SJCS Scientific Journal of Computer Science
futuristech PT. Teknologi Futuristik Indonesia
Received: March 30, 2026; Revised: May 23, 2026; Accepted: June 12, 2026; Published: June 13, 2026; Current version: June 13, 2026. e-ISSN: 3110-3170
Digital Object Identifier 10.64539/sjcs.v2i2.2026.479

Review

Secure, Intelligent, and Energy-Efficient Architectures for Next-Generation Smart Homes: A Review

Haruna Kawuwa[1,*], Nura Muhammad Sani[2], Ninyikiriza Deborah Lynn[1], Mohammed Mansur Ibrahim[3], Mustapha Ismail[4], Musbahu Bala Ibrahim[3]

[1] Department of Informatics Engineering, Universitas Dian Nuswantoro, Semarang, Indonesia; e-mail: haruna.kawuwa@gmail.com (H. Kawuwa), dninyikiriza000@gmail.com (N. D. Lynn).
[2] Department of Computer Science, Federal Polytechnic Kaltungo, Gombe State Nigeria; e-mail: nuramuhammad07061@gmail.com (N. M. Sani).
[3] Directorate of Information & Communication Technology, Federal University of Kashere, Gombe, Nigeria; e-mail: mansuribrahim59@fukashere.edu.ng (M. M. Ibrahim), musbahubibrahim@gmail.com (M. B. Ibrahim).
[4] Department of Computer Science, Gombe State University, Gombe State, Nigeria; almustea1@gmail.com (M. Ismail).
* Correspondence

The authors received no financial support for the research, authorship, and/or publication of this article.

Abstract: The fast adoption of Internet of Things (IoT) technologies in smart home has driven the demand for secure, smart and energy efficient homes. However, findings from previous research were limited. This study aims at addressing the growing demand for common and scalable solutions in next generation smart home environments by performing a systematic literature review of smart home systems featuring IoT. The Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA 2020) framework was used in the study. The literature was collected from major peer-reviewed academic databases. The Assessments published during the period 2021-2026 were selected for qualitative synthesis after screening, eligibility and quality evaluation. The five main dimensions were analyzed: architectural trends, communication trends, security and privacy mechanisms, Human Activity Recognition (HAR) and intelligent automation, energy management strategies, and research challenges. Results reveal that smart home systems are increasingly multi-layer and hybrid edge-cloud systems based on technologies like Wireless Fidelity (Wi-Fi), ZigBee, Bluetooth Low Energy (BLE), Long Range (LoRa), and Z-Wave. Typical applications for Machine Learning (ML) and Deep Learning (DL) include energy optimisation (forecasting, reinforcement learning), as well as intrusion detection, automation, and context-aware decision making. Challenges faced are interoperability issues, cyber security concerns, computational problems, device variations, and lack of real-world testing. The aim of the study is to create an integrated synthesis and comparative taxonomy that can guide the future development of scalable, secure and intelligent smart home ecosystems.

Keywords: Internet of Things; Smart Home Automation; System Architecture; Machine Learning; PRISMA Framework.

1. Introduction

The rate at which the IoT is being developed has re-designed conventional living environments into a digitalized environment that is able to sense, process and react to user demands. A smart home system is a system that uses a combination of embedded sensors, actuators, wireless communication technology and intelligent models of decision making so as to automate, monitor and control household functions. These systems are designed to add to their convenience, safety, energy consumption, and general living standards by automatically controlling patterns like lighting, temperature control, appliance control, intrusion management and energy savings [1]. There are a number of important challenges that IoT enabled smart homes are facing despite their advantages. Security and privacy are also the most urgent issues because the introduction of heterogeneous devices and open communication standards leaves gaps that have the potential to be used to compromise the system via unauthorized access, malware injection or manipulation of devices [2].

Recent report indicates that cyber-attack on smart homes has become increasingly complex and the new security protocols such as lightweight cryptography, intrusion detection and AI-based threat analysis need to be implemented [3], [4]. Besides the issue of security, intelligent automation relies substantially on precise information on Multimodal sensing and Human Activity Recognition (HAR) as well as context aware decisions. Despite enhanced performance in activity recognition brought by deep learning models like Convolutional Neural Network (CNNs), Long Short-Term Memory networks (LSTMs) and Graph Neural Networks (GNNs), there are still limitations on the application of these new models in actual households due to the computational constraints, cross-user and privacy concerns [5], [6]. On the same note, edge-computing solutions have been developed to address the increasing demand of low latency, and privacy preserving HAR solutions [7], [8].

