Smart Homes: Energy Efficiency and Safety Issues

Shokrollah Ghadyani [1] ✉,

[1]Tekdata Co., Tehran, Iran

Received: 03.03.2026

Accepted: 12.03.2026

Published: 31.03.2026

https://doi.org/10.54414/BPOY9265

Abstract: This article comprehensively examines energy efficiency and security issues in today's rapidly evolving smart home technologies. As a result of the adoption of new technologies such as digitization, automation, and the Internet of Things (IoT), significant achievements have been made toward optimizing energy use, enhancing security, and managing resources in residential buildings. Smart home systems not only provide home comfort but also prevent energy waste, reduce environmental load, and serve sustainable development goals. The article extensively analyzes the structural principles of smart home technologies, energy management mechanisms, the role of artificial intelligence (AI) and cloud technologies, as well as information security and cybersecurity issues. In the global experience, the application of smart home systems in the USA, Japan, Germany, and Scandinavian countries has resulted in 15-30% savings in energy consumption. In addition, the article examines the ways of localization of these experiences for Azerbaijan, state programs, and development directions of the normative-legal framework. The study shows that widespread adoption of smart home systems contributes to both energy independence and environmental sustainability. However, increasing network connections, the proliferation of IoT devices, and cloud-based data processing processes are creating new cybersecurity risks. For this reason, the article emphasizes the importance of implementing information security standards (ISO/IEC 27001, GDPR, etc.) in addition to ensuring technological efficiency. In general, the research aims to determine the scientific, technological, and social aspects of smart home models that increase energy saving, security level, and user well-being, as well as to evaluate the development prospects of this field in the conditions of Azerbaijan.

Keywords: smart home, energy efficiency, cybersecurity, IoT, AI, environmental sustainability, green energy, digital transformation

1. Introduction

The 21st century is characterized as an era where the global energy crisis and digital transformation intersect. Growing energy demand, climate change, urban congestion, and limited natural resources force humanity to look for smarter and more efficient technological solutions [1]. If the 20th century was the period of the industrial revolution, the 21st century can be evaluated as the stage of "digital and energy revolution". At the center of these changes is the concept of "smart home" - it is not just a technological innovation, but also a key component of social and environmental transformation. Smart homes connect home equipment, devices, and systems through information and communication technologies, optimizing energy use and providing user comfort [2]. These systems automatically manage heating, lighting, security, household appliances, and even water resources. Thus, the need for human intervention is minimal, energy losses are reduced, and the quality of life is increased. According to UN data for 2024, 35% of the world's

energy consumption is accounted for by residential buildings, and 28% of carbon emissions are formed in this sector [3].

This fact shows that the efficient use of energy is not only an economic issue, but also an issue of environmental and social responsibility. The modern approach is that the "living space" is not only a space, but also an "intelligent system" that collects information and saves energy. The government of Azerbaijan has also taken a number of steps in this direction. "Green energy" policy, "Smart city" and "Smart village" projects, especially the "Green Zone" initiatives in Karabakh and Eastern Zangezur, represent an important turning point in the country's energy and technological policy [4]. These projects ensure not only technological modernization but also environmental protection, energy security, and the implementation of a sustainable development strategy.

2. Smart Home Concept and Technological Basics

The technological infrastructure of smart homes is mainly based on the Internet of Things (IoT), artificial intelligence (AI), sensor technologies, cloud services, and automated control systems [5]. These systems operate at three interconnected levels and collect and analyze data in real time.

Physical level: At this stage, data is collected through various sensors and devices. Temperature sensors, motion detectors, light sensors, energy monitoring devices, and security cameras monitor the activity of the house. For example, a temperature sensor adjusts the temperature according to weather changes, a motion sensor turns off the lights when no one is in the room, and an energy monitoring device monitors consumption. Thanks to these technologies, energy consumption is reduced to a minimum, and the level of comfort increases.

