Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 6, December 2025, pp. 4601~4613
ISSN: 2302-9285, DOI: 10.11591/eei.v14i6.9674

Artificial intelligence in smart home security: balancing innovation with ethics

Ashraf Al Sharah[1], Tareq A. Alawneh[1], Hamza Abu Owida[2], Jawdat S. Alkasassbeh[1], Zahid Iqbal[3]
[1]Department of Electrical Engineering, Faculty of Engineering Technology, Al-Balqa Applied University, Amman, Jordan
[2]Department of Medical Engineering, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan
[3]Department of Computer Science, Air University, Islamabad, Pakistan

Article Info

Article history:

Received Dec 8, 2024
Revised Sep 13, 2025
Accepted Sep 27, 2025

Keywords:

Artificial intelligence
Automation
Ethics
Machine learning
Privacy
Security
Smart home

ABSTRACT

Because of the evolution of artificial intelligence (AI), home security has progressed from a basic security system to an active architecture that is responsive and adaptive to real world situations. Due to the rapid adoption of AI in smart systems, there is increasing suspicion surrounding privacy issues and ethical ambiguity, as well as gaps when it comes to regulating these technologies. We provide an overview of AI in smart home security applications and examine the area of security, access control, intrusion detection, human action recognition, and research on intelligent automation. We summarize the last decade of evolution, with some summaries of previous on computer vision, authentication systems, and finding unusual patterns recently. Our key findings include the development of approaches to improve real time security monitoring, dramatic reductions in false alarms, and customization of home access using AI. Improvements in security have also increased risk with respect to ethical ambiguity as well as technical issues in certain cases. In this paper, we offers pathways for improved AI system design, proposed formal data protection regulations, and examples of simplifying complex system for user comprehension, which also establishes the groundwork for future efforts. Home security should balance new opportunities with ethical considerations.

Corresponding Author:

Ashraf Al Sharah
Department of Electrical Engineering, Faculty of Engineering Technology, Al-Balqa Applied University
Amman, Jordan
Email: aalsharah@bau.edu.jo

1. INTRODUCTION

Heavy-duty locks in the past used to be a security system, and it was the limit of home protection technology. Home security has changed like everything else, with the rapid growth of technology, the time of the smart home has arrived [1]–[3]. The modern home is an intelligent system connected with many sophisticated devices, sensors, and artificial intelligence (AI) systems that all work together to ensure not only security but also safety and ease of operation in daily activities. Implementation of AI within the framework is the best improvement for smart home protection. This integration also provides proactive protection of the occupants inside the home. These effects can go further than security. They can be reached into how we see the home in social and cultural terms. Modern homes act almost like living systems. They can be adjusted, learn from user habits, and react instantly to threats when they arise [4], [5].

This paper shows how technology is not only convenient, but it can also affect people's lives in AI and smart home security. The smart home model of the current world is an active, formal, sensitive, and predictive body in which devices are not installed. This use of AI has exposed the reality that the days'

homeowners were just citizens while responding to a breach or already invaded are long gone, and, in reality, breaches will never be a breach again. There will be a consciousness of an already identified and attempted breach. The reality of home system security is already in the focus of AI-generated smart home systems and, to be confident, will be in the near and succeeding upcoming decades.

A result of AI, our very surroundings in our homes are able to think, learn, and take over on our behalf concerning what this entails for protection. The traditional security system in this case will be completely unwanted; our homes will instead be watched 24/7 by a living guardian. Moreover, with the AI-equipped devices, the house is capable of more than just monitoring for basic motion detectors and alarms. It will be able to recognize faces, understand and analyze voices, and comprehend the unique behavioral patterns the surroundings of each and every home bring. The house's protection has advanced from a formally passive security system to one that is fully proactive and abundant [6], [7]. Figure 1 illustrates the application of AI in modern smart home security systems.

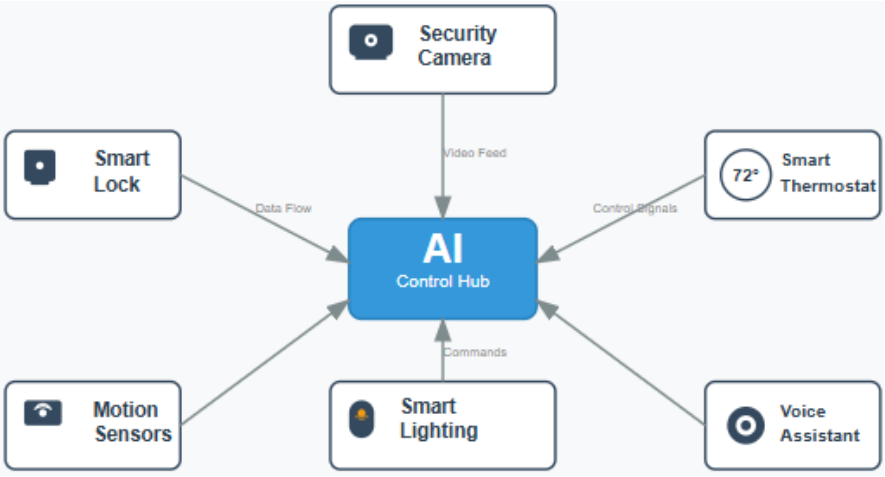

Figure 1. AI in smart home security

This in-depth reading integrates many aspects and uses of AI in smart home security, along with the pros and cons of this specific tech advancement. In the end, many ethical dilemmas will arise, especially issues of. Based on voice control and attitude management or facial recognition and secure access, through intrusion control. Every use case offers a different perspective on how one may safeguard one's home, comfort one's life, and protect one's identity simultaneously as never before. Given that the role of technology in people's everyday life constantly grows, and the line between technology and non-technology-based aspects of human lives becomes thinner and thinner, it is essential for AI in smart home security matters to be better understood, and the question of how much responsible and moral use is justified be asked. Each of these issues will be further addressed and discussed in the later sections of the current comprehensive study, taking the reader through the chronology of AI development in the field of smart home security and the factors determining the level of responsible and moral use.

While prior works may have looked either at the technical aspects of smart home instrumentation or at ethical concerns related to the application of AI, very few really looked at both sides from the residential perspective. With little critical analysis of how these systems behave in real environments or where ethical concerns persist in user's activities, most existing surveys examine device categories, communication protocols, or stand-alone aspects of AI. This paper addresses this gap through a dual-perspective review evaluating and reflecting the functioning of AI-enabled smart home security in regarding to ethical issues on bias, privacy, and consent. This may guide engineers and policymakers in focusing on the real-world within the framework of responsible AI deployment.