Another pillar of smart home research that is important is energy management. Load monitoring, forecasting, demand response scheduling and optimization: EHEMS are efficient systems that are machine-based to monitor energy within homes through the utilization of machine learning and optimization. The current literature has shown that forecasting models and smart control strategies have the ability to minimize energy usage and enhance system reliability [9]-[11]. Nonetheless, there have been difficulties in terms of user behavioral variability, compatibility with renewable energy source, as well as incorporated distributed edge-cloud resources [12], [13]. Although there is extensive research on the individual domains of smart home security, intelligent automation, and energy management, the majority of reviews analyze these domains individually. This disaggregation prevents knowledge of the interaction of these three pillars in contemporary IoT systems. Therefore, a consistent synthesis that combines architectural, algorithmic, communication and operational viewpoints into one systematic framework is required.

To address this gap, the present Systematic Literature Review (SLR) synthesizes research across these domains using a structured Preferred Reporting Items for PRISMA methodology. The review aims to identify architectural trends, communication technologies, security mechanisms, intelligent automation methods and energy management strategies in IoT-enabled smart homes, while highlighting emerging challenges and research opportunities.

The contribution this study can make is four-fold. First, this review gives a synthesis of the next-generation smart home systems, integrating security, intelligent automation, and energy management, in a single overall analytical framework that was not the case for many other existing review studies. Second, its organization and the systematically classification of existing smart home research based on architectural models, communication technologies, machine learning method, edge-cloud integration method, provide a well-structured taxonomy of current scholarly work in smart homes. Third, the paper considers the current challenges with interoperability, scalability, data protection, computational costs and field application for smart homes in various domains. Lastly, the study outlines some emerging technologies such as edge intelligence, federated learning, TinyML, generative artificial intelligence, blockchain-based security, and 6G communication are identified as enablers for future smart home environments and emphasizes their significance for future research to realize safe intelligence, scale and energy efficiency in future home environments.

2. Methodology

The current study used systematic literature review (SLR) procedure, following the reasonable principles generally used to perform an evidence-based research synthesis in the studies of computing and information systems. The PRISMA 2020 review process aims to propose the transparency, replicability, and methodological rigor of all steps planned, implemented, and reported [14]. The planning, search design, review protocol, and documentation process were also informed by the principles of recent SLR guidance specific to the studies of computer science and engineering [15]-[17]. The general concept of this SLR is to gather the literature on the topic of IoT-based smart homes, and to generalize the results of such studies in the three key broad areas, namely security, intelligent automation and energy management.

Figure 1 shows that IoT plays a central role in enabling modern smart home applications by connecting everyday household devices to sensing, communication, and automation networks. Smart homes use IoT technologies to support a wide range of functions, including lighting control, temperature regulation, motion detection, keyless entry, alarm and security monitoring, and energy management optimization.

2.1. Review Framework

This research paper employed Systematic Literature Review (SLR) as the methodology to systematically identify, analyse and synthesize the existing research literature of smart home IoT system. The review process was done with methodological transparency, in a reproducible and rigorous way, guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) [14]. Adopting a scientific method related to the specific field is quite crucial when extracting the scientific content from vast scientific papers shared across different research

Table 1. Research Questions of the Study.

RQ	Research Question	Objective
RQ1	What architectural and communication approaches are commonly adopted in IoT-enabled smart home systems?	To identify dominant smart home architectures, communication protocols, and integration models.
RQ2	What security and privacy mechanisms are applied in smart home environments?	To examine cybersecurity techniques, intrusion detection methods, and privacy-preserving approaches.
RQ3	How are intelligent automation and human activity recognition techniques implemented in smart homes?	To analysed machine learning and deep learning approaches used for intelligent automation and behavioural monitoring.
RQ4	What energy management and optimization strategies are employed in smart home systems?	To investigate intelligent energy optimization techniques and efficiency improvement methods.
RQ5	What are the major research challenges and gaps affecting next-generation smart home systems?	To identify limitations, interoperability challenges, scalability issues, and future research directions.