Network layer: Data is transmitted through IoT communication protocols (ZigBee, LoRaWAN, MQTT, Z-Wave). ZigBee provides short-range communication with low power consumption, while LoRaWAN is suitable for longer distances and finds wide application in rural areas. The MQTT protocol allows reliable data exchange with low bandwidth. Thanks to these systems, all devices in the house can be connected to a central control panel or mobile application.

Cloud layer: Cloud technologies process the collected data and analyze it with AI models. For example, by looking at the user's energy consumption history, the system can suggest new settings for energy saving. Cloud services also enable remote control: the user can monitor and control their home from anywhere in the world through a mobile application [6].

The role of artificial intelligence: Artificial intelligence and machine learning algorithms analyze user behavior to ensure optimal energy management. For example, the system learns the time the user leaves the house every day and automatically reduces the heat, thus reducing energy consumption by up to 25%. AI also optimally adjusts the indoor climate, taking into account weather forecasts. International experience shows that households saved 15% annually on gas and electricity due to the application of the "Nest Learning Thermostat" in the USA [1]. In Europe, Smart Grid technologies have reduced energy loss by 10-12% by balancing energy distribution [7]. As a result of the "E-Energy" project implemented in Germany, energy efficiency in buildings has increased up to 40%. In the reality of Azerbaijan, the implementation of these systems is taking place gradually. The smart meter system implemented by "Azerishiq" OJSC facilitates the monitoring of energy consumption and prevents illegal use [6]. Smart lighting, heating, and security systems are installed in new residential complexes in the capital and regions, which serve to save energy and improve the quality of life.

3. Energy Efficiency and Management Mechanisms

Energy efficiency is one of the main indicators of environmental and economic stability. The International Energy Agency (IEA) states that by 2030, the implementation of intelligent management systems in

buildings can reduce global energy demand by 10% [1]. Energy management in smart homes is formed in four main directions:

Real-time monitoring: Smart meters monitor energy consumption on a second-by-second basis and provide graphical and analytical information to the user. This information increases the transparency of energy behavior and encourages users to save. For example, according to a study conducted in Great Britain, energy consumption was reduced by an average of 18% in homes with a real-time monitoring system installed [1].

Adaptive control: Sensors automatically adjust devices based on indoor temperature, light, and motion [5]. For example, when there is no one in the room, the lights turn off, the curtains close automatically according to the angle of sunlight, and the air conditioner switches to the optimal mode. This process reduces energy consumption and saves electricity costs.

Renewable energy integration: Solar panels, wind turbines, and battery systems are integrated into smart homes [4]. These systems balance energy production, storage, and distribution. Already produced energy can be transferred to the grid or stored in a "home energy bank". In Japan's Panasonic Smart Town project, houses consume 30% less energy per year [3].

Analytical forecasting: AI systems predict future demand by analyzing past energy data, weather forecasts, and usage patterns. It plays an important role, especially in "dynamic regulation of energy price" systems [1].

Houses built on the basis of the "Net Zero Energy" concept in Scandinavian countries produce their own energy and transfer excess energy to the network [7]. Denmark and Sweden are already building "energy positive" buildings, meaning they produce more energy than they consume. For Azerbaijan, these approaches are of strategic importance for the future. In particular, the Nakhchivan and Karabakh regions have high potential in terms of solar energy [4]. The implementation of "greenhouses" and "energy independent villages" projects here is appropriate both from the economic and ecological point of view.

4. Cybersecurity and Data Protection

In addition to the widespread use of smart home systems, information security issues are becoming more and more relevant [8]. The proliferation of IoT devices makes home networks a potential target for cyberattacks. According to the US Cyber Security Agency's 2023 report, 46% of smart home devices have experienced a cyber threat at least once [7].

An in-depth analysis of key cybersecurity risks in smart homes. Although the technologies applied in smart homes make everyday life easier, these systems also create new cybersecurity challenges. The main risks are: weak authentication mechanisms, delay of firmware updates, poor protection of home routers, data leakage in cloud services, and unauthorized connection of devices to the network [9]. Each of these problems should be analyzed from both technical and user behavioral perspectives.

