International Journal of Social and Education (INJOSEDU) e-ISSN: 3047-6151
Vol. 2 No. 8 October 2025, hal., 2497-2505

EXPLORING THE CONVERGENCE OF IOT AND SMART HOME TECHNOLOGIES: A LITERATURE REVIEW OF INTEGRATION AND INNOVATION PATHWAYS

Mira Wellya Fatma
Politeknik Negeri Padang
mirawellya@pnp.ac.id

Maresa Prasafitri
Politeknik Negeri Padang
maresa@pnp.ac.id

Al Amin
Department of Islamic Economics, Faculty of Economics and Business, Universitas Airlangga, Surabaya, Indonesia.
Department of Economics and Business, Universitas Islam Negeri Bukittinggi, Bukittinggi, Indonesia
al.amin-2024@feb.unair.ac.id

Abstract

Purpose – This study aims to explore the convergence of Internet of Things (IoT) and smart home technologies through a systematic literature review. The main objective is to identify key integration frameworks, interoperability challenges, security and privacy issues, and emerging innovation pathways that shape the evolution of IoT-based smart home ecosystems. **Design/Methodology/Approach** – A Systematic Literature Review (SLR) approach was employed following the PRISMA protocol. Academic publications indexed in Scopus, IEEE Xplore, and ScienceDirect from 2013 to 2024 were systematically screened. Inclusion criteria focused on studies addressing IoT-smart home integration, interoperability, efficiency, security, and innovation. Data were analyzed qualitatively using thematic content analysis to extract major research themes and identify research gaps. **Findings** –The review identifies four dominant research themes: (1) Architectural integration leveraging sensing, networking, and application layers with cloud and edge computing; (2) Interoperability challenges due to fragmented platforms and lack of global standards; (3) Security and privacy concerns involving data breaches, unauthorized access, and system vulnerabilities; and (4) Technological innovation driven by Artificial Intelligence (AI), Machine Learning (ML), blockchain, and 5G technologies. Despite significant progress, the literature highlights the need for adaptive integration frameworks, AI-based security mechanisms, and empirical evaluation of hybrid IoT–AI–Blockchain systems. **Originality/Value** – This study provides a comprehensive synthesis of recent advances in IoT-smart home research, mapping existing frameworks and identifying unresolved issues. It contributes to the body of knowledge by offering a conceptual foundation for future interdisciplinary research, practical implementation strategies, and policy development for secure, efficient, and user-centric smart home ecosystems.

Keywords – *Internet of Things (IoT); Smart Home; Systematic Literature Review; Integration; Interoperability; Security; Artificial Intelligence; Blockchain; Innovation Pathways.*

Introduction

The rapid development of digital technology has given birth to a significant transformation in the way humans interact with the environment in which they live. One of the manifestations of this transformation is the emergence of smart homes, which are household systems that utilize digital technology to optimize comfort, energy efficiency, and safety for residents. The integration of the Internet of Things (IoT) as the backbone of this system allows various devices to communicate with each other and operate automatically through the internet network. The concept of smart homes is no longer just futuristic, but has become a tangible part of the smart city ecosystem and global digital transformation (Zhang et al., 2022).

IoT plays a crucial role in building connectivity between devices, such as sensors, actuators, and home appliances that are capable of collecting and exchanging data in real-time. Through this integration, smart homes can improve energy efficiency, minimize operational costs, and strengthen security through smart monitoring systems (Al-Fuqaha et al., 2015). Additionally, IoT allows users to remotely control devices and implement machine learning algorithms to tailor individual preferences, thus providing a more personalized experience (Perera et al., 2015).

While various benefits have been identified, challenges in integration between platforms and devices are still a major concern. The fragmentation of the IoT ecosystem hinders interoperability, while the lack of universal standards creates bottlenecks in scalability and security (Sadeghi et al., 2015). The reliance on various communication protocols and the diversity of devices makes it difficult to achieve a seamless and secure connection. Therefore, literature studies that map integration and innovation approaches are important to understand the direction of sustainable smart home ecosystem development.

In addition to technical integration, security and privacy aspects are also critical issues in the application of IoT in smart homes. Connected systems are widely vulnerable to cyberattacks, data leaks, and user privacy breaches (Roman et al., 2018). With the increasing volume of data collected from household activities, strong encryption mechanisms, authentication, and data governance policies are needed. The inability to guarantee security can lower user trust levels and hinder widespread adoption of technology (Lin & Bergmann, 2016).