In collecting and analyzing relevant literature, this investigation used a structured approach. An attempt was made to gather peer-reviewed sources from five central digital libraries, namely IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Google Scholar. As for the time range, studies published between 2019 and 2024 were considered to ensure that the review represents recent advancements. Inclusion criteria selected only those sources that directly discussed AI techniques in smart homes or security mechanisms, or ethical aspects. A study was rejected if it restricted itself to industrial IoT, lacked technical

depth, or did not mention any security-related use cases. Through qualitative content analysis, ethical themes were identified. Keywords in the topics, such as privacy, bias, surveillance, consent, and fairness, were coded and categorized, enabling the paper to track ethical risks concerning specific AI functionalities such as facial recognition, anomaly detection, or voice control.

2. SMART HOME ECOSYSTEM AND ARTIFICIAL INTELLIGENCE'S ROLE

It is great to see the current generation that allows the interconnected devices and systems that make up the present-day smart home. With remarkable consolation, comfort, and protection, it changes the notion of 1's home, and signifies alternate in the relationship between the man or woman and the environment, the term refers back to the composite of interconnected elements that work closer to a wise, included safety solution.

2.1. Smart home ecosystem: a detailed overview

Smart homes, at their core, are made up of technologies and devices in many different categories. These include surveillance cameras, which care the "eyes" of a smart home, are necessary to monitor the immediate surroundings of the home. These cameras are designed to capture high-definition video and are equipped with advanced cameras and lenses to allow homeowners to see their property in real-time. Motion sensors: The motion sensor is the "ear" of a smart home security system. Passive infrared (PIR) and ultrasonic sensors are used to detect changes in motion and temperature. The sensors are strategically located in high-traffic areas and special detection zones, where they act as alarm triggers or automated systems [8], [9]. It also includes door locks, smart door locks provide added convenience and security. These doors allow homeowners to control access rights and lock/unlock doors remotely. It is possible to use biometric access verification technology, such as fingerprint recognition. Last category is alarm systems, which consist of sensors, such as PIR sensors, fire and carbon monoxide detectors, and various other detectors designed to detect a wide variety of things, from gas leaks to fires, and damaged surfaces. Homeowners begin signaling the alarm when the alarm goes off, and in some instances, the system can contact law enforcement or a security company directly [10].

Residents' safety and security are protected through environmental sensors that monitor the surroundings. These include smoke detectors, gas-related injury prevention systems, and devices that warn users of fire hazards. Audio and video intercoms are another type of device. They include the electronic systems of smart homes, such as the hubs, gateways, and routers, which serve to strengthen the interrelations of smart devices. Devices are able to share signals and can even send signals to other devices that are far from them. They make real-time communication possible, allowing users to control devices remotely. Services such as smartphones and digital tablets, in addition to AI voice devices, serve to empower users to monitor systems in their homes. Consumers can even count on the AI devices, such as Amazon Alexa and Google Assistant, which are capable of answering the voice requests of users. This interaction enables users to freely control the systems with minimal risk of hand contact with the smart security systems of their homes. Other mobile applications are available in the systems to offer users real-time access to faster processing systems [11].

2.2. Artificial intelligence's role in transforming smart home security

AI is the core of the ongoing revolution in smart home security. It transforms smart home security systems from simple hardware and software systems to complex, sensitive, and data-driven mechanisms. The multitude of functions that AI has in the sector can be summarized through several simple ideas.

AI has raised the capabilities of household surveillance. It enables real-time monitoring of premises using AI-powered surveillance cameras that can recognize and classify several objects [12]–[15]. To tell the difference between humans, pets, and vehicles, these systems rely on deep learning and computer vision. therefore, remote systems can provide very detailed responses to specific requests, for instance, an AI camera can tell the difference between a family member that has returned home and a thief that is trying to break into the home, which means reducing false alarms and increasing the effectiveness of the system. An example of a system that monitors household activity is an AI system that uses other documents to determine the level of noise in the premises and the movements recorded. It learns what is normal in a specific family setup so that it can recognize abnormal activity. The system can send notifications quickly if it notices any deviations from the predicted norm, which leads to improving the security awareness for this by making the intelligent home security system preempt possible security dangers [16].

Recognition of human activity, AI can also analyze human activity inside the house in real time, by using methods like recurrent neural networks (RNNs) and long short-term memory networks (LSTMs), the system keeps learning daily behavior patterns and separates normal activities from suspicious ones [17]–[20]. For example, it can tell the difference between someone cooking or watching TV and someone trying to enter

the home by force. This kind of activity recognition makes security systems faster, more flexible, and more responsive [21]. Beyond surveillance, AI can also perform facial recognition [22], support voice-activated biometrics [23], and improve automation by linking the security system with other smart devices in the home. Their intelligent, advanced, and seamlessly integrating architecture in the form of drivers in the home ecosystem makes them flexible for integrated security creations. We will discuss the impact of AI on home security systems, to rationally analyze the potential for safe, smart, and connected homes in their different phases.

3. REAL-TIME MONITORING WITH ARTIFICIAL INTELLIGENCE

In every smart home, the owner is given real-time information on the perimeter surveillance, which is made available because of the constant monitoring. This constant monitoring of the perimeter allows further enhancement to the level of protection of the smart home. In AI-driven cameras, the level of perimeter risk surveillance is dramatically reduced. The cameras can tell, name, and track specific objects, and can even monitor and analyze human activity, including behavior anomalies. Such cameras, and their associated systems, have transformed home security in the sense that real-time monitoring is no longer a stream of data, but a contextual and analytical evaluation of home activity.

3.1. Real-time monitoring: a cornerstone of smart home security

In smart home security design, continuous tracking is very important to success; these kinds of improvements affect how people inside the home experience safety, which allows them to shape both the sense of protection and the feeling of control over their environment [24].

3.2. AI-powered surveillance cameras: recognizing and categorizing objects

AI security cameras are one of the proofs that show improvements in AI can provide advanced real-time surveillance. The primary deep learning techniques responsible for these changes are convolutional neural networks (CNNs) and computer vision. These cameras have graduated from simple status figures to sophisticated observers with the ability to classify and identify objects in their fields of observation.

Object recognition, is a camera that AI can classify some targets as animals, people, and cars, among others. It goes beyond the simple action of detecting movement to the more advanced classification of objects and their behaviors. Therefore, an instance of using the camera to identify people is when it is able to separate a stranger who is trying to enter from a relative coming back from work. Homeowners can make better decisions because false alarm panic is greatly reduced, their understanding of the scenario is better, and the evaluation of the given situation is more informed.

Also, context-aware notifications where AI cameras send context-rich alerts; therefore, descriptive text may be included with alerts sent out to home mortgage holders as opposed to their movement detection messages. Alerts could say something like "Car detected in the driveway" or "Person identified near front door." Such aware alerts set the householder immensely in a better position to evaluate a situation and take necessary steps, thus building a more robust security setup than the conventional ones. AI infiltration: AI can detect threats in the home environment when it detects a departure from known patterns or from the expected norm. AI models that identify patterns and anomalies are being used for this task, such as isolation forests and one-class SVMs.