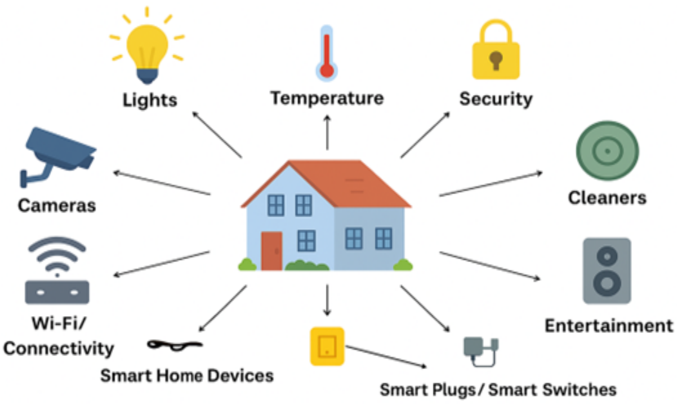

Figure 1. Applications of IoT in Smart Home.

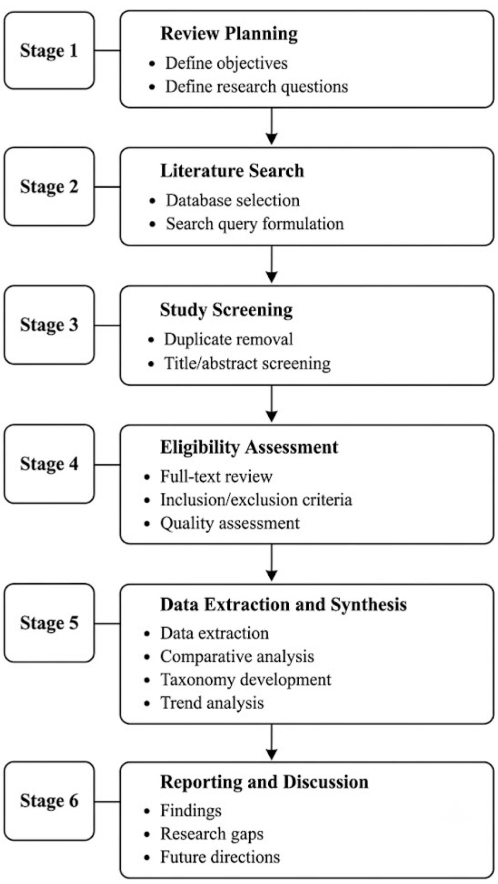

Figure 2. Systematic Literature Review Workflow.

areas such as smart home security, intelligent automation, and energy management, which is solved by using the SLR. Responses to the "translations" were guided by an overall review starting with the planning of the review, followed by the identification of the literature, screening of the studies, assessment for eligibility, and synthesis of the final set of studies. Literature was retrieved from the major scientific databases and quality assessed based on predefined inclusion, exclusion and quality criteria. The importance of computer science and information systems research led to the adoption of known SLR guidelines [15]-[17] to aid the methodology.

The overall process steps of the systematic literature review that was carried out in this study are summarized in the Figure 2. The work flow outlines the key tasks in review planning, literature identification, literature screening, eligibility assisted, synthesis and reporting. The SLR workflow showcases the sequential, systematic and transparent approaches used throughout the SLR process. A staged process also allowed researchers in the selected studies to be evaluated in a consistent manner based on predetermined research questions, inclusion criteria, and quality evaluation criteria.

2.2. Research Questions

The review is guided by the following research questions, formulated in alignment with contemporary SLR planning guidelines for information systems and computing research [16], [17]. The research questions are shown in Table 1. A set of five research questions were formulated to guide the systematic literature review process, which was based on the objectives of the study, and the major thematic areas that were identified in the research of smart homes in the contemporary era. The literature search, comparative analysis, study selection, and synthesis performed during the review, followed these research questions.

2.3. Search Strategy and Study Selection

A systematic search procedure was used to find relevant IoT-enabled smart home systems related studies. To

Table 2. Search Queries Used for Literature Retrieval.

Database	Search Query
IEEE Xplore	(“smart home” OR “IoT smart home”) AND (“security” OR “machine learning” OR “energy management” OR “human activity recognition”)
ACM Digital Library	(“IoT-enabled smart home” OR “smart home systems”) AND (“cybersecurity” OR “deep learning” OR “edge computing”)
ScienceDirect	(“smart home architecture”) AND (“IoT” AND “energy management” AND “automation”)
SpringerLink	(“smart homes” AND “machine learning”) AND (“privacy” OR “activity recognition” OR “edge AI”)
MDPI	(“IoT smart home”) AND (“security mechanisms” OR “HAR” OR “energy optimization”)

Table 3. Inclusion and Exclusion Criteria.

