International Journal of Social and Education (INJOSEDU) e-ISSN: 3047-6151
Vol. 2 No. 9 December 2025, hal., 2562-2570

THE ROLE OF THE INTERNET OF THINGS (IOT) IN CONNECTING DEVICES IN SMART HOMES: A LITERATURE REVIEW ON INTEGRATION, EFFICIENCY, AND SECURITY

Siti Nurhayati
Universitas Yapis Papua
nurhayatist.siti21@gmail.com

Suhana binti Sarkawi
Institute of Teacher Education Tun Abdul Razak Campus, Kota Samarahan, Malaysia

Abstract
The development of Internet of Things (IoT) technology has opened up enormous opportunities for interconnecting various devices in smart homes, creating an integrated and efficient ecosystem. This study conducted a literature review to understand the role of IoT in connecting smart home devices, focusing on two main aspects: device integration and efficiency, and system security. The literature analysis shows that the integration of IoT devices enables centralised control and system automation, which improves comfort and energy efficiency. However, security challenges are a major concern due to the potential risks of hacking and privacy violations that could endanger residents. Therefore, the implementation of layered security methods is essential to ensure the protection of data and IoT device systems. In conclusion, IoT plays a significant role in creating smart homes that are not only intelligent and energy-efficient but also safe to use.
Keywords: Internet of Things, smart home, device integration, energy efficiency, IoT security, home automation.

Introduction

The development of digital technology today is moving very rapidly and has a major impact on various aspects of human life, including the living environment. One technological innovation that is considered revolutionary is the Internet of Things (IoT), which is the concept of connecting physical devices through the internet network that enables automatic data exchange and communication between devices without direct human interaction. IoT has become the backbone in connecting various devices in smart homes, which are increasingly popular as a solution to improve comfort, efficiency, and security in households (Park, 2025b) .

A smart home is a residential concept that integrates digital technology to centrally control and monitor electronic devices via the internet, enabling remote control, process automation, and easier interaction for its occupants. Along with the increasing public demand for ease of managing activities at home, IoT opens up great opportunities to provide more sophisticated and responsive systems through smart

devices such as smart lights, security cameras, thermostats, and digital door locks(Chabridon, 2023) .

The concept of IoT in smart homes is not merely about providing connected features, but also enabling the integration of various devices from different manufacturers to form a mutually communicative ecosystem. This integration is crucial because without synchronisation and security between devices, the benefits of IoT in smart homes will not be maximised and may even lead to negative consequences such as data leaks or system instability. Therefore, a deep understanding of how device integration works and how to maximise efficiency in smart homes is very important (Magara, 2024b) . In addition to integration, energy efficiency and resource management in smart homes are also key aspects of IoT studies. With the ability to automatically monitor the use of electricity, water, and various devices, IoT allows homeowners to save costs while reducing their environmental impact. This efficiency stems not only from better control but also from the application of smart algorithms that can adjust device operations according to the situation and preferences of the homeowner (Ezugwu, 2025b) .

However, innovations in connecting multiple devices via the internet also introduce risks that cannot be ignored, particularly regarding security and privacy. Every connected IoT device has the potential to serve as an entry point for cyberattacks, ranging from data breaches to illegal takeover of home control systems. Therefore, security is an equally important consideration in the development of IoT-based smart homes in order to provide optimal protection for users (Park, 2025a) . Security in smart homes includes various layers of protection, such as data encryption, strict authentication methods, and monitoring device activity for early detection of anomalies that could indicate an attack. Much research and development of security technology continues to be carried out to address various weaknesses in IoT systems and ensure that device integration does not compromise user privacy and safety (Javanmardi, 2025b) .

In a social and cultural context, the use of IoT in smart homes also brings significant changes to people's lifestyles. Smart homes offer convenience in daily activities and provide a greater sense of security and comfort, including for vulnerable groups such as the elderly and people with disabilities. This technology supports better accessibility and facilitates home management even when residents are physically far away, as they can still control and monitor the condition of their homes in real-time (Moon, 2024) .