Learning normal patterns, these AI for real systems learn what normal behavior looks like for a given household, this is an iterative process where the system reviews past data, and identifies patterns, for example, it might look at how family members generally move through certain areas of the house at specific times to see if pets might be active during specific times of day whether any doors or windows should remain closed at night.

Identify anomalies, once you have a good idea of the normal behavior of the system, it's particularly straightforward to recognize anomalies. Anomalies can take many forms, including unusual movement, unusual noise, as well as deviations from normal. For example, there may be actual system observations of a totally empty house or an open window around dusk; all of these actions are seen by the system, presented as anomalies, and are accelerated. Providing signals: the AI-based totally intelligence-fueled framework gives proactive notifications at the point of detection of errors. Mortgagees receive convenient alerts through many channels, along with textual content messages, direct communication with protection expert agencies, and cellular notifications. Often, the device will become a watchdog alert, constantly alerting property owners to incorrect information so they respond and take suitable action immediately [25]–[27].

3.3. Recognizing human activities in real-time

The ability to continuously capture human activity is another application of artificial intelligence. RNNs and LSTMs may use both the instantaneous information to identify suspicious behavior universally distinguishable from testing how the normally perform. The ability to recognize human activity in real-time is one more application AI can use. RNNs and LSTMs are able to analyze time series data to distinguish between potentially suspicious behavior and simple everyday activity ultimately defining these opportunities.

In temporal analysis, AI systems analyze the sequence of activities over time, it recognizes and defines common activities like working, watching TV, and cooking. The system learns to identify these patterns based on commonly evolving behaviors.

Beyond normal and suspicious, the issue of distinguishing suspicious activity from abnormal activity signifies to systems a usable form of security solution exhibits security solutions like alerts, notify users of the alarms and may call the police if they see motions which somewhat denote an attempt to enter. Integrating of this situation become vigorous. Context increasing security situations: One of the satisfactions of AI ability to recognize human activities is its ability to contact lesser or normal to more secure management issues. It allows the system to determine whether the operation is safe or is entering into risky actions or gestures. Greater sensitivity to this capability will enable each security solution to respond more quickly and efficiently thus offer more secure solution [28], [29].

4. FACIAL RECOGNITION AND BIOMETRICS

Facial recognition technology is one of the most significant developments in smart home safety. The application of AI has quickly made it very important aspect of home security facial recognition technology is a new frontier in home safety using deep learning algorithms to find match and analyze facial features, while giving a seamless and personalized experience within the smart home ecosystem and enhancing security to add the new concept of monitoring most visitors, using facial recognition offers extra comfort and safety.

4.1. Facial recognition: a revolutionary addition to smart home security

Facial popularity era isn't continually the key alternate in smart home protection. Specifically, this era makes use of deep style knowledge to research facial capabilities and complicated AI algorithms, such as CNNs.

Safety enhancements increase safety to an excellent degree is one of the predominant advantages of a great facial popularity. The accuracy of this technology need to be very high as human beings pay attention how they ought to be seen. Illegal get right of entry to is basically eliminated and get entry to is improved. This reinforces the security of the smart home by using denying access to best marked and certified clients.

Personalization is an AI-powered facial reputation gear can recruit humans to trust them at home. This transition turned into in no way so easy. For example, if a regarded family member configures the front door, the machine can reply right away, unlocking it with a robot, changing the lighting and heating settings in keeping with gender, or maybe being transported with the aid of information becomes a smart home it is bendy and designed to healthy its occupants.

Facial popularity has redefined the method to the generation due to simplicity. The male or woman homepage acts as a smart home key, replacing extra traditional techniques which include keys or PIN devices. In addition to being extremely convenient, this arms-loose solution reduces the dangers related to traditional door-to-door techniques. Weak pins and motionless keys disappear from the past [30]–[32].

4.2. Visitor tracking through facial recognition

Not most effective does facial reputation offer protection and customization, however it also creates another angle: vacationer monitoring. This provider further improves home protection by way of allowing the machine to identify and reply to all of us within the area of the property:

Visitor detection, facial popularity generation scans someone's face even as it's far nevertheless within range. The device can be customized to provide greetings for authorized people, like family members and guests. This way device can unlock doors, activate security settings and according to visitor's needs.

Unknown visitors, even if the visitor faces cannot be recognize by the system, the device can still manage this situation or problem in effective way. It could record people through images or videos which can be reviewed later. If there is any suspicious behavior, the system will send an alert to either homeowners or security agency. Accessibility in smart homes can be managed or improved by giving controlled entry to certain visitors or guests. For example, if there is some work at the home workers may gain temporary access within a specific time window, this way ensures that the services will be completed safely within limits that are defined by the homeowners. The combination of facial recognition and smart home security has created a new level for personalization and safety, and guaranteeing high security level. This transforms the way we understand home security, and enabling delivery to be an ideal and intelligent process. Which is achieved by

improving visitor access and redesigning entry routes. These advances are reshaping the way of home security and smart living experiences [33]–[35].

5. VOICE CONTROL AND AUTOMATION

One of the key components of smart home security are automation and voice control, these evolution have improved the overall security measures and simplify user interaction. The combination of voice-activated virtual assistants like Google Assistant and Amazon Alexa has completely changed how people use their smart security devices. Accordingly, AI automation allows homeowners to easily create highly customized products that combine advanced safety features with comfort.

5.1. Voice control: pioneering seamless interaction

A key feature of today's smart home safety is voice manipulate, which allows people talk with their devices. The advent of voice-activated virtual assistants has dramatically changed the person revel in. This is an extra accurate evaluation of the position of sound in smart home safety:

Hands-free when the usage of smart devices, voice manipulate eliminates the need for manual enter. Voice instructions offer a smooth manner to control your security device, whether or not you're busy doing chores, want to position groceries in, or simply need to use it fingers-free.

Understanding commands, where natural language processing (NLP) and AI allow digital assistants to understand and execute common language instructions. All a long time and technical skills can use smart home safety thanks to its simple interface. Your safety machine may be configured with simple instructions consisting of "lock the front door" or "test the popularity of the surveillance cameras."

Also in rapid response the safety system responds quickly to voice commands. This quick response is especially important under security conditions when you must respond immediately, in addition to arming or disabling systems, checking fame of sensors, or locking doors.

While easy access by using voice command enables smart home security which makes it easier for everyone, including people with mobility problems or disabilities to interact and communicate with their security systems. This ease of access shows how technology can make differences [36], [37].