Criteria Type	Inclusion Criteria	Exclusion Criteria
Publication Type	Peer-reviewed journal articles and conference papers	Editorials, abstracts, posters, theses, and non-peer-reviewed articles
Language	Studies published in English	Non-English publications
Publication Period	Studies published between 2021 and 2026	Studies published before 2021
Research Domain	Studies related to IoT-enabled smart homes, security, intelligent automation, human activity recognition, communication architectures, and energy management	Studies unrelated to smart home systems or outside IoT applications
Methodological Quality	Studies with clear methodology, technical contribution, and sufficient experimental or analytical detail	Studies lacking methodological clarity or technical depth
Accessibility	Full-text articles accessible through selected databases	Articles with inaccessible full text

retrieve literature, five academic databases (IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and MDPI) were used. The databases chosen are because they offer the most comprehensive coverage of peer-reviewed research into the computer science, Internet of Things (IoT), Artificial Intelligence (AI), Cybersecurity and Smart Energy systems research field.

Considering the recent developments in technology and research trends in the field of next generation smart home systems, literature that was published from year 2021 to 2026 was taken in to account. The literature search was carried out from January through March 2026, using boolean queries on terms related to smart home, IoT architectures, cybersecurity, machine learning, human activity recognition, edge computing and energy management. Examples of search terms used were: (“smart home” OR “IoT smart home”) AND (“security” OR “machine learning” OR “energy management” OR “human activity recognition”) (See Table 2).

Selection of studies was done in successive phases. First, duplicate records from various databases were eliminated. Second, a title and abstract screening was done to exclude irrelevant studies. Third, a full-text assessment was performed to assess methodological quality, relevance and contribution to the objectives of this review. The following criteria were used for the inclusion of the articles: papers published in peer-reviewed English-language journals and conference proceedings which discussed smart home systems using IoT, as well as research relating to the security, intelligent automation, communication architectures and energy management. The exclusion criteria were as follows: non-peer reviewed publications, editorials, short abstracts, and studies that were not technically or methodologically detailed.

Additionally, backward citation tracking was conducted by applying references of selected studies to find potentially relevant publications and review comprehensiveness. The last group of selected studies was synthesized and analyzed following the predetermined research questions of this review. Search terms were slightly adjusted to ensure consistency of keywords and main ideas while adjusting for differences in indexing structures and search syntax across databases. Inclusion and exclusion criteria for studies are summarized in Table 3.

2.4. Quality Assessment

The eligibility phase of the review involved a quality assessment of selected studies to ensure the selection of studies was reliable and methodologically strong. The assessment was carried out to assess the relevance, clarity, methodological soundness, and technical contribution of each study that was part of the final synthesis. The quality evaluation process was modified from the widely used guidelines used in the systematic review of literature in computer science and information systems research [15]-[17]. For each study, the quality assessment criteria were predefined and they were all evaluated based on these criteria in relation to the research objectives, methodology,

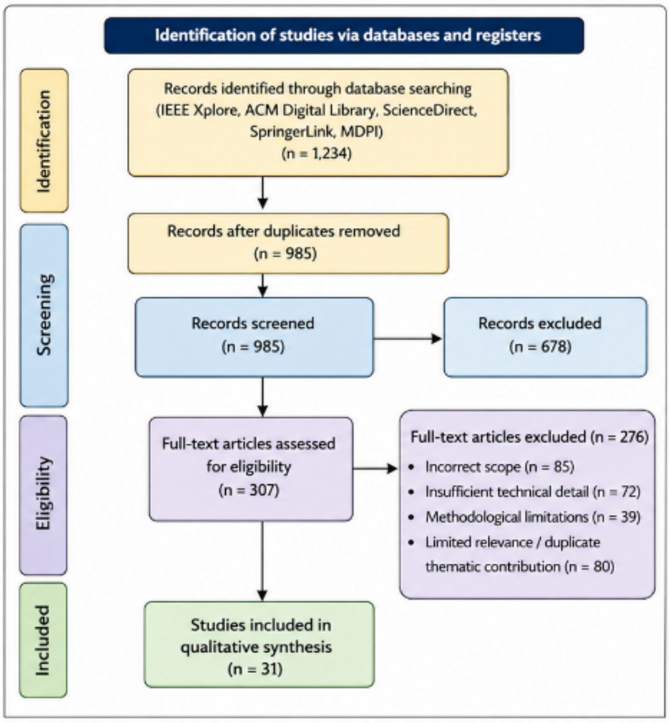

Figure 3. PRISMA 2020 flow diagram.