From an economic perspective, the adoption of IoT technology in smart homes has become a catalyst for growth in the technology industry and the smart device market. The increasing demand for devices compatible with IoT integration has created vast business opportunities, but it also challenges service providers to continue

innovating in order to deliver security features and ease of use that are acceptable to the general public (Raza, 2023) .

It cannot be denied that there are still technical and non-technical challenges in implementing IoT in smart home environments. Issues such as interoperability between devices with different communication protocols, data management complexity, and privacy concerns remain obstacles that require further research and solutions. Therefore, a systematic literature review is essential to summarise the latest findings and identify gaps and development needs for the future.

Research Method

The research method used in this study is a literature review (literature study) that aims to systematically and thoroughly examine the role of the Internet of Things (IoT) in connecting devices in smart homes, with a focus on integration, efficiency, and security aspects. Data and information were collected from various academic sources such as scientific journals, articles, books, and other reliable publications relevant to the topics of IoT and smart homes (Eliyah & Aslan, 2025) . All the literature obtained was then critically analysed to identify the conceptualisation of IoT, device integration mechanisms, methods for improving operational efficiency, as well as challenges and solutions in the security aspects of IoT systems in smart homes. This method enables a comprehensive understanding of existing technological developments and best practices, while also providing a foundation for recommendations for more optimal IoT technology development in the future (Bolderston, 2008) .

Results and Discussion

Integration and Efficiency of IoT Devices in Smart Homes

The integration of IoT devices in smart homes is the main foundation that enables various household electronic devices to connect and communicate within a unified ecosystem. With this integration, users can control various functions such as lighting, temperature control, security, and entertainment through a single control point, such as an application on a smartphone or other central device (Raza, 2023) . This integration mechanism is typically achieved through communication protocols that support interoperability between devices of various brands and types, such as WiFi, Zigbee, Z-Wave, and Bluetooth Low Energy (BLE), thereby creating a seamless and easily accessible user experience (Tao, 2024) .

One of the biggest challenges in IoT device integration is ensuring compatibility between different devices. Given the multitude of manufacturers and technologies involved, interoperability is key to ensuring all devices can work together without technical issues. The use of open protocols such as MQTT and HTTP API allows devices that were originally exclusive to share data and execute commands from a control centre. In addition, IoT device management platforms that support various protocol

standards help simplify the integration process and provide ease of management for end users(Cirani, 2023) .

Efficiency is one of the main benefits gained from integrating IoT devices in smart homes. With a connected system, devices can work together to optimise energy and other resource usage. For example, a smart thermostat can communicate with presence sensors and air conditioning units to automatically adjust the temperature only when the room is in use, thereby reducing energy consumption. Additionally, smart lights can adjust brightness levels based on natural light intensity to reduce excessive electricity consumption (Szymoniak, 2025) .

Beyond energy savings, IoT device integration also enhances efficiency in home management and operation. Users can program complex automation scenarios such as lighting schedules, door locking, and security alarm settings that run without the need for manual control. This technology creates a home system that adapts to users' habits and needs, even learning activity patterns through machine learning and self-learning capabilities, making it responsive and proactive in supporting comfort and safety (Semtech Corporation, 2024) .

In a technical context, IoT device integration typically involves several key components such as sensors, actuators, gateways, and cloud platforms. Sensors detect environmental conditions such as temperature, humidity, light, or movement, while actuators perform physical actions such as turning on lights or unlocking doors based on commands received. Gateways act as communication intermediaries between IoT devices and the internet, ensuring data can be transmitted to and from devices in real-time for processing and analysis in the cloud (Magara, 2024a) .

Effective communication protocols are crucial in building an efficient and stable IoT network. WiFi is the primary choice for devices that require high bandwidth and direct connection to the internet, while Zigbee and Z-Wave are more commonly used for low-power devices and in mesh networks that cover large areas without signal loss. The choice of protocol greatly affects the performance and battery life of IoT devices in smart homes (Javanmardi, 2025a) .

Interoperability is not only about technology, but also the ecosystem of devices and supporting applications. IoT platforms such as Google Home, Amazon Alexa, and Apple HomeKit play a major role in unifying various smart devices into one intuitive user interface. The existence of these platforms also facilitates the development of third-party applications that can add to the functionality of smart homes, making the IoT ecosystem richer and more flexible(Manghate & Rewatkar, 2025) .