5.2. Automation: customized routines for enhanced convenience and security

Smart home safety structures are constructed round automation by using AI it helps houses to create custom designs that provide extra protection and luxury. Below is a deeper study the position of automation in a smart home ecosystem:

Security measures where automation lets in house owners to install security features which are deliberate or caused with the aid of activities. For instance, house owners can really arm security structures, lock doors, and activate movement detectors as they shuttle to paintings. Upon go back, the device can turn off safety functions, change lighting to a snug surroundings, and manage the thermostat for comfort.

Automation permits wise machines to paintings together. When an alarm happens, the device is able to show on all applicable devices, including lights, safety offerings and the owner of a house's smartphone, this coordinated reaction improves the overall safety device.

Preventive measures is one of the maximum important tools to prevent viable attacks is automation. For example, in case the device detects a tried attack, it may cause a series of activities consisting of activating lighting, sounding an alarm or loud song, and sending a notification by following these steps you can disrupt an attacker's progress and decrease their potential danger.

In environmental improvement automation goes beyond protection and improves the pleasant of existence. Homeowners can get a smart thermostat device to maximize electricity performance. Technology can robotically alter the temperature to save you power outages whilst humans depart the house. The thermostat guarantees that the residence is again to a pleasing temperature. This enables to reap environmental dreams and reduces power fees [38]–[40].

6. INTEGRATION WITH OTHER SMART DEVICES

One of the aspects of the big and larger interrelated smart device ecosystem is smart home security, the ecosystem includes many smart devices dedicated to improving home comfort, protection and security, including lighting devices controls, entertainment frames, and thermostats. These devices and AI communicate with each other easily and form a combined and powerful ecosystem, Table 1 presents some examples of it involves integration with other intelligent devices.

Table 1. AI integration with other smart devices

Aspect	Description
Integration with smart lighting systems	Coordinated reactions to security incidents are made possible by the seamless integration of smart lighting and home security systems. One way to improve visibility and discourage trespassers is by setting up lights to switch on automatically when motion sensors detect activity.
Connectivity with smart thermostats	Secure measures that use less energy are made possible by integration with smart thermostats. A home's temperature can be optimally controlled without sacrificing security when the security system recognizes when it is empty. It can accomplish this by communicating with the thermostat.
Collaboration with smart locks	Security systems and smart locks can work together to improve access control. For example, smart locks can automatically secure entry points when the security system is armed, giving homeowners an extra degree of security and peace of mind.
Interaction with smart entertainment	To improve user experience, smart entertainment devices and home security systems can communicate with each other. To keep residents informed about security incidents while they're having fun, for instance, security warnings can be sent through smart speakers or shown on smart TVs.

6.1. The smart home ecosystem: a symphony of devices

The intelligence of the smart home today consists of smart devices with security systems and is continuously expanding. These devices are designed to boom internal capability and connectivity:

With the help of smart thermostat, the heating and cooling device of the residence may be optimized. Residents' plans and choices are aligned, lowering power intake and software bills and increasing consolation.

Homeowners who set up smart lights structures have whole flexibility over their lighting fixtures elements such as timing, color and brightness by allowing customers to set custom lighting fixtures or even mechanically flip lights off whilst the room is empty they help maintain the power grid strolling.

In entertainment hardware entertainment is provided by unobtrusive TV speakers and in home cinema they can effects interact with the smart homes wide community provided portable relaxation and centralized command.

Smart home appliances like smart ovens, washers and refrigerators are being created for more inexperienced home appliances and instant connectivity, home owners can monitor and control such appliances remotely, saving power and bringing comfort.

The main domains that govern the smart home are voice assistants in the shape of Google Assistant and Amazon Alexa they provide a homogenized and human-friendly interface with voice correction to many devices [41]–[43].

6.2. Artificial intelligence-driven integration: the loom that weaves the smart fabric

AI is a guiding function to effectively integrating sperate devices inside the smart home it acts as an integrator that connects and coordinate devices allowing them to work together more efficiently and successfully, the predominant capabilities of AI powered integration encompass the following:

AI powered structures are designed to be compatible with a big variety of devices and networks built in connectivity this called interactivity, that allows owners to mix capabilities from exceptional producers to create a smart homes this is flexible and adaptable.

AI is taking automation to a brand new stage in smart home control. For example, a protection device can trigger a series of occasions which include turning on lighting fixtures, sounding an alarm and locking doorways when it detects an outsider and the device can conserve electricity by means of changing the timing of lighting and thermostats with house owners attending to work.

AI is needed to facilitate data sharing between devices. This means that the devices are able to choose which objects can be protected based on the information received. For example, a security system could detect that a house is empty and connect it to a thermostat to change the temperature. This saves energy and reduces electricity bills.

In case of customization when homeowners use multiple devices, customization can be done. A typical "good morning" ritual involves turning on the coffee machine, changing brightness of the lights, and setting the thermostat to the appropriate scale They can be provided by voice commands, planned opportunities, or other incentives for additional products performance has improved and enjoyment of daily life has increased [44]–[47].

The key part of smart home security is how well it connects with many other smart devices to create a unified ecosystem. AI is at the heart of managing and enhancing these interactions. Real-world examples like Home Assistant and Samsung SmartThings showcase this integration beautifully. Home Assistant, which is open-source, allows for local automation that respects your privacy, linking devices like motion sensors, locks, lights, and voice assistants. It can handle complex AI-driven routines, such as turning on lights and unlocking doors only when a familiar face approaches during specific hours. On the other hand, Samsung SmartThings provides a commercial option where cloud-based AI manages devices from different brands

through routines and scenes, like automatically locking doors when someone leaves or starting camera recordings when motion is detected. To clarify the system architecture, Figure 2 presents a flow diagram that illustrates how smart home components interact.