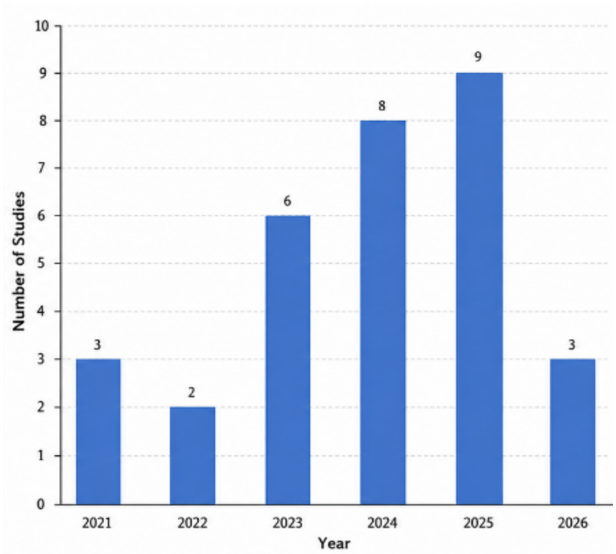

Figure 4. Publication Trend of Selected Studies (2021-2026).

experimental validation and applicability of the research questions. There was a 3-point scale for assigning a score to each criterion: "Yes" = 1, "Partially" = 0.5, "No" = 0. Eligibility assessment (selection) was performed and studies which were poorly methodologically designed or lacked technical detail were not included.

2.5. PRISMA Flow Diagram

PRISMA 2020 flow diagram is an outline of the study selection process and clearly shows the route that the records travelled before the identification, screening, an evaluation of their eligibility and eventual approval [14]. The records obtained in databases, removals made, studies filtered on title and abstract, full certain documents examined, reasons why the further study should be done and the final records that are to be incorporated in the review are documented. This diagram makes the whole process of research more transparent and allows readers to understand how the final studies were selected.

The PRISMA 2020 flow diagram used in the selection of studies in this systematic literature review is presented in Figure 3. A total of 1,234 records were found from various academic databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink and MDPI through pre-defined search queries regarding Internet of Things (IoT)–enabled smart home systems, cybersecurity, intelligent automation and energy management. After the removal of duplicates and some initial preprocessing, 985 data points were left for further evaluation.

Titles and abstracts in the screening stage were evaluated based on the set inclusion/exclusion criteria. A total of 678 records were excluded during the title and abstract screening stage because they were not technically relevant, were non-English publications, did not focus on smart home technologies, or were outside the scope of this review. These 307 studies were further examined to determine their eligibility for further evaluation in the full-text articles phase, based on the following criteria: methodological quality, technical contribution, experimental validation and relevance to the research questions. The remaining 307 studies advanced to the full-text articles phase, where methodological quality, technical contributions, experimental validation and relevance to the research questions were carefully assessed.

Some of the additional studies were not included after the completion of the eligibility evaluation because they were not sufficiently technically deep, lacked methodological aspects, experimental validation was weak, there was duplication of thematic coverage, or they were of limited relevance to the objectives of this review. In particular, 85 studies were rejected due to incorrect research scope, 72 studies due to the lack of technical detail, 39 due to methodological limitations and 80 due to limited relevance and duplicate thematic contributions. After the final inclusion, 31 studies were included for qualitative synthesis and comparative analysis.

The PRISMA 2020 framework provided greater transparency, reproducibility and systematic traceability, because it ensured structured identification, screening, evaluation and synthesis of literature with a minimum amount of selection bias during the review process.

3. Results and Discussion

This section presents the synthesized findings of the systematic literature review and provides an in-depth discussion of emerging trends, dominant approaches, and critical limitations in smart home systems. The analysis is structured according to the research questions, enabling a comprehensive understanding of architectural designs, security mechanisms, intelligent automation, and energy management strategies.

3.1. Overview and Trends of Selected Studies

The following studies were selected for their overview and trends: Thirty-one (31) studies were selected after applying the predefined inclusion and exclusion criteria through the PRISMA-guided selection process. The identified studies were mainly published from 2021 to 2025, indicating an increasing number of studies and the ongoing trend of research in the field of smart home technologies with IoT.

