric vehicle charging. Smart management systems and energy-efficient homes are becoming more and more popular among eco-conscious buyers; these homes typically sell 10–15% faster than comparable homes without these features.

Health & Wellness Monitoring Systems-
Smart homes can significantly help with comprehensive home health monitoring that tracks stress levels, sleep patterns, air quality, and overall wellness indicators across your living space. Many wearables can be connected to home systems that monitor vital signs and alert medical professionals in case of an emergency. Smart homes can also analyze air quality, allergens, and other environmental factors to ensure a healthy living space. The limits of health and wellness technologies are being pushed by innovations meant to enhance both physical and emotional well-being. The many products that are created to facilitate the simplicity of technology while also enhancing our health and well-being are ushering in a new era in domestic life.

Next Generation Home Security with Autonomous Features-
Next-generation home security features are replacing passive monitoring with autonomous and protective threat detection and response. Autonomous drones, AI-powered hazard detection, and predictive security measures are just a few examples of the artificial intelligence-powered security solutions that surpass traditional cameras and alarms. If you want to live in a safe neighborhood, these state-of-the-art home security systems provide the best protection available. Currently, many insurance companies offer 10–20% discounts to homeowners that have sophisticated smart security systems.

Voice-First Home Control for All Ages-
Today, sophisticated voice control technologies enable smart home equipment to be used by users of all ages and technical proficiency levels. Voice control has progressed beyond simple commands to mimic real-world discussions. Intricate multi-step requests, partiality memory, and context comprehension are all hoped for by modern systems. Increased accessibility, ease of use, and energy efficiency, as well as the simplicity of everyday tasks, are important benefits of voice control.

5G-Enabled Ultra-Fast Smart Home Networks-
5G-enabled networks advance device recital and open up a novel class of requests by providing a smart home with dissolute and dependable connectivity. Instantaneous communication between devices is made possible by high-speed 5G connectivity, which also creates completely new opportunities for smart home functionality. Nowadays, homeowners are in a good position to benefit from these lightning-fast smart home features as 5G connectivity spreads quickly around the Triangle. These networks are revolutionizing how we respond to our home settings and changing living places [10].

8. REAL-WORLD APPLICATIONS OF SMART HOME SECURITY

Without a doubt, home IoT devices provide unparalleled convenience. You will be astonished to learn about the essential gadgets that make a home smart:

i. **Smart Household Security-** People invest money on home security systems that are smart in order to render their homes more advanced and safer. These cutting-edge technologies give you real-time safety status updates and keyless admission to your house. You can use a phone or a pin on digital locks for unlocking your door.

ii. **Smart Locks & Alarms-**Smart locks provide remote control of the main door and improve home security. You may program a timer to let individuals in at a certain moment. For example, the eye Lock is a solution that uses iris-based verification to allow access to only authoritative persons. IoT-enabled locks can too function as intelligent housebreaker alarms.

iii. **Cameras-**With IoT, you can make use of cameras to keep an eye on your house. You may use the cameras on smartphones and tablets for free with a smart security solution from many things. These features are transformed into advanced video monitoring cameras with motion detection and live streaming by their application. When something suspicious or out of the ordinary happens, these devices use the IFTTT protocol to drive an email or text alert.

iv. **Video Door Entry Systems-** Video door entry systems allow you to handle access in your home-based using your voice and face, which can advance safety and comfort. Siri, Google Home, and Amazon Alexa are all well-matched with these video inspection devices. When mutual, they work flawlessly to allow you to completely utilize the promise of interoperability. Installing these devices allows you to monitor your home remotely and even engage with visitors via video chats.

v. **Fire/Smoke Sensors-** Installing fire or smoke sensors in your home is essential so you can be notified immediately if something goes awry. When they detect dangerously high concentrations of the gas, carbon monoxide detectors—which are commonly found in smart homes—sound an alert. They can also instinctively switch on the sprinklers or summon the fire department to keep things within control and stop the fire from destroying property or killing people.

vi. **Connected Switches-**Another essential component of smart home security systems are smart switches. Siri, Google Home, Amazon Echo, tablets, and smartphones may all be used to operate them. The gadgets provide convenience and enhance your experience by allowing you to easily operate electrical appliances, lights, and curtains [11].

9. USER PRIVACY CONCERNS

This is the new section focusing on privacy issues specifically associated with facial recognition motion detection systems in smart homes.