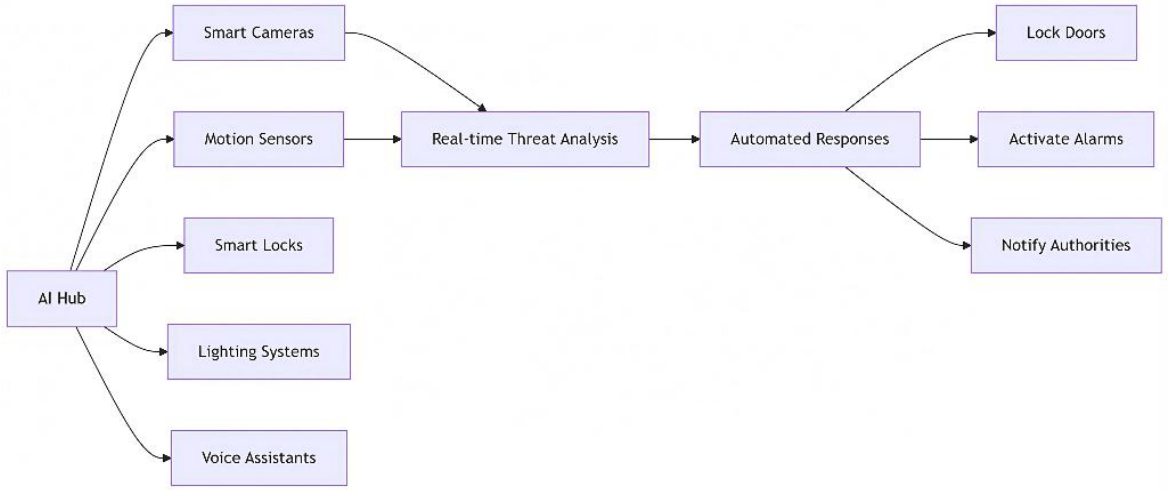

Figure 2. AI integration architecture in smart home ecosystems

7. ENHANCED SECURITY AND ENERGY EFFICIENCY

The integration of smart devices with a larger smart home system basically means, enhanced safety and efficiency. This article significantly enhances safety and efficiency from the combination of smart devices and AI. Increased security, the expansion beyond standard devices, AI-driven integration is slowly impacting home security. The creation of a smooth communication system between security devices and smart devices will increase the possibility for combined dynamic response devices. The integrated devices act as a hidden response, which leads the system to initiates a protocol in response to a security breach.

Real-time security updates will flow through smart speakers to the homeowner also lights blink wildly, and alarms ring to stop and scare thieves so they run away. This joint or coordinated response prevent incidents and increases the reality of protection status in the home. Integration also enable the reactive models, for example, a security system can interact with a smart lock to ensure automatically secure once the system is armed. This comprehensive integration dynamically influences the security ecosystem, where elements work together to protect the home. When components react robustly to the ever changing nature of potential threats, this ensures that security AI-driven communication creates an intelligent and robust security community [48], [49].

The ultimate goal of building sustainable and energy-efficient homes is achieved by AI and intelligent devices to improve energy efficiency. To adjust the heating system intelligently, the security system senses if house is empty and initiates a communication with the thermostat. According to this data, the thermostat will ensures that all systems required temporarily power or are operated at reduced power are stopped, this leds to save energy without affecting the comfortless. Based on access strategies detected by the security system, AI can optimize the use of other devices that intense energy. For example, it can reduce energy consumption, it simply can tell smart lighting systems to change lighting or turn it off according to the room situation like if its empty or not [50], [51]. All of these elements cooperate with each other to create a home that is very safe, and secure and overall is energy efficient. Together, AI and smart devices assure intelligent use of energy, reduce operating costs and this will also have a positive environmental impact, also will improved security and energy efficiency on homes. As smart home technology continues to improve, AI-driven home structures shows that, the solutions can be developed are not only smart and safe but also practical and sustainable.

8. REAL EXPERIMENTAL FRAMEWORK FOR AI IN SMART HOME SECURITY

As a scientific contribution, a real experimental setup was designed and implemented with available commercial hardware and software, to implement a real case validation of AI driven security functionalities in a smart home environment, the installation was carried out in a controlled environment, which can

simulate the entrance of a home and includes tiny room, and a main door for entering. Surveillance was provided by Wyze Cam v3; access control was provided by a Yale Assure SL lock motion was detected by an Aqara sensor and voice commands were given via a Google Nest Hub. The AI edge processing device was a Raspberry Pi 4 paired with a Google Coral USB Accelerator. Integration of devices automation of events and monitoring of systems were managed by Home Assistant, NodeRED, MQTT, Frigate, and InfluxDB.

A wireless or wired ethernet connection was made between all the devices the system was tested in five predefined steps from phases 1 to 5 which simulate recognition, automation, and alerting functionality. These are authorized user recognition rejection of unfamiliar people acceptance and rejection of good commands in noiseless and noisy environments and acceptance and rejection of disguised people. Objective performance tests included recognition rate, intruder detection, false alarm rate, and voice command delay, experimental results reaffirmed that it did better than expected performance in certain aspects. It reached 95% for intrusion detection accuracy while facial recognition maintained a steady 90% recognition rate in normal circumstances. Voice commands were executed in the range of 400-800 msec depending on the noise level. However, face recognition dropped to 78% in the event of partial occlusion, thus showing a typical weakness of contemporary AI models in real-world usage, the false alarm rate was below 10%, with the majority of the exceptions due to low-light misclassifications.

These experimental results clearly show that these AI features we presented do function. Also, we found some practical issues like how the AI struggles with blocked lines of sight and background noise. This framework not only enhances our research but also helps to lay the groundwork for the successful implementation of AI in smart home security for future research.

9. FUTURE TRENDS IN ARTIFICIAL INTELLIGENCE AND SMART HOME SECURITY

Smart home security is on the edge of a major shift as technology continues to advance very fast. This section explores the key trends that will help to shape the future of AI in smart home security. Advances in AI algorithms, closer human device interaction, and broader use of AI in threat detection and mitigation are the main keys to shaping the development of new and more effective security systems.

9.1. Advancements in artificial intelligence algorithms

Ongoing refinement of AI algorithms is crucial for the future of smart home security. There are several key trends:

Increased visibility, smart cameras with preferred range, can be able to uniquely identify between human and vehicles. More accurate identification will lead to fewer false alarms, and basically enhance ordinary security capabilities. Behavioral analysis, where AI will help security systems to not only detect anomalies but also detect the context surrounding the anomaly. For example, the system will be able to recognize individuals that are a family members in distress, who is trying to access a door with a key, from a thief who is trying to get through a door.

In predictive analysis AI will evolve from our current state detection based response to smart analysis response recognition. Security systems will be designed to recognize opportunities for security breaches, by analyzing past data and human behavior, and actual backup of response security will help mitigate against a security breach through proactive response, like locking a door or putting an alarm into an active state. While in multisensory AI will have a more acute sense of its surrounding environment, by using widgets with multi-sensory capability along with audible, visible, and infrared sensing to establish their security awareness systems, which take security capabilities to an enhanced level [52], [53].

9.2. Enhanced human-machine interaction

The future of AI for home security in the smart home will be user experience. Some of the key trends in the market:

NLP as voice systems and security devices are getting more advanced, they are more natural to talk that means user can have a normal conversation with their security system, making it easier to use and simpler to communicate. Facial recognition and gestures: This can be integrated into security systems so the owners of homes can use gestures or facial expressions to communicate with the system, which makes it a personal experience.

Virtual reality (VR) and augmented reality (AR) are going to be widely used for practice and safety training to make it more engaging, VR headsets or AR overlays can be used at safety events to experience real life safety scenarios [54], [55].