The year distribution of the selected studies in this review is shown in Figure 4. As shown in the publication trend, the research interest in the field of IoT-enabled smart home systems is rising, with the topics of cybersecurity, intelligent automation, edge intelligence, and energy efficient architectures of smart home systems being the primary areas of interest. The growth is particularly strong from 2023 to 2025, highlighting the increasing relevance of smart home technologies that integrate and are intelligent. According to a trend analysis, the following points are made:

- **Security and privacy** are the most extensively studied domains, reflecting growing concerns about cyber threats in interconnected environments.
- **Intelligent automation**, particularly HAR, has gained significant attention due to advancements in deep learning.
- **Energy management**, although critical, is comparatively less explored in integrated synthesis.

Importantly, only a limited number of studies address these domains in a good manner, confirming the fragmentation identified in existing literature. This highlights the need for unified approaches that combine multiple functionalities within a single architecture.

Table 4 also presents a summary of the primary characteristics of the research studies, the common fields of research, methods, and constraints. Most research focuses on not more than one of the individual areas like security, automation, or energy management and little effort is being made to merge the frameworks. Additionally, methodologies, in most cases, are rooted in controlled conditions implying that large-scale validation of the theory is not done in real-life.

3.2. Architectural and Communication Trends

It shows that smart home systems today are based mostly on layered architectural designs, broken down into perception, network, middleware, and application layers. These architectures improve the modularity, scalability and organization of the systems. There is also wide usage of communication technologies with different protocols including Wi-Fi, ZigBee, Bluetooth Low Energy (BLE), LoRa, and Z-Wave. Each of the protocols possesses various strong sides in terms of range, power consumption, and data rate. However, as a result of several standards of communication, there exists severe interoperability problems which nonetheless continue to be the focus of concern to successful integration of the systems. The second trend is that hybrid edge-cloud architecture is being adopted more with latency sensitive tasks being executed at the edge and additional computation tasks being executed in the cloud. Such a solution would cause systems to be responsive, reduce the bandwidth consumption, and increase the privacy of systems. Importantly, although flexibility is provided by such architectures, such architectures also cause the complexity of coordination of the system, control of resources, and implementation of security among distributed items.

Layered and hybrid edge-cloud architectures provide better scalability and distributed processing, but most of the existing solutions are still very dependent on the variety of communication standards, which makes interoperability and system integration so complex. Also, some architectures have been evaluated only under controlled conditions, and therefore are not necessarily applicable to a smart home deployment with devices that are diverse, network conditions that are unstable, and user behaviour that is dynamic.

3.3. Security and Privacy Mechanisms

Security is one of the major issues in smart home environment because of the existence of resource constrained devices and non-homogeneous communication protocols. The analysed articles revealed that machine learning techniques are often used for threat detection such as intrusion detection system (IDS), anomaly detector system, automated technique for malware classification, etc. Human activity recognition (HAR) and intelligent automation (IA) have been greatly enhanced in smart home environments by deep learning technologies, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), and Graph Neural Net-works (GNNs). They can however be constrained in the application by computational overhead, energy consumption, which is inappropriate when dealing with low power IoT devices. Cryptography and blockchain-related access control measures, which are lightweight in nature, are nowadays proposed in addition to machine learning to enhance the data security and trust. Albeit blockchain has been shown to be decentralized, transparent, its scalability and latency issue make it unsuitable in actual application to real time smart home systems. The future works should be based on high quality lightweight and adaptive security frameworks that are

Table 4. Summary of Selected Studies in Smart Home Systems.