The main risks are:

Weak authentication mechanisms and duplicate passwords

Most smart home systems are equipped with simple and identical passwords during the initial installation phase. For example, many devices store default passwords such as "admin/admin" or "12345". Since most users do not change these passwords, cybercriminals can easily access home systems using this publicly available information [6].

Weak authentication mechanisms are not only related to password simplicity, but also to single-step authentication. If the system does not implement two-factor authentication (2FA), it is almost impossible to prevent cyber attacks.

Attackers use methods such as "credential stuffing" (that is, testing the same passwords on different systems) and "brute-force" (breaking passwords with force). According to a report by Bitdefender in 2023, 45% of attacks on IoT devices were due to password vulnerabilities.

Solutions:

- Strengthening the password policy (at least 12 characters, a combination of letters, numbers, and special characters);
- Application of two-factor authentication (2FA);
- Compulsory change of initial passwords of devices;
- Automatic login blocking (on repeated unsuccessful login attempts).

In the reality of Azerbaijan, awareness among users in this field is still weak. A 2024 report by the Ministry of Energy and Digital Development notes that 68% of users use the same password for multiple accounts on smart devices. This is a serious source of risk.

Delay of firmware updates

Firmware is the software that runs inside the device. Updating this software is important for both functional improvement and security. But many users and some manufacturers do not pay due attention to firmware updates. As a result, vulnerabilities in older versions become an open door for cybercriminals.

As a result of the delay in firmware updates, attacks such as "remote code execution", "data exfiltration", and "botnet connection" occur. For example, in 2016, an attack called the Mirai Botnet connected thousands of vulnerable IoT devices to launch one of the world's largest DDoS attacks. The reason for this attack was outdated firmware and unmodified passwords.

Measures to reduce risks:

- Activating the automatic update mechanism;
- Follow manufacturers' safety notices;
- Providing devices with original firmware (avoid fake versions).

Using reliable servers for updates. The Cyber Resilience Act has been adopted in the European Union since 2022, and according to this law, all manufacturers must provide firmware updates for at least 5 years. It is important to apply such requirements to the devices sold on the Azerbaijani market.

Weak protection of home routers

Home routers are considered the "gateway" of the smart home ecosystem. All smart devices access the internet through this network. When a router is poorly secured, the security of the entire system is compromised. The most common problems:

- An unencrypted “HTTP” interface is used during installation:
- Remote access to the router's control panel remains open;
- Instead of WPA2, the old WEP encryption standard is used.

Firmware updates are not performed. Cyber attackers can use these vulnerabilities to intercept data flows and download malware to devices through man-in-the-middle attacks.

Precautions for safety:

Activation of WPA3 encryption;

Changing the router's default management ports;

Disabling the "Remote Management" function;

Keeping the firewall function active;

Regular checking of router logs.

The US Federal Communications Commission (FCC) has set minimum security requirements for home networks in 2023. These requirements can also be applied in Azerbaijan, especially in newly built "smart housing" projects; manufacturers should be obliged to fulfill these technical norms.

Data leakage in cloud services

Cloud systems play the role of the "brain" of smart homes, because all data (temperature, camera images, energy consumption, user behavior, etc.) is collected here. However, if data protection is not ensured in cloud-based services, large-scale data leaks can occur. The most observed risks:

- Weak encryption of cloud servers;
- Transfer of information to third parties;
- Improper setting of access control;
- Absence of "TLS" (Transport Layer Security) use in device-server connection.

For example, in 2022, as a result of a vulnerability discovered in the cameras of the "Eufy Smart Camera" company, it was possible for third parties to watch user videos. This incident showed that cloud systems, however convenient, require a high level of security.

Solution directions:

- Data encryption at AES-256 or RSA-2048 level;
- "Zero-knowledge" model (only the user can see the information, not the server);
- Data storage on regional servers (in Azerbaijan or the EU);
- Personal data processing according to GDPR principles [9].

In the context of Azerbaijan, it is planned to prepare technical standards on cloud security for state bodies and the private sector within the framework of the "Digital Development Strategy" starting from 2024. This will increase the reliability of smart home services.