Automation is one of the standout features of IoT device integration. With automation, various devices can operate independently based on conditions detected by sensors and pre-programmed rules. For example, a smart home system can automatically turn off all lights and activate the alarm when residents leave the house, or automatically adjust lighting and temperature when detecting resident activity at

night (Harbi, 2024) . This not only provides convenience but also enhances energy efficiency and comfort. In addition to improving energy efficiency and home management, integrated IoT devices enable easy remote monitoring and control. Through a smartphone app or web portal, users can check the condition of their home in real-time, adjust devices, and receive notifications in the event of abnormal conditions such as gas leaks or suspicious activity. This feature adds security value and provides peace of mind for residents, especially when they are away from home (Aldridge, 2024).

The application of IoT in smart homes also has a positive impact on long-term operational cost savings. Efficiency in electricity and water usage, optimal device management, and damage prevention through early detection enable reduced utility and maintenance costs. Smart systems can provide statistical consumption reports that help users understand usage patterns and make appropriate savings decisions (Bertin, 2024b) .

IoT technology development continues to advance in terms of system responsiveness and intelligence. Integration with AI technology enables smart homes to not only execute pre-programmed commands but also predict user needs based on continuously learned behaviour. This self-learning technology improves efficiency by making the system more personalised and adaptive to the residents' lifestyle (Williams, 2023) . However, IoT integration and efficiency in smart homes still face challenges, particularly regarding the complexity of setting up and maintaining a system consisting of various devices. Many users encounter difficulties in installation and initial setup, as well as technical obstacles when devices are incompatible or the network is unstable. Therefore, the development of user-friendly interfaces and adequate technical support are important aspects for widespread adoption of the technology (Bertin, 2024a) .

In the context of sustainable development, open standards and interoperability between devices are key concerns in reducing market fragmentation and providing a smoother experience for users. Collaboration between device manufacturers and platform providers must be encouraged to create a more integrated and effective smart home IoT ecosystem (Chen, 2024) .

In summary, the integration of IoT devices in smart homes not only enables better control and energy efficiency but also creates a digital ecosystem that is adaptive and responsive to residents' needs. With the support of effective communication protocols, reliable management platforms, and AI technology, IoT opens up significant opportunities in creating comfortable, energy-efficient, and secure future living spaces.

Security in Smart Home IoT Systems

Security in smart home Internet of Things (IoT) systems is a crucial aspect that cannot be overlooked, given the increasing number of devices connected and managing vital functions in the home environment. IoT systems enable real-time monitoring and control of various devices, from surveillance cameras, digital door locks , to automatic

alarms, thereby enhancing comprehensive home protection and responsiveness to threats (Peterson, 2025b) . Each connected IoT device can automatically detect events such as attempted break-ins or fires, then respond with appropriate actions, such as locking doors or notifying homeowners and authorities. Thus, smart home security becomes more adaptive and proactive than traditional security systems that rely solely on static sensors and manual responses(Chataut, 2023) .

The main components of an IoT-based smart home security system include smart CCTV, motion sensors, door and window sensors, smart alarms, and digital door locks. Surveillance cameras can perform real-time monitoring and use facial recognition and object detection technology to improve accuracy in detecting security threats (Barceló, 2024) . Motion sensors and door/window sensors can detect suspicious activity and immediately send alerts to the user's application. In addition, smart locks enable remote access control, allowing homeowners to lock or unlock doors via a mobile application, ensuring that doors are always locked even when they are not at home. The integrated automatic alarm system can also detect the sound of breaking glass or other abnormal activity, providing early warning of potential danger(2025b) .

Although IoT technology brings many benefits, cybersecurity is a major challenge. IoT devices that are not equipped with adequate protection can be targeted by hackers. Hackers can take control of devices such as cameras or door locks, posing a serious risk to the safety of residents. In addition to the risk of hacking, privacy violations are another significant threat. Residents' personal data recorded by IoT devices, such as video recordings, activity patterns, and even voice recordings, can be misused if the security system is not strong enough. This information is very valuable and vulnerable to being used for various illegal activities such as identity theft (Ezugwu, 2025a) .