Nature of Biometric Data & Sensitivity

- Facial images / facial embeddings are **biometric identifiers**, which are more sensitive than, say, passwords or ordinary personal data. Once compromised, they are hard or impossible to change.
- These data can leak additional personal attributes: age, gender, race/ethnicity, emotional state, etc., sometimes without the individual's conscious consent.

Data Collection, Storage & Retention

- When and how is data collected? E.g., continuous video feed, or only when motion triggers capture. Continuous capture increases risk.
- Where is data stored? Locally (on-device) vs in the cloud or remote servers. Cloud storage typically increases risks (hacks, unauthorized access).
- How long is data retained? Long retention increases risk; deletion policies often are weak or nontransparent.

Consent, Transparency & User Control

- Users must consent to collection of biometric data; implicit or uninformed consent is insufficient.
- Users often lack clear information about what data is being collected, how it is treated, how extended stored, and who has access or shares data.
- Users should have control: ability to delete their data, opt in or opt out, or choose which data remains local or shared.

Misuse, Profiling & Surveillance

- Possible misuse includes tracking or profiling individuals beyond the original purpose (e.g. using facial recognition door cameras to track visitors or bystanders).
- Data could be shared or sold to third parties without user knowledge.
- There are risks of government or corporate surveillance, especially in regions without strong legal protection.

Algorithmic Bias, Errors & Discrimination

- Facial recognition systems may have different error rates across demographic groups (e.g. race, gender, age), which can lead to unfair outcomes (false positives/negatives).
- Error leading to wrongful denial of access or false alarms is not just inconvenient but potentially harmful.

Security Risks

- Hacking of biometric databases: illegal access, uniqueness theft, or misappropriation of stored face data.
- Spoofing attacks: presentation attacks (photos, masks), deepfake attacks, etc.
- Weak or no encryption of data in transit or at rest.

Psychological & Social Impacts

- Knowledge or belief of being constantly watched in one's own home can affect behavior, sense of autonomy.
- By-standing privacy: people who visit the home (guests, workers) may be recorded without their consent.

Legal & Regulatory Frameworks

- Varying by country: some have strong data protection / biometric laws; others have weak or no regulations.
- Laws about consensus, subjects' privileges, obliteration, sharing, and consequences are critical [12].

10. CONCLUSION

The foremost benefits of motion detection and facial recognition smart home security are automation, response, and deterrence. Yet, there are significant discretion implications that must be sensibly considered. If appropriate design, implementation, and regulation are not shadowed, risks such as surveillance, bias, misuse of biometric data, and absence of consent may exceed the welfares. A well-rounded approach that incorporates user control, transparency, legal protection, and technical precautions is essential for espousal to be both safe and communally acceptable. Motion detection, facial recognition, and Internet of Things-based smart home security systems have

a hopeful future. These technologies are expected to advance in intelligence, effectiveness, and security in the following years. As technology advances and goes yonder simple monitoring tools, these systems will grow into fully self-directed security environments that make homes safer, smarter, and further connected.

REFERENCES

[1]. Saxena, N., & Varshney, D. (2021). Smart home security solutions using facial authentication and speaker recognition through artificial neural networks. International Journal of Cognitive Computing in Engineering, 2, 154-164.
[2]. Smart Home: Definition, How It Works, Pros and Cons https://www.investopedia.com/terms/s/smart-home.asp
[3]. Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. IEEE access, 8, 139110-139120.
[4]. Karakaya, Ahmet. "Motion Sensors: Enhancing Security and Automation." Int J Sens Netw Data Commun 12 (2023): 213. [5]. https://www.elprocus.com/working-of-different-types-of-motion-sensors/
[6]. Why Motion Detectors Are Essential for Security Cameras Overview – The Big Picturehttps://www.dtiq.com/blog/video-surveillance/motion-detectors-for-security-cameras
[7]. Facial Recognition: applications, benefits and challenges https://keyless.io/blog/post/facial-recognition-applications-benefits-and-challenges
[8]. Top 5 Facial Recognition Challenges & Solutions, https://research.aimultiple.com/facial-recognition-challenges/
[9]. Smart Home Trends Transforming Homes in 2025, https://raleighrealty.com/blog/smart-home-trends
[10]. https://raleighrealty.com/blog/smart-home-trends
[11]. IoT-Based Home Security System: Benefits, Examples & Top Devices, https://www.intuz.com/blog/iot-smart-home-security-benefits-use-cases-and-top-devices
[12]. Sun, Z., & Liu, Z. (2025). Ensuring privacy in face recognition: a survey on data generation, inference and storage. Discover Applied Sciences, 7(5), 441.