Unauthorized connection of devices to the network

Multiple IoT devices can create hundreds of connections in a home network. If these connections are left unattended, cyber attackers can enter the system through "unauthorized access". In particular, home cameras or smart doors can be hacked through "default" open ports (e.g., 23/Telnet and 554/RTSP). The most commonly used attack methods:

- MAC spoofing: An attacker presents their device as a genuine device. Evil twin attack: Deceiving the user by creating a fake Wi-Fi hotspot.
- Device cloning: Access to the system by creating a new device with the same identifier.

Recommended countermeasures:

- Network segmentation - Allocating separate Wi-Fi and VLANs for IoT devices;
- Access control (Access Control Lists - ACL) application; • Track MAC addresses of devices;
- Create a blocking policy for automatically unknown devices on the network.

For example, in South Korea, real-time network monitoring systems are implemented for all smart homes within the framework of the "Smart Home Security Framework". This system immediately detects suspicious connections and sends an alert.

Standardization and international practice

- It is important to apply international standards to prevent these dangers.

- ISO/IEC 27001 - international norm on information security management system; •ISO/IEC 27701 - additional standard on personal data protection;
- NIST Cybersecurity Framework - risk-based approach and action plan;
- GDPR (EU) - principles of legal protection of personal data and transparent processing.

It is important for Azerbaijan to adopt these standards at the national level, prepare the local "Smart Home Security Guideline" document, and hold awareness programs.

Human factors and education

No matter how advanced technology is applied, the human factor is still the weakest link. According to statistics, 70% of users do not change their device's default passwords, and 60% postpone software updates [6]. For this reason, in addition to technical measures, it is also important to form the knowledge and habits of users.

Users should be encouraged to behave safely through awareness campaigns, public social ads, and automatic alerts in mobile applications.

Although these issues are new for Azerbaijan, within the framework of the "Digital Development and Transport Strategy (2022-2026)", the creation of a cybersecurity ecosystem and the improvement of the "CERT.AZ" system have been identified as priority directions [4].

Cybersecurity is not only a technological issue, but also an ethical one. Smart home devices record user behaviors, voices, and even movement patterns. Sharing this information with third parties raises concerns for individual liberties and privacy [9]. Therefore, both the government and the producers must follow the principles of transparency in the collection and use of data.

5. The Role of Artificial Intelligence and Automation

Artificial intelligence (AI) is the basis of the management system of smart homes [5]. AI learns behavioral patterns by analyzing data collected from devices, adjusts energy balance, and ensures safety.

AI-based technologies:

Predictive energy management: The system predicts future energy needs [3]. For example, a system that predicts whether the weather will be cloudy allocates solar energy resources more efficiently.

Security: Performs facial recognition, voice recognition, and motion analysis [8]. The system learns the faces of the residents of the house and gives signals about strangers. At the same time, it can detect unusual sounds (for example, the sound of breaking glass).

Voice control: provides human-machine interaction through the Google Assistant and Amazon Alexa systems [1]. These systems not only execute commands, but can also understand context and provide personalized responses. Automatic fault detection: AI algorithms detect device faults in advance and send alerts. For example, the system notifies the user when there is a pressure drop in the boiler system, an overheated electric cable, or a leak in the water system.

In countries such as Singapore, Korea, and the UAE, AI-based Smart Nation programs are implemented at the state level [7]. All residential buildings in Singapore are equipped with smart energy management systems, which have increased energy efficiency by 25%. For Azerbaijan, it is appropriate to create specialties in universities and promote "startup laboratories" in the direction of AI application [10]. In particular, it is important to develop AI solutions for local conditions, as climate, culture, and user behavior differ across regions.

1. State policy, regulatory framework, and local practice.

2. The "Law on Energy Efficiency" adopted in the Republic of Azerbaijan in 2022 opened a new stage in energy management [4]. The law makes the energy audit and certification process mandatory.