9.3. Artificial intelligence for threat prevention

Security systems are made more reactive as AI plays a larger part in defending against threats. By Automated decisions, AI is able to use past data and current information to make decisions on its own. With

Intelligent controls, AI will have a wide of control options using restrictions that change based on activity, and threat as a means of security. Automatically aligned that permits appropriately, as per actual or required security threats, ensures the real time management of access. In collaborative security, AI will provide a dual security in both physical and digital world, this will be made by protecting against cyber-attacks and intrusion of physical security [56]–[59].

9.4. Critical evaluation of current artificial intelligence systems

It is good to make the home security system feasible for the potential usage of AI in the home security systems, although it is clear from a review from their advantages and problems. Facial recognition, smart voice systems, and real time monitoring have been found to reduce false alarms and reduce response times. There are several issues are raised in their field implementation, such as, facial recognition does not function under poor lighting conditions or when a person is wearing a hat, glasses, or other accessories, while voice assistants are impossible to use with rising surrounding sound or unknown accents which can cause limit accessibility. Furthermore, such AI models can leads to wrong results in facial recognition because they work different for different groups with different accuracy levels. Most of the systems are not reliable and require retraining when the user behavior changes or the home layout is changed, there is always a privacy versus functionality trade-off, as some aspects of the solutions will need to resort to cloud processing, risking data to the public. All these problems highlight the need for AI models to be accurate, explainable, and adaptable to user needs.

10. CONCLUSION

AI is changing smart home security into intelligent ecosystems, making them able to recognize behavior, anomalies, and automating safety features. However, it has serious privacy and ethical concerns, the implementers will have to implement data protection and user authorization as well as transparency of AI decision making. Future studies have to be focused on developing potential alignment between technological capabilities and regulatory frameworks, and the trust of the public. This work is important for future design to be able to create secure, ethical, and sustainable smart environments, with greater use of AI in our daily lives.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ashraf Al Sharah	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tareq A. Alawneh	✓	✓		✓	✓	✓			✓	✓		✓		✓
Hamza Abu Owida		✓	✓		✓	✓		✓		✓	✓			✓
Jawdat S. Alkasassbeh				✓	✓		✓		✓	✓		✓		✓
Zahid Iqbal	✓	✓							✓	✓				✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] K. Zhao, J. Zhong, and J. Ye, "Smart Home Security Based on the Internet of Things," in *Advances in Intelligent Systems and Computing*, vol. 1283, 2021, pp. 388–393, doi: 10.1007/978-3-030-62746-1_57.

[2] X. Guo, Z. Shen, Y. Zhang, and T. Wu, "Review on the application of artificial intelligence in smart homes," *Smart Cities*, vol. 2, no. 3, pp. 402–420, Aug. 2019, doi: 10.3390/smartcities2030025.

[3] M. Z. Fakhar, E. Yalcin, and A. Bilge, "A survey of smart home energy conservation techniques," *Expert Systems with Applications*, vol. 213, p. 118974, Mar. 2023, doi: 10.1016/j.eswa.2022.118974.

[4] J. Tao, H. Wu, S. Deng, and Z. Qi, "Overview of intelligent home security and early warning system based on internet of things technology," *International Core Journal of Engineering*, vol. 8, no. 5, pp. 727–732, 2022, doi: 10.6919/ICJE.202205_8(5).0093.

[5] W. Li, T. Yigitcanlar, A. Liu, and I. Erol, "Mapping two decades of smart home research: A systematic scientometric analysis," *Technological Forecasting and Social Change*, vol. 179, p. 121676, Jun. 2022, doi: 10.1016/j.techfore.2022.121676.

[6] A. Tripathi, N. Sindhwani, R. Anand, and A. Dahiya, "Role of IoT in Smart Homes and Smart Cities: Challenges, Benefits, and Applications," *EAI/Springer Innovations in Communication and Computing*, pp. 199–217, 2023, doi: 10.1007/978-3-031-04524-0_12.

[7] B. Basarir-Ozel, H. B. Turker, and V. A. Nasir, "Identifying the Key Drivers and Barriers of Smart Home Adoption: A Thematic Analysis from the Business Perspective," *Sustainability*, vol. 14, no. 15, pp. 1-19, Jul. 2022, doi: 10.3390/su14159053.

[8] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "Access control and surveillance in a smart home," *High-Confidence Computing*, vol. 2, no. 1, p. 100036, 2022, doi: 10.1016/j.hcc.2021.100036.

[9] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, doi: 10.1155/2022/9307961.

[10] A. Darem, A. A. Alhashmi, and J. H. A, "Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem," *IJCSNS International Journal of Computer Science and Network Security*, vol. 22, no. 3, pp. 303–310, 2022, doi: 10.22937/IJCSNS.2022.22.3.39.

[11] O. Alsamarah, K. A. Alshare, and P. L. Lane, "Determinants of individual's intention to use the Internet of Things for smart home technology: a cultural moderating effect," *International Journal of Mobile Communications (IJMC)*, vol. 21, no. 3, pp. 316–340, 2023, doi: 10.1504/IJMC.2023.129980

[12] S. F. A. Abuowaida, H. Y. Chan, N. F. F. Alshdaifat, and L. Abualigah, "A novel instance segmentation algorithm based on improved deep learning algorithm for multi-object images," *Jordanian Journal of Computers and Information Technology*, vol. 7, no. 1, pp. 74–88, 2021, doi: 10.5455/jjcit.71-1603701313.

[13] M. Muzammul, Muhamad, and X. Li, "Comprehensive review of deep learning-based tiny object detection: challenges, strategies, and future directions," *Knowledge and Information Systems*, vol. 66, pp. 1-89, 2025, doi: 10.1007/s10115-024-02188-2.

[14] H. A. Owida, O. S. M. Hemied, R. S. Alkhawaldeh, N. F. F. Alshdaifat, and S. F. A. Abuowaida, "Improved Deep Learning Approaches for Covid-19 Recognition in Ct Images," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 13, pp. 4925–4931, 2022.

[15] A. Al Sharah, H. A. Owida, F. Alnaimat, and S. Abuowaida, "Application of machine learning in chemical engineering: outlook and perspectives," *IAES International Journal of Artificial Intelligence (IJAI)*, vol. 13, no. 1, pp. 619–630, 2024, doi: 10.11591/ijai.v13.i1.pp619-630.

[16] A. A. Zaidan and B. B. Zaidan, "A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations," *Artificial Intelligence Review*, vol. 53, no. 1, pp. 141–165, 2020, doi: 10.1007/s10462-018-9648-9.

[17] S. F. A. Abuowaida and H. Y. Chan, "Improved deep learning architecture for depth estimation from single image," *Jordanian Journal of Computers and Information Technology*, vol. 6, no. 4, pp. 434–445, 2020, doi: 10.5455/jjcit.71-1593368945.