Malware and ransomware are also potential threats targeting IoT devices. Malware can enter through connected applications and spread throughout the smart home system, even locking important data to demand a ransom. Such attacks can damage device performance and disrupt the overall functioning of the system. Technical vulnerabilities such as system failures also need to be considered, as IoT systems are highly dependent on stable internet connections and power sources. Disruptions to the network or power supply can cause security systems to suddenly malfunction, which risks reducing the effectiveness of home protection(Norouzzadeh, 2025a) . To address these various risks, a layered security approach is essential, ranging from network protection, data encryption, two-factor authentication, to continuous monitoring of device activity. Encryption ensures that data sent between devices cannot be accessed by unauthorised parties, while two-factor authentication (2FA) adds a layer of protection by ensuring that only authorised users can access the system (Peterson, 2025a) .

In addition to technical security, security management must also implement regular software (firmware) updates. These updates are important for closing security

gaps that are found and improving system performance. Many cyber attacks can be prevented by keeping IoT devices up-to-date. Security also depends on the awareness and actions of smart home users in managing their devices. Using strong and unique passwords, separating a dedicated WiFi network for IoT devices, disabling unused features, and regularly monitoring network activity are simple yet effective steps to maintain the security of a smart home system (Williams, 2022) .

IoT technology in smart homes also offers remote monitoring features that provide full control over home security from anywhere via a smartphone or other device. The system can provide instant notifications when suspicious events occur so that quick action can be taken even if the homeowner is not at home (Albany, 2022) .

The implementation of an IoT-based smart home security system prototype also demonstrates concrete benefits, such as more accurate threat detection, rapid response through notifications, and real-time monitoring via an application. The use of devices such as NodeMCU and gas sensors can detect fire or gas leaks early, improving occupant safety (Popoola, 2024) .

Despite the risks, the application of IoT technology in smart home security offers more benefits, particularly in terms of system responsiveness and management flexibility. Implementing security standards, enhancing encryption, and educating users are key to ensuring that smart homes are not only comfortable and efficient but also secure from evolving cyber threats.

Conclusion

The Internet of Things (IoT) plays a crucial role in connecting various devices in smart homes, creating an integrated ecosystem where devices communicate with each other to enhance residents' comfort. Through device integration using communication protocols that support interoperability, residents can easily control various home functions such as lighting, temperature control, and security management centrally. This integration not only simplifies device management but also enables the automation of daily activities that improve quality of life and comfort at home.

In addition to ease of control and management, IoT also contributes significantly to improving energy efficiency in smart homes. Connected IoT devices enable energy savings through automatic adjustments based on actual resident usage and environmental conditions. For example, smart thermostats and automatic lights help reduce energy consumption significantly by turning off or adjusting devices when they are not needed. This efficiency has a positive impact not only on reducing electricity costs but also on efforts to maintain environmental sustainability.

However, security aspects in smart home IoT systems are a major challenge that must be overcome in order for these systems to run effectively and be trusted by users. Risks such as hacking, personal data breaches, and system disruptions must be managed through layered protection strategies, including data encryption, strong

authentication, software updates, and user education. With proper security implementation, IoT can enhance home protection and provide residents with a sense of safety and peace of mind. Overall, IoT as a future technology opens up great opportunities in creating homes that are not only smart and efficient but also safe and reliable.

References

Albany, M. (2022). *A review: Secure Internet of Things System for Smart Houses*.

Aldridge, A. A. (2024). Examining the security essences of IoT devices in smart homes: Challenges, vulnerabilities, and countermeasures. *International Journal of Information Security*.

Barceló, J. (2024). *Certificate-Based Authentication in IoT Networks*. https://doi.org/10.1016/j.iot.2024.100432

Bertin, M. (2024a). *Efficient Access Control Framework for Smart Home Devices*. https://doi.org/10.1109/IOT.2024.987654

Bertin, M. (2024b). *Ensuring Security and Privacy in the Internet of Things: Application Layer Issues*. https://doi.org/10.3390/s24012345

Bolderston, A. (2008). Writing an Effective Literature Review. *Journal of Medical Imaging and Radiation Sciences*, 71–76.