State programs - "Green Energy Zone," "Smart City and Village Concept" - support technological transformation. "Smart grid" systems are being tested in the pilot projects implemented by "Azerishiq" and "Azerenergy" [6]. Intelligent lighting and energy management modules are applied in Ganja and Sumgait. Street lighting in these cities is automatically adjusted depending on the degree of darkness, resulting in a 30-40% reduction in energy consumption.

International cooperation is also important. The "Energy Efficiency 2030" project is implemented jointly with the World Bank and the UN Development Program [3]. Within the framework of this project, technical assistance is provided, training is organized, and pilot projects are financed to increase energy efficiency in Azerbaijan. In the future, the creation of a "green technologies fund" within the framework of the public-private partnership model can stimulate investments in this area. This fund can provide pilot loans, subsidies, and concessional loans for energy efficiency projects.

1. Social, environmental, and ethical aspects.

2. Smart home technologies are important in terms of social welfare and environmental sustainability [3]. For the elderly and physically challenged, these systems increase safety with voice control and emergency alarm functions [1]. For example, people with limited mobility can control the lights, curtains, TV, and open and close the door with voice commands.

From an ecological point of view, smart homes reduce energy waste and carbon emissions by up to 30% [3]. This also plays an important role in the fight against climate change. Smart homes help to use natural resources more efficiently - monitor water consumption, reduce waste, and optimize energy consumption. From a social point of view, these technologies change human behavior and encourage responsible use of energy [2]. Thanks to real-time monitoring, users directly see the results of energy consumption and tend to change their behavior. Ethical aspects are related to personal data processing [9]. Smart devices collect user habits and voices. Legal mechanisms are required for the proper management of these data [8].

Azerbaijan needs to adapt the "Law on Personal Data Protection" to international standards. In particular, the purpose of data collection, the storage period, conditions of sharing with third parties should be clearly defined. 1. Future perspectives and recommendations 2. In the future, smart homes will serve not only energy saving, but also social inclusion, health monitoring, and resource management [1]. In the next decade, smart homes will become energy-positive buildings, generate their own energy, and even provide power for electric cars. The health monitoring system will monitor the health status of the elderly and those suffering from chronic diseases, and will transmit information to doctors and relatives in case of urgent need for help.

6. The Secret to the Popularity of Smart Homes

The Internet of Things (IoT) is not just a fad. There are many factors affecting the growing popularity of smart home devices:

1. Rapid technological evolution. Hardware and software potential are developing every year. Current developments are different from what we knew before, which inevitably affects customer expectations and market transformations.

2. Emerging opportunities in cloud computing. Cloud infrastructure, which is indispensable for Internet of Things (IoT) solutions, is more accessible than ever. Smart home providers can benefit from flexible service options offered by popular cloud platforms such as AWS, Microsoft Azure, and Google Cloud.

3. Mandatory environmental standards. Many developed countries (smart meters) are incorporating smart home solutions into their environmental protection measures.

How to Connect Smart Home Elements?

There are four connection types:

- **Wi-Fi** is considered the most popular communication protocol for IoT devices. Since it is also the protocol that consumes the most energy, devices need to be charged regularly.
- **Bluetooth,** although less common than Wi-Fi, Bluetooth devices are cheaper and consume less energy. Its biggest disadvantage is low connection capacity. All IoT elements need to be positioned closer to each other, and users cannot control IoT systems outside the home.
- **Z-Wave**, It is a low-power consumption mesh network technology that provides high connection speed and allows adding any number of devices to the network. However, the Z-Wave signal only reaches up to 100 meters, so users cannot control their homes remotely.
- **Zigbee** is another affordable, low-power network technology used to connect smart home devices. Zigbee provides secure data transmission using 128-bit encryption keys and controls devices at a distance of 10-100 meters indoors. The Zigbee Alliance currently includes more than 600 companies (such as Siemens, Philips, Bosch, and others). This means that there are thousands of Zigbee-compatible devices, and their number is increasing every year.