[18] D. Bouchabou, S. M. Nguyen, C. Lohr, B. Leduc, and I. Kanellos, "A survey of human activity recognition in smart homes based on iot sensors algorithms: Taxonomies, challenges, and opportunities with deep learning," *Sensors*, vol. 21, no. 18, pp. 1-28, 2021, doi: 10.3390/s21186037.

[19] Y. Djenouri, A. N. Belbachir, A. Cano, and A. Belhadi, "Spatio-temporal visual learning for home-based monitoring," *Information Fusion*, vol. 101, pp. 1-9, 2024, doi: 10.1016/j.inffus.2023.101984.

[20] N. F. F. Alshdaifat, M. A. Osman, and A. Z. Talib, "An improved multi-object instance segmentation based on deep learning," *Kuwait Journal of Science*, vol. 49, no. 2, 2022, doi: 10.48129/kjs.10879.

[21] H. Abedi, A. Ansariyan, P. P. Morita, A. Wong, J. Boger, and G. Shaker, "AI-Powered Noncontact In-Home Gait Monitoring and Activity Recognition System Based on mm-Wave FMCW Radar and Cloud Computing," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9465–9481, 2023, doi: 10.1109/JIOT.2023.3235268.

[22] X. Wu, Z. Zhou, and S. Chen, "A mixed-methods investigation of the factors affecting the use of facial recognition as a threatening AI application," *Internet Research*, vol. 34, no. 5, pp. 1872-1897, 2024, doi: 10.1108/INTR-11-2022-0894.

[23] R. Alazaidah, M. A. Almaiah, and M. Al-Luwaici, "Associative classification in multi-label classification: An investigative study," *Jordanian Journal of Computers and Information Technology*, vol. 7, no. 2, pp. 166–179, 2021, doi: 10.5455/JJCIT.71-1615297634.

[24] O. Tarawneh *et al.*, "The Effect of Pre-processing on a Convolutional Neural Network Model for Dorsal Hand Vein Recognition," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 1284–1289, 2024, doi: 10.14569/IJACSA.2024.01503126.

[25] P. U. Maheswari, V. R. Karishma, and T. Vigneswaran, "Artificial intelligence in video surveillance," *Handbook of Research on Deep Learning Techniques for Cloud-Based Industrial IoT*, pp. 1–17, 2023, doi: 10.4018/978-1-6684-8098-4.ch001.

[26] S. Wan, L. Qi, X. Xu, C. Tong, and Z. Gu, "Deep Learning Models for Real-time Human Activity Recognition with Smartphones," *Mobile Networks and Applications*, vol. 25, no. 2, pp. 743–755, 2020, doi: 10.1007/s11036-019-01445-x.

[27] S. Qiu *et al.*, "Multi-sensor information fusion based on machine learning for real applications in human activity recognition: State-of-the-art and research challenges," *Information Fusion*, vol. 80, pp. 241–265, 2022, doi: 10.1016/j.inffus.2021.11.006.

[28] D. F. Romero-Moreno, "AI facial recognition and biometric detection: Balancing consumer rights and corporate interests," in *2021 International Carnahan Conference on Security Technology (ICCST)*, Hatfield, United Kingdom, 2021, pp. 1-5, doi: 10.1109/ICCST49569.2021.9717403.
[29] P. Kaur, K. Krishan, S. K. Sharma, and T. Kanchan, "Facial-recognition algorithms: A literature review," *Medicine, Science and the Law*, vol. 60, no. 2, pp. 131–139, 2020, doi: 10.1177/0025802419893168.
[30] D. Utegen and B. Z. Rakhmetov, "Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models," *Journal of Digital Technologies and Law*, vol. 1, no. 3, pp. 825–844, 2023, doi: 10.21202/jdtl.2023.36.
[31] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020, doi: 10.1109/JIOT.2020.3004077.
[32] S. Nivash *et al.*, "Implementation and Analysis of AI-Based Gesticulation Control for Impaired People," *Wireless Communications and Mobile Computing*, vol. 2022, 2022, doi: 10.1155/2022/4656939.
[33] B. Li *et al.*, "Trustworthy AI: From Principles to Practices," *ACM Computing Surveys*, vol. 55, no. 9, 2023, doi: 10.1145/3555803.
[34] G. Tolomei, C. Campagnano, F. Silvestri, and G. Trappolini, "Prompt-to-OS (P2OS): Revolutionizing Operating Systems and Human-Computer Interaction with Integrated AI Generative Models," in *2023 IEEE 5th International Conference on Cognitive Machine Intelligence (CogMI)*, Atlanta, GA, USA, 2023, pp. 128–134, doi: 10.1109/CogMI58952.2023.00027.
[35] D. Bilika, N. Michopoulou, E. Alepis, and C. Patsakis, "Hello Me, Meet the Real Me: Audio Deepfake Attacks on Voice Assistants," *arXiv preprint*, 2023, doi: 10.48550/arXiv.2302.10328.
[36] K. K. H. Ng, C. H. Chen, C. K. M. Lee, J. (Roger) Jiao, and Z. X. Yang, "A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives," *Advanced Engineering Informatics*, vol. 47, 2021, doi: 10.1016/j.aei.2021.101246.
[37] A. Wilner and C. Babb, "New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour," *NL ARMS*, pp. 401–417, 2021, doi: 10.1007/978-94-6265-419-8_21.
[38] S. Sahoo and C. Y. Lo, "Smart manufacturing powered by recent technological advancements: A review," *Journal of Manufacturing Systems*, vol. 64, pp. 236–250, 2022, doi: 10.1016/j.jmsy.2022.06.008.
[39] A. Farooq, "The convergence of IoT and Image Processing in Sericulture: an overview of innovative applications," *International Journal of Social Analytics*, vol. 8, no. 6, pp. 16–35, 2023.
[40] A. Bodepudi and M. Reddy, "Cloud-Based Gait Biometric Identification in Smart Home Ecosystem," *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 49–59, 2021.
[41] N. Abdi, X. Zhan, K. M. Ramokapane, and J. Such, "Privacy norms for smart home personal assistants," in *Proceedings of the 2021 CHI conference on human factors in computing systems*, 2021, pp. 1-14, doi: 10.1145/3411764.3445122.
[42] H. Manglani, G. L. Hodge, and W. Oxenham, "Application of the Internet of Things in the textile industry," *Textile Progress*, vol. 51, no. 3, pp. 225–297, 2019, doi: 10.1080/00405167.2020.1763701.
[43] A. Aldoseri, K. Al-Khalifa, and A. Hamouda, "A Roadmap for Integrating Automation with Process Optimization for AI-powered Digital Transformation," *Preprints*, pp. 1-23, 2023, doi: 10.20944/preprints202310.1055.v1.
[44] F. Firouzi, B. Farahani, and A. Marinšek, "The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT)," *Information Systems*, vol. 107, p. 101840, 2022, doi: 10.1016/j.is.2021.101840.
[45] J. P. Bharadiya, "Machine learning and AI in business intelligence: Trends and opportunities," *International Journal of Computer (IJC)*, vol. 48, no. 1, pp. 123–134, 2023.
[46] Z. Lv, L. Qiao, A. Kumar Singh, and Q. Wang, "AI-empowered IoT Security for Smart Cities," *ACM Transactions on Internet Technology*, vol. 21, no. 4, 2021, doi: 10.1145/3406115.
[47] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274–283, 2022, doi: 10.1016/j.comcom.2021.09.029.
[48] K. Alhusayni, R. Wazirali, M. AlAkhras, M. Almasri, and S. Alhazmi, "A Multi-Stage Secure IoT Authentication Protocol," *Computer Systems Science & Engineering*, vol. 45, no. 1, 2023, doi: 10.32604/csse.2023.028536.
[49] H. Farzaneh, L. Malehmirchegini, A. Bejan, T. Afolabi, A. Mulumba, and P. P. Daka, "Artificial intelligence evolution in smart buildings for energy efficiency," *Applied Sciences*, vol. 11, no. 2, pp. 1–26, 2021, doi: 10.3390/app11020763.
[50] E. Saxena, P. Shoran, and M. Yadav, "Smart systems and services by artificial intelligence algorithms," *Applying Drone Technologies and Robotics for Agricultural Sustainability*, pp. 245–258, 2023, doi: 10.4018/978-1-6684-6413-7.ch015.
[51] T. Mazhar *et al.*, "Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review," *Electronics*, vol. 12, no. 1, pp. 1-25, 2023, doi: 10.3390/electronics12010242.
[52] R. Rawat, "Harnessing the Power of IoT and AI for Human Evolution," *International Journal of Research in Science & Engineering*, vol. 3, no. 3, pp. 58–68, 2023, doi: 10.55529/ijrise.33.58.68.
[53] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "The Future of the Human–Machine Interface (HMI) in Society 5.0," *Future Internet*, vol. 15, no. 5, pp. 1-23, 2023, doi: 10.3390/fi15050162.
[54] P. Tyagi and S.K. M. bargavi, "Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 1, pp. 1–10, 2023, doi: 10.59461/ijdiic.v2i1.42.
[55] M. Wang, N. Yang, and N. Weng, "Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System," *Electronics*, vol. 12, no. 9, pp. 1-19, 2023, doi: 10.3390/electronics12092100.
[56] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review," *Electronics (Switzerland)*, vol. 12, no. 18, pp. 1-19, 2023, doi: 10.3390/electronics12183958.
[57] G. Samara *et al.*, "A Comprehensive Review of Machine Learning-Based Intrusion Detection Techniques for IoT Networks," *Studies in Computational Intelligence*, vol. 1113, pp. 465–473, 2023, doi: 10.1007/978-3-031-43300-9_38.
[58] A. Arabiat and M. Altayeb, "Enhancing internet of things security: evaluating machine learning classifiers for attack prediction," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 5, pp. 6036–6046, 2024, doi: 10.11591/ijece.v14i5.pp6036-6046.
[59] S. Nafaa *et al.*, "Advancing Roadway Sign Detection with YOLO Models and Transfer Learning," in *2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI)*, Mt Pleasant, MI, USA, 2024, pp. 1-4, doi: 10.1109/ICMI60790.2024.10586105.