Innovations in system architecture, artificial intelligence algorithms, and the use of cloud computing and edge computing are key to overcoming existing technical limitations. This kind of innovative approach not only improves the performance and efficiency of the system, but also opens up opportunities for new business models and user-oriented solutions (Gubbi et al., 2013). A systematic review of the current literature can uncover key innovation trends and identify research gaps that need to be bridged to accelerate the convergence of IoT and smart home technologies.

Based on this context, this study aims to explore the convergence between IoT and smart home technology, focusing on the evolving pathways of integration and innovation

in the academic literature. Through a literature review approach, this article identifies key trends, challenges, and opportunities in system integration, operational efficiency, and data security. The findings are expected to contribute to the development of more adaptive and secure architectures, as well as the basis for future research agendas in the field of IoT-based smart homes.

Literature Review

The Concept and Evolution of IoT in Smart Home

The concept **of the Internet of Things (IoT)** is rooted in the idea of connecting physical devices to a digital network to exchange data and enable automated interactions without human intervention. IoT is the main foundation in the development of **smart homes**, which are oriented towards energy efficiency, user comfort, and improving quality of life (Gubbi et al., 2013). The implementation of IoT in smart homes enables the automation of functions such as lighting, temperature, security, and energy management through interconnected sensors and actuators (Al-Fuqaha et al., 2015). This trend marks a paradigm shift from conventional home systems to smart ecosystems that operate on a data-driven basis.

Integration of Architecture and Supporting Technologies

Recent literature shows that the integration of IoT architecture in smart homes involves three main layers: the sensing layer, the network layer, and the application layer (Perera et al., 2015). Supporting technologies such as cloud computing and edge computing play an important role in processing data efficiently and reducing system latency (Roman et al., 2018). In addition, the use of *middleware* is a solution to overcome system fragmentation due to the diversity of communication devices and protocols (Gong et al., 2023). However, there is no universal integration model that is able to guarantee full interoperability across platforms, which is a significant research gap.

Interoperability and Standardization Challenges

Although the potential of IoT in smart homes is enormous, the main challenge lies in the interoperability between devices from different manufacturers and platforms (Alaa et al., 2017). The absence of global standards makes it difficult to develop systems scalably and compatiblely. Some studies propose the use of *open-source frameworks* and standard protocols such as MQTT and CoAP to improve cross-platform communication (Zhang et al., 2022). However, the literature also suggests that application in the field is still limited due to cost, compatibility, and industry resistance to standardization.

Security and Privacy Issues

Security and privacy aspects are fundamental challenges in the convergence of IoT and smart homes. Intensively interconnected systems have the potential to increase the risk of cyberattacks, such as *data breaches*, *unauthorized access*, and device manipulation (Lin & Bergmann, 2016). A study by Sadeghi et al. (2015) highlights the importance of a

security-by-design approach, including the use of end-to-end encryption, multi-factor authentication, and role-based access management. However, existing solutions often focus on a technical level without considering aspects of user behavior and awareness of digital security risks.

Technological Innovation and Future Trends

Recent innovations in this field include the integration of Artificial Intelligence (AI) and Machine Learning (ML) to support adaptive decision-making in smart home systems (Lee & Lee, 2020). The use of AI allows for predictions of user behavior and automatic adjustments of the system to individual preferences. In addition, the adoption of **blockchain technology** is beginning to be explored as a solution to increase transparency and trust in smart home data management (Zhang et al., 2022). This combination of innovations is expected to overcome the traditional limitations of conventional IoT architectures.

Research Gap and Development Direction

From the various studies that have been reviewed, there is still a research gap in terms of developing a comprehensive and sustainable integration framework. Most of the literature focuses on technical aspects, while social, economic, and policy aspects have not been extensively studied. A multidisciplinary approach involving user-centered design, innovative business models, and regulations that support an open and secure ecosystem is needed (Gubbi et al., 2013; Gong et al., 2023). Follow-up studies need to be directed at the development of interoperable architectures, AI-based security models, and measurement of the socio-economic impact of the implementation of IoT-based smart homes.

Research Methods

Research Approach

This study uses the Systematic Literature Review (SLR) approach to identify, evaluate, and analyze the scientific literature that discusses the convergence between the Internet of Things (IoT) and smart home technology. The SLR approach was chosen because it provides a systematic and transparent structure in collecting and synthesizing findings from various academic sources in order to gain a comprehensive understanding of emerging trends, challenges, and innovation pathways (Kitchenham & Charters, 2007). This method also allows researchers to identify research gaps and propose relevant future research directions.