7. Content of Smart Home Systems

Smart homes use advanced technology to make life more comfortable, create efficient housing facilities and daily family affairs management systems, and integrate facilities related to daily life. A smart home includes many types of home products; It serves users through smart communication, covering everything such as TV, bathroom, refrigerator, air conditioner, door lock, and other products. Smart home technology provides energy saving as well as security and comfort. Smart home systems will become more common day by day with the advancement of technology. These systems will provide benefits in terms of energy efficiency as well as advantages such as comfort, security, and time saving.

A complete smart home system is not just one device, but a combination of many home products with different functions. The user in a family consists of multiple users, not one person. The goal of smart home systems is to efficiently and intelligently coordinate home products and people into a unified system that can learn, connect, and self-adapt. Compared with interactive buttons and touch screens, voice assistant hardware is more convenient, and voice control has now become an important entry point for smart homes. The most important features of smart home systems are comfort, security, energy saving, and environmental friendliness. Home automation systems in smart homes are determined according to the needs of the people living at home, and the features of each smart home can be designed in a unique way. For example, the expectation of a smart home for disabled and elderly people in need of care is to ensure that health checks can be carried out and they can take their medications properly; the needs of a university student who wants to celebrate at home may include changing the sound system, video systems, and lighting of the house.

8. Healthcare Applications

Smart homes also have numerous applications in healthcare. They can be used to monitor the health and well-being of the inhabitants, particularly the elderly or those with chronic conditions. Devices like smart watches can track vital signs and activity levels, while smart cameras can detect falls or other emergencies. This data can be used to alert healthcare providers or family members in case of any abnormalities.

Furthermore, smart homes can facilitate telemedicine, allowing patients to consult with healthcare providers from the comfort of their homes. This can be particularly beneficial for those with limited mobility or those living in remote areas.

9. Future of Smart Homes

The future of smart homes looks promising, with advancements in technology and a growing awareness of the benefits they offer. As artificial intelligence and machine learning continue to evolve, the automation capabilities of smart homes are expected to become more sophisticated. This could lead to homes that can fully adapt to the habits and preferences of their inhabitants, providing a truly personalized experience.

Furthermore, as more and more devices become connected, the potential applications of smart homes will continue to expand. This could include everything from advanced healthcare monitoring to integrated energy management systems. However, these advancements will also bring new challenges, particularly in terms of privacy, security, and interoperability. Therefore, it will be crucial to address these issues to ensure the successful adoption of smart homes.

10. Use of Artificial Intelligence in Smart Home Systems

Table 1 illustrates the use of AI in smart home systems.

Table 1. Comparison of Artificial Intelligence Applications in Smart Home Systems.

Topic and Purpose	Technology and Feature	Result and Future Recommendation
Using deep learning to monitor daily nutrition [3].	Nutrition data are processed using Optical Character Recognition (OCR). Bayesian methods are used for classification.	A daily accuracy of 96.8% has been achieved. Integration with physiological monitoring systems is recommended to reduce errors and improve automatic diet tracking.
Monitoring system for elderly people using object tracking and sensor-based human-robot interaction in smart homes [7].	The system includes an assistive robot. ASUS Xtion Pro Live RGB-D camera integrated with a robotic wheelchair and a two-wheel robotic platform using BOSCH INDY5 IMU. Amazon Alexa and a deep learning architecture (DESA) are used.	Filtering techniques improve recognition accuracy. Integration with a comprehensive robotic assistant system is recommended.
Gamification system for sharing smart home data among family members and between families [11].	Motion sensors and environmental sensors collect data. GPU and DSP processors accelerate analysis.	Experiments show increased engagement through gamification, although some negative motivational effects were observed.
Detecting network anomalies in smart homes to monitor traffic problems and network security [12].	Machine learning methods detect unusual anomalies and prevent attacks in early stages. Data classification algorithms are applied.	Simulation results show that local anomalies can help identify suspicious network packets.
Using the Telegram application to control home entry-exit monitoring devices [12].	The Raspberry Pi camera module performs face recognition. Arduino and NodeMCU act as communication modules. Histogram and Binary Histogram algorithms are	The system allows monitoring people in front of the house camera. Performance depends on device speed, memory, and internet connection.
Testing artificial intelligence algorithms [13].	Sensor data coming from the smart home is transmitted through a gateway device to an MQTT server and stored in a MySQL database. The simulation process uses these recorded data. Software that enables this process is developed in JavaScript and designed to run in the Node.js runtime environment.	By modifying the simulation algorithm, the system can process real-time data collected from sensors. Artificial intelligence algorithms can be tested in different conditions in both real and virtual environments to evaluate their accuracy.
Examining the components of IoT-based smart home technologies, the motivation behind these technologies, the related issues, and the development of smart homes [14].	Communication protocols such as ZigBee, ZigBee Pro, ZigBee IP, low-power WPANs over IPv6, WiFi, Bluetooth Low Energy, RFID, and cloud computing technologies are used. CoAP, UDP, and HTML5 WebSocket	These components should be monitored and managed properly to ensure secure and reliable operation while reducing energy consumption under different conditions.