BIOGRAPHIES OF AUTHORS

Ashraf Al Sharah has completed his Ph.D. from Tennessee State University. USA. He was a research associate at cyber vis research lab. He currently serves as an Assistant Professor in the Department of Electrical Engineering at Al-Balqa Applied University, following his previous role as an Assistant Professor in the Department of Computer Engineering at Al-Ahliyya Amman University. His research interest includes wireless security, IoT, smart attack, AI, and game theory. He can be contacted at email: aalsharah@bau.edu.jo.

Tareq A. Alawneh received the B.S. and M.S. degrees in computer engineering from the Jordan University of Science and Technology (JUST), Irbid, in 2006 and 2009, respectively, and the Ph.D. degree in computer engineering from the University of Hertfordshire, U.K., in 2021. From 2010 to 2013, he was a full-time Lecturer with the Electrical and Computer Engineering Department at Tafila Technical University (TTU), Al-Tafila, Jordan. He was an Assistant Professor at Fahad Bin Sultan University (FBSU), Saudi Arabia, in 2021. He is currently an Assistant Professor with the Electrical Engineering Department at Al-Balqa Applied University. He can be contacted at email: tareq.alawneh@bau.edu.jo.

Hamza Abu Owida has completed his Ph.D. from Keele university, UK. He was a postdoctoral Research Associate: developing xeno-free nanofibrous scaffold methodology for human pluripotent stem cell expansion, differentiation and implantation towards a therapeutic product, Keele University, Institute for Science and Technology in Medicine (ISTM), Staffordshire/UK. He is associate professor in medical engineering department in Al-Ahliyya Amman University. He has published more than 30 papers in reputed journals. He can be contacted at email: h.abuowida@ammanu.edu.jo.

Jawdat S. Alkasassbeh was born in 1983 in Jordan. He received a B.Sc. in communications engineering from the Department of Electrical Engineering, Faculty of Engineering, Mutah University, Al-Karak, Jordan, in 2006 and a master's degree in communications engineering from the University of Jordan, Amman, Jordan, in 2011. Alkasassbeh earned his Ph.D. degree from the School of Mechanical Engineering and Electronic Information, China University of Geosciences, Wuhan, China, in 2021. He is an Assistant Professor at the Electrical Engineering Department at Al-Balqa Applied University, Amman, Jordan. His current research interests include applications of evolutionary algorithms, applied AI, power reduction of mobile communication mechanisms, digital wireless communication systems, radio link design, and digital image processing. He can be contacted at email: jawdat1983@bau.edu.jo.

Zahid Iqbal holds a Ph.D. in Computer Science from Universiti Sains Malaysia and has over 15 years of teaching and research experience. Since January 2025, he has been serving as Assistant Professor and Chair of the Department of Computer Science at Air University, Kharian Campus, and previously worked as a Senior Lecturer at the University of Gujrat from 2012 to 2024. His professional background includes a six-month research internship at OMRON OSX, Japan, and two years as a Software Engineer at Algorithm Consulting Company, providing him with valuable industry experience. His research interests include federated learning, deep learning, computer vision, artificial intelligence, and optimization. He is also an IBM Certified Data Scientist and IBM Certified Machine Learning Engineer. He can be contacted at email: zahid.iqbal@kc.au.edu.pk.