Ref	Focus Area	Method/Technique	Key Contribution	Limitation
[1]	Security	ML-based traffic classification	Detects IoT device behavior using network data	Limited real-world validation
[2]	Security	Survey of IoT security methods	Identifies threats and countermeasures	Lacks implementation analysis
[3]	Automation (HAR)	Motion sensor-based recognition	Supports independent living via activity detection	Limited scalability
[4]	Security	AI-based threat detection	Uses generative models for cyber threat detection	High computational cost
[5]	Automation (HAR)	Deep learning (CNN, multimodal)	Improves activity recognition accuracy	Resource-intensive models
[6]	Automation (HAR)	Context-aware systems	Enhances personalization and awareness	Privacy concerns
[7]	Security	Edge AI framework	Enables secure real-time processing at edge	Limited large-scale testing
[8]	Automation (HAR)	Edge-based HAR system	Preserves privacy using local processing	Device constraints
[9]	Energy	ML-based energy management	Optimizes energy consumption and scheduling	Depends on accurate forecasting
[10]	Energy	Optimization techniques	Improves energy storage efficiency	Complex implementation
[11]	Energy	Hybrid Deep Learning Forecasting	Enhances load prediction accuracy	Limited generalizability across households
[12]	Architecture	Edge-cloud computing	Improves distributed processing	Integration complexity
[13]	Architecture	IoT-edge-cloud survey	Identifies system challenges	Mostly conceptual
[18]	Architecture	Generic IoT framework	Defines layered smart home architecture	Limited implementation detail
[19]	Security	AI-driven cybersecurity	Adaptive malware detection	Computational overhead
[20]	Security	Blockchain-based access control	Enhances trust and decentralization	Scalability issues
[21]	Security	Generative AI security	Advanced threat modeling	Emerging, limited validation
[22]	Automation	CNN-based	High recognition accuracy	Requires large datasets
[23]	Automation	Multimodal deep learning	Improves robustness of HAR systems	Data fusion complexity
[24]	Energy	Renewable integration	Enhances sustainability	Integration challenges
[25]	Energy	Intelligent energy systems	Improves efficiency using AI	Limited real-world deployment
[26]	Architecture	6G + IoT integration	Future communication support	Still theoretical
[27]	Energy	Predictive ML models	Enhances grid stability	Data dependency
[28]	Energy	Reinforcement learning	Adaptive scheduling optimization	Training complexity
[29]	Automation	Multimodal data fusion	Improves decision-making accuracy	Computational cost

capable of achieving a good trade-off between performance, energy consumption and privacy as suggested in the discussion above.

Even with the power of machine learning and blockchain security solutions, most proposed solutions remain too costly to use on the low-power IoT devices typical of a smart home. Additionally, the absence of a standardized security framework and limited validation in the field raises concerns about scalability, deployment feasibility and adaptability over time to address evolving cyber threats [30].

3.4. Intelligent Automation and Activity Recognition

Intelligent automation is used in smart homes, although it is significantly influenced by advances in HAR and context-aware computing. It is demonstrated that global and local forms of user behavior are quite common to forecast by using deep learning, as well as CNNs, LSTMs, and mixed architectures. Imaging Multimodal sensing or co-sensing techniques, or which integrate information across two or more of direction, e.g. wearable devices, sensors in the immediate environment or vision, have been more precise and consistent [31]. However, there are complexities of data fusion, privacy and high-computational requirements with these practices. Another notable observation in this case is that the HAR models are mostly tested under controlled experimental settings that forms a major limitation to the application of models in actual life. The users, environment variables and device configurations are also variable hence makes deployment even more difficult. Consequently, there is a need for adaptive, personalized and privacy-preserving automation systems capable of operating effectively in real-world environments [31].

Deep learning-based HAR systems have high recognition accuracy in experimental environments but have not yet demonstrated good generalization to various households or the variety of human behaviours. Practical application of large-scale deployment of multimodal sensing systems in residential settings is also hindered by privacy issues of a continuous behavioural monitoring and the computational load.

3.5. Energy Management Strategies

The energy control has taken one of the focal points of the smart home system and research has focused on the load prediction, appliance scheduling and optimization processes. Machine learning systems typically predict energy consumption and system optimization with the use of regression, neural networks, and reinforcement learning models. Reinforcement learning models particularly, can be used to make the best choice dynamically by learning optimal control strategies. These technologies have great possibilities of energy consumption saving and attaining cost-effectiveness.

However, it has several limitations which can be perceived. Many of the studies utilize simulated data or controlled conditions that lack the reflection of the real-world use of energy. The fact that the user behavior can vary and the fact that the sources of renewable energy can be included also lead to the further complexity. This implies that the following research would concern more practical implementation and easy to use design as well as the relationship on energy management solutions and renewable energy to enhance feasibility of the energy management systems. Although machine learning and reinforcement learning approaches hold great promise in the field of intelligent energy optimization, numerous studies utilize synthetic data sets and laboratory setups. As a result, there is a lack of long-term reliability, adaptability and acceptance in real world residential environments.