	communication protocols are also utilized.	
Customizing homes according to individuals' needs by using smart home decision mechanisms [15].	Integrated Decision Support Systems (IDSS) for smart homes, User-Centered Design (UCD), and Human–Computer Interaction (HCI) approaches are applied.	Future studies should focus on challenges such as sensor fusion, contextual awareness, uncertainty, and security issues in smart home technologies.
Efficient energy use and energy saving in smart homes using IoT-based devices and artificial intelligence [16].	SCADA systems are used to monitor and manage energy production units by different teams. Smart Electronic Devices (IED), mobile-based solutions, and Ethernet-based systems are also used.	IoT-based solutions are considered cost-effective. These hybrid solutions enable electrical energy to be managed efficiently.
Systematically reviewing smart home literature and evaluating the current situation from the perspective of users [17].	Artificial intelligence, sensors, and IoT technologies.	Future research should analyze consumer attitudes and preferences more comprehensively. Most existing studies have been conducted in England and the USA; therefore, future studies should focus more on Eastern countries to better understand the benefits and services of smart homes.
Evaluating new approaches for integrating sensors for applications such as identifying energy consumers and storage, human interaction, and developing wearable technologies using traditional micro-electromechanical system-based microsensors [18].	Triboelectric nanogenerators (TENG), nanogenerators (NG), artificial intelligence (AI), micro-electromechanical systems (MEMS), and High-Profile Bayes Point Machine Test (HPBMT).	Significant research has been conducted to further develop HMI, voice recognition, and IoT-based smart home control systems. Through micro-devices, smart interfaces, and skin-compatible wearable devices, new generation health monitoring systems capable of detecting physical and chemical signals have been proposed.

Recommendations:

- Promoting local "smart device" production: Developing local manufacturers will not only diversify the economy but also reduce dependence on foreign supply chains.
- Expanding energy audit and certification: An energy efficiency certificate requirement should be applied to all new buildings and old buildings undergoing major renovation.
- Applying national cybersecurity standards: Minimum security requirements for smart home devices should be defined, and compliance with these requirements should be made mandatory.
- Creating artificial intelligence centers: Centers specialized in AI research and application should be created in universities and research institutes.
- Formation of educational programs and curricula on smart home technologies: Specialties in the installation, management, and repair of smart home systems should be taught in vocational schools and universities.
- Security awareness campaigns for users: Users should be familiarized with safe usage rules of smart devices through mass media, social networks, and training seminars.

As a result of these measures, Azerbaijan could become one of the leading countries of a "green and digital economy."

11. Conclusion

Smart home technologies are one of the most efficient solutions responding to the energy, safety, and ecological challenges of the modern world. They play a crucial role in energy savings, creating a safe environment, and ensuring ecological sustainability [1].

For Azerbaijan, this direction holds strategic importance. The state's "green energy", "digital transformation", and "smart city" policies form a solid base in this field [4].

Successful results are possible not with the import of technology, but with the development of a local knowledge base, human resources, and security infrastructure [10].