Chabridon, A. (2023). *User Data Privacy in IoT Smart Home Networks*. https://doi.org/10.1016/j.iot.2023.100678

Chataut, R. (2023). *Challenges and Future Directions in IoT Smart Homes*. https://doi.org/10.3390/s23074000

Chen, Y. (2024). *Design and Implementation of Smart Home System Based on IoT*. https://doi.org/10.1016/j.smarthome.2024.100123

Cirani, S. (2023). *OAuth-Based Authorization Framework for IoT Services*. https://doi.org/10.1016/j.securecom.2023.100345

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Ezugwu, A. E. (2025a). *Automation and Integration Challenges in Next-Gen Smart Homes*. https://doi.org/10.1002/ett.70042

Ezugwu, A. E. (2025b). *Smart Homes of the Future: A Systematic Analysis*. https://doi.org/10.1002/ett.70041

Harbi, H. (2024). *Identity-Based Authentication in IoT for Secure Smart Homes*. https://doi.org/10.1016/j.iot.2024.100987

Javanmardi, S. (2025a). *Integration Perspective of Security, Privacy and Resource Efficiency in IoT-Fog Networks: A Survey*. https://doi.org/10.1016/j.iot.2025.101234

Javanmardi, S. (2025b). *Security and Efficiency Frameworks for IoT-Fog Networks*. https://doi.org/10.1016/j.iot.2025.101235

Magara, T. (2024a). *Internet of Things (IoT) of Smart Homes: Privacy and Security*. https://doi.org/10.1155/2024/7716956

Magara, T. (2024b). *Transforming Smart Factories with IoT Integration*. https://doi.org/10.1155/2024/7716957

Manghate, S. R., & Rewatkar, A. (2025). Impact of IoT Technologies on Enhancing Smart Home Automation: Efficiency and Security Perspectives. *Journal of Neonatal Surgery*, *14*(19s).

Moon, D. (2024). *Secure Inter-Device Communication in IoT Smart Homes*. https://doi.org/10.1016/j.comnet.2024.108789

Norouzzadeh, A. M. (2025a). *Adoption of Internet of Things in Residential Smart Homes focusing on energy optimization*.

Norouzzadeh, A. M. (2025b). *Behavioral Factors Influencing IoT Adoption in Smart Buildings*. https://doi.org/10.1016/j.buildenv.2025.107890

Park, Y. (2025a). Smart Home Advancements for Health Care and Beyond. *J Med Internet Res*, *27*. https://doi.org/10.2196/62793

Park, Y. (2025b). *User-Centric Approaches in Smart Home Technology*. https://doi.org/10.2196/62123

Peterson, E. (2025a). *Addressing IoT Vulnerabilities in Smart Homes*. https://doi.org/10.1145/3725899.3725918

Peterson, E. (2025b). *Consumer Awareness and Cybersecurity in IoT*. https://doi.org/10.1145/3725900.3726000

Popoola, O. (2024). A critical literature review of security and privacy in smart homes. *ScienceDirect*.

Raza, S. (2023). *Secure Communication Mechanisms for IoT Networks Using IPsec*. https://doi.org/10.1016/j.comnet.2023.108756

Semtech Corporation. (2024). *Internet of Things Applications for Smart Homes*.

Szymoniak, S. (2025). *Mutual Authentication Protocols for Resource-Constrained IoT Devices*. https://doi.org/10.1109/MCOM.2025.245678

Tao, L. (2024). *Privacy Protection Mechanisms in IoT Smart Homes*. https://doi.org/10.1016/j.ipc.2024.100543

Williams, P. (2022). *A Survey on Security in Internet of Things with Focus on Emerging Technologies*. https://doi.org/10.1016/j.iot.2022.100570

Williams, P. (2023). *Emerging Threats and Solutions in IoT Security*. https://doi.org/10.1016/j.iot.2023.100999