Review Process and Stages

The SLR stage is carried out following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guideline which includes four main steps: (1) *identification*, (2) *screening*, (3) *eligibility*, and (4) *inclusion* (Moher et al., 2009). At the

identification stage, the researchers collected articles from reputable databases Scopus, IEEE Xplore, and **ScienceDirect**. The screening process is carried out based on the suitability of the title and abstract with the research topic. Irrelevant or duplicate articles are eliminated. The feasibility stage ensures the article meets the inclusion criteria, while the final stage produces a set of studies to be analyzed.

Literature Search Strategy

The search strategy is carried out using a combination of keywords: *("Internet of Things" OR "IoT") AND ("Smart Home" OR "Home Automation") AND (Integration OR Interoperability OR Security OR Innovation).* The search focused on English-language articles published between 2013 and 2024, as this period reflects a pivotal decade in the development of IoT and the adoption of smart home technology. In addition, only articles from reputable Scopus indexed journals and conferences are included to guarantee the scientific quality of the data sources.

Inclusion and Exclusion Criteria

Inclusion criteria include: (1) articles that discuss IoT integration in the context of smart homes; (2) articles that review aspects of interoperability, efficiency, security, or innovation; and (3) studies with clear methodologies such as reviews, surveys, or comparative analysis. Meanwhile, the exclusion criteria include: (1) non-scientific articles such as opinion or editorials; (2) non-specific research on the domain of smart homes; and (3) publications that are not available in full *text*.

Data Analysis Techniques

The collected data is analyzed qualitatively through *a content analysis process* to identify key themes, research trends, and innovative approaches that emerge from the literature. Each article is coded based on the focus of the study (e.g. integration of architecture, security, interoperability, or technological innovation). The results of the analysis are then synthesized into thematic tables and narrative summaries that describe the relationship between the concept and the direction of research evolution (Snyder, 2019). In addition, *literature mapping* is used to visualize the relationship between the topic and the research period.

Validity and Reliability

To ensure the validity and reliability of the study results, the researcher applied a double verification process to the selection of articles and categorization of themes. Two independent researchers conducted a literature screening, and differences of opinion were resolved through discussion until a consensus was reached. The triangulation approach is used by comparing findings from multiple sources and ensuring consistency of analysis results. Thus, the results of this study are expected to represent the current conditions of the convergence of IoT and smart homes with a high level of reliability

Results and Discussion

Overview of Findings

From the literature screening process using the PRISMA protocol, 30 scientific articles published in 2013–2024 were obtained that met the inclusion criteria. The articles are mostly from reputable journals such as *IEEE Communications Surveys & Tutorials*, *Future Generation Computer Systems*, and *Journal of Network and Computer Applications*. Based on the results of the content analysis, four main themes were found in the literature: (1) integration of architecture and technology, (2) interoperability and standardization, (3) security and privacy, and (4) innovation and future direction. Each theme represents a critical dimension in understanding the convergence of IoT and smart homes.

Architecture and Technology Integration

Most studies highlight that the successful implementation of smart homes is highly dependent on the integration of IoT architectures consisting of *sensing layer*, *network layer*, and *application layer* (Gubbi et al., 2013; Al-Fuqaha et al., 2015). The use of cloud computing and edge computing is a key strategy in real-time data processing and latency reduction (Roman et al., 2018). A study by Gong et al. (2023) shows that *middleware-based* integration can overcome fragmentation between devices. However, despite significant advances in technical integration, the literature still shows a lack of alignment between architectural aspects and end-user needs, especially in the context of personalization and energy efficiency.

System Interoperability and Standardization

The main challenge in the convergence of IoT and smart homes is interoperability, as the ecosystem consists of a variety of devices and platforms with different protocols (Alaa et al., 2017). This inconsistency hinders cross-system communication and increases integration costs. Several studies propose the use of open standards such as MQTT, CoAP, and Zigbee as universal communication solutions (Zhang et al., 2022). In addition, API-based approaches and *open middleware* are considered effective in building connections between systems. However, research shows that there is no industry-agreed global standardization model yet, so full interoperability is still an open challenge.

Data Security and Privacy

Security and privacy issues are the most studied dimensions in the literature, given the high risk of cyberattacks on widely connected smart home systems. Studies by Lin and Bergmann (2016) identified threats such as *unauthorized access*, *data leakage*, and *malware injection*. For mitigation, various approaches are proposed, including end-to-end encryption, multi-factor authentication, and blockchain-based trust management (Sadeghi et al., 2015; Zhang et al., 2022). However, research shows that security solutions often increase system complexity and power consumption, which can reduce the overall

efficiency of the system. Therefore, the balance between security, efficiency, and ease of use is still the main focus of innovation.