In the future, smart homes will become one of the main infrastructure elements, ensuring not only energy savings but also social welfare, safety, and sustainable development [3].
The widespread dissemination of these technologies will be a step towards a cleaner, more efficient, and fairer energy future. Azerbaijan's active participation in this process will strengthen the country's energy independence, improve its ecological situation, and help increase citizens' quality of life.

Author Contributions

Shokrollah Ghadyani is solely responsible for the conceptualization, literature review, analysis, and writing of the manuscript, and approved the final version for publication.

Conflict of Interest

The author declares no conflicts of interest.

Funding

This research received no external funding.

Acknowledgment

The author would like to thank Tekdata Co. (Tehran, Iran) for its support during the preparation of this manuscript.

References

[1] EA, U. E. P. (2022). International Energy Agency, 2022. *Buildings-Energy System-IEA*.
[2] Hüseynova, A., Əslamov, R., & Mahmudova, N. (2023). *Əşyaların interneti: İnkişaf komponentləri və tətbiq sahələri*. Bakı, Azərbaycan.
[3] United Nations Environment Programme. (2022). Global status report for buildings and construction. https://www.unep.org
[4] Ministry of Energy of the Republic of Azerbaijan. (2024). Renewable energy and green energy development targets for 2030 (policy framework). Baku, Azerbaijan.
[5] Qasımov, E. (2024). *Artificial intelligence and smart technologies*. Baku, Azerbaijan: Elm Publishing House.
[6] Azərişıq Açıq Səhmdar Cəmiyyəti. (2023). Ağıllı sayğac sistemlərinin tətbiqi təcrübəsi. Bakı, Azərbaycan.
[7] Sundaravadivel, P., Kesavan, K., Kesavan, L., Mohanty, S. P., & Kougianos, E. (2018). Smart-log: A deep-learning based automated nutrition monitoring system in the IoT. *IEEE Transactions on Consumer Electronics*, *64*(3), 390-398.
[8] International Organization for Standardization/International Electrotechnical Commission, J. (2022). ISO/IEC 27001: 2022—Information security management systems. *URL: https://www. iso. org/standard/27001*.
[9] European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] Azərbaycan Respublikasının Dövlət Şəhərsalma və Arxitektura Komitəsi. (2024). Rəsmi veb sayt. https://arxkom.gov.az
[11] Erol, B. A., Majumdar, A., Lwowski, J., Benavidez, P., Rad, P., & Jamshidi, M. (2018). Improved deep neural network object tracking system for applications in home robotics. In *Computational Intelligence for Pattern Recognition* (pp. 369-395). Cham: Springer International Publishing.
[12] La Tona, G., Luna, M., Di Piazza, A., & Di Piazza, M. C. (2019). Towards the real-world deployment of a smart home ems: A dp implementation on the raspberry pi. *Applied Sciences*, *9*(10), 2120.
[13] Bicakci, S., & Gunes, H. (2020). Hybrid simulation system for testing artificial intelligence algorithms used in smart homes. *Simulation Modelling Practice and Theory*, *102*, 101993.
[14] Zaidan, A. A., & Zaidan, B. B. (2020). A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. *Artificial Intelligence Review*, *53*(1), 141-165.
[15] Mekuria, D. N., Sernani, P., Falcionelli, N., & Dragoni, A. F. (2021). Smart home reasoning systems: a systematic literature review. *Journal of Ambient Intelligence and Humanized Computing*, *12*(4), 4485-4502.
[16] Singh, P. P., Khosla, P. K., & Mittal, M. (2019). Energy conservation in IoT-based smart home and its automation. *Energy conservation for IoT devices: concepts, paradigms and solutions*, 155-177.
[17] Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change*, *138*, 139-154.
[18] Haroun, A., Le, X., Gao, S., Dong, B., He, T., Zhang, Z., & Lee, C. (2021). Progress in micro/nano sensors and nanoenergy for future AIoT-based smart home applications. *Nano Express*, *2*(2), 022005.