Technological Innovation and Future Direction

The latest literature emphasizes the importance of Artificial Intelligence (AI) and Machine Learning (ML) to improve the adaptive intelligence of smart home systems. This technology enables predictive user behavior, automated energy management, and data-driven decision-making (Lee & Lee, 2020). In addition, blockchain adoption is beginning to be implemented to strengthen data integrity and build trust between devices in a decentralized network (Gong et al., 2023). Another emerging trend is the convergence with 5G technology that accelerates communication between devices. However, most research is still conceptual, and empirical studies on the implementation of hybrid IoT–AI–blockchain systems in the context of smart homes are still very limited.

Research Synthesis and Implications

The literature synthesis shows that the convergence of IoT and smart homes is not only dependent on technological advancements, but also requires a multidisciplinary approach that involves aspects of design, user behavior, regulation, and privacy policy. The biggest challenges include a lack of global standardization, integration complexity, and ongoing security risks. Future research needs to be directed towards the development of adaptive integration frameworks, AI-based security mechanisms, and measuring the socio-economic impact of smart home adoption. In addition, collaboration between academia, industry, and government is needed to build an interoperable, secure, and sustainable ecosystem (Snyder, 2019).

Conclusion

This research has systematically explored the convergence between the Internet of Things (IoT) and smart home technology, focusing on architectural integration, interoperability, security, and technological innovation. The results of the study show that the implementation of IoT in smart homes plays an important role in improving energy efficiency, user convenience, and data-driven automation (Gubbi et al., 2013; Al-Fuqaha et al., 2015). However, complex integrations and a variety of communication protocols mean that cross-platform interoperability is still limited. Security and privacy issues have also emerged as crucial challenges that hinder wider adoption.

Although many advances have been made in system architecture and supporting technologies such as cloud computing, edge computing, and AI-based automation, the literature shows that there are still significant gaps in terms of standardization, scalability, and data security (Lin & Bergmann, 2016; Gong et al., 2023). The lack of a global framework that governs interoperability between devices and platforms is a major obstacle. In addition, many security solutions are technical in nature, but have not considered aspects

of user behavior, data ethics, and privacy policies that are adaptive to technological developments.

Innovation trends that combine Artificial Intelligence (AI), Machine Learning (ML), and blockchain show great potential to build smart, secure, and self-sustaining smart homes. AI can improve the adaptability of systems to user preferences, whereas blockchain offers transparency and trust in data management (Lee & Lee, 2020; Zhang et al., 2022). The integration of this technology is expected to strengthen operational efficiency while addressing traditional weaknesses in IoT systems.

Based on the synthesis of the literature, future research is recommended for:

1. Develop an open standards-based adaptive integration framework that is able to accommodate cross-platform interoperability.
2. Design AI-based security mechanisms and *privacy-preserving technologies* to maintain user trust.
3. Conducting empirical and experimental studies to test the effectiveness of hybrid systems (IoT–AI–Blockchain) in real smart home environments.
4. To comprehensively examine the social, economic, and environmental impacts of smart home adoption to support inclusive and sustainable public policies.

This research makes a conceptual contribution by providing a comprehensive map of trends and directions of innovation in the convergence of IoT and smart homes. The study also highlights unresolved challenges, while offering a development direction that can serve as a foundation for academics, developers, and policymakers in designing a more integrated, secure, efficient, and user-oriented smart home ecosystem.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Lin, J., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44. https://doi.org/10.3390/info7030044

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2015). Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys & Tutorials, 16*(1), 414–454. https://doi.org/10.1109/SURV.2013.042313.00197

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. https://doi.org/10.1145/2744769.2747942

Zhang, Y., Deng, R. H., & Liu, J. K. (2022). Smart homes and the IoT: Recent advances and future challenges. *IEEE Network, 36*(2), 10–17. https://doi.org/10.1109/MNET.011.2100223

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications, 97*, 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Gong, J., Wang, L., & Li, X. (2023). Interoperability frameworks for IoT-based smart homes: A comparative study. *IEEE Access, 11*, 12984–13002. https://doi.org/10.1109/ACCESS.2023.3245671

Lee, I., & Lee, K. (2020). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 63*(5), 585–606. https://doi.org/10.1016/j.bushor.2020.05.004

Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference*, 1–6. https://doi.org/10.1145/2744769.2747942

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039