3.6. Cross-Domain Synthesis of Smart Home Systems

From the literature review, an important finding was that most of the smart home solutions focus on the security, intelligent automation and energy management as separate research areas. Nevertheless, next-generation smart home environments call for integrated architectures that can support secure communication, intelligent decision making and energy-efficient operation in a single smart home environment. In light of the insights gained from the above presented review, a conceptual integrated architecture is discussed to conceptually consolidate the key components found across the studies selected. This framework integrates multi-layer IoT architectures, edge-cloud computing, artificial intelligence, cybersecurity mechanisms, human activity recognition, and intelligent energy management, all in an integrated system model.

Heterogeneous IoT sensors and smart devices continuously gather data related to environmental, behavioural, and energy aspects at the perception layer. The communication layer is designed to allow data to pass over wireless technology including Wi-Fi, ZigBee, BLE, LoRa and Z-Wave. The edge layer also facilitates computing-intensive applications such as anomaly detection, human activity recognition, and local decision-making, and the cloud infrastructure allows for storing large amounts of data, optimizing models, and conducting large-scale analytics. The security mechanisms, such as lightweight encryption, intrusion detection systems, blockchain-based access control, and AI-based threat detection, are implemented on every architectural level, ensuring the privacy, integrity, and reliability of systems. At the same time, context-aware computing and intelligent automation modules are used to facilitate adaptive user services, while energy management modules implement forecasting, scheduling and optimization tools to optimize energy consumption.

The smart home environment is the perfect example of how security, automation and energy management are all interdependent. The security and reliability of communication infrastructure, for instance, is vital for intelligent automation systems, and real-time contextual sensing is increasingly used to support energy optimization mechanisms. Likewise, edge intelligence supports low latency automation and security and energy efficient processing. This cross-domain synthesis shows that the future research on smart homes should overcome the single domain approaches to reach more holistic and synergetic smart home architectures, which are scalable, intelligent, secure and energy-conscious, to support the development of energy-smart living environments.

3.7. Cross-Domain Integration and Research Gaps

One of the most significant findings of this review is the lack of integrated synthesis that simultaneously address security, intelligent automation, and energy management. Most existing studies focus on individual domains, resulting in fragmented and isolated solutions.

Key research gaps identified include:

a. Interoperability challenges across heterogeneous devices and communication protocols
b. Privacy and data protection issues, particularly in data-intensive applications
c. Limited availability of standardized datasets for benchmarking and evaluation
d. Lack of large-scale real-world validation, with many studies relying on simulations

Table 5. Comparative Taxonomy of Reviewed Smart Home Studies.

Ref	A1	A2	A3	A4	AI/ML Techniques	Real-World Validation	Key Limitation
[1]	✓				ML Traffic Classification	Partial	Limited scalability
[4]	✓			✓	Generative AI	No	High computational cost
[5]		✓			CNN, Deep Learning	Partial	Resource-intensive
[7]	✓	✓		✓	Edge AI	Partial	Limited large-scale testing
[8]	✓	✓		✓	Edge-based HAR	Partial	Device constraints
[9]			✓		ML Optimization	Partial	Forecast dependency
[12]			✓	✓	Edge-Cloud Collaboration	No	Integration complexity
[20]	✓				Blockchain	No	Scalability issues
[23]		✓			Multimodal Deep Learning	Partial	Data fusion complexity
[24]			✓		Renewable Integration	Partial	Integration challenges
[26]	✓	✓	✓	✓	6G + Edge Intelligence	No	Mostly conceptual
[28]			✓		Reinforcement Learning	Partial	Training complexity

Note: *A1: Security, A2: Intelligent Automation, A3: Energy Management, A4: Edge/Cloud Integration.*

These challenges highlight the need for holistic and standardized smart home architectures that unify multiple functionalities while ensuring scalability, security, and efficiency. To further examine the level of integration across the reviewed literature, a comparative taxonomy of selected studies was developed based on their coverage of security, intelligent automation, energy management, edge-cloud integration, artificial intelligence techniques, and real-world validation. The synthesis presented in Table 5 highlights the dominant research focus areas and existing limitations across contemporary smart home studies.

Table 5 shows that most of the existing research is dedicated to a specific domain area of the smart home, either in the field of security, intelligent automation, or energy management but not to an integrated smart home framework. Furthermore, very few studies integrate edge-cloud intelligence within a unified architecture with AI and cross-domain optimization. A second notable fact is that many studies are based on simulations or controlled experiments, and there is little, if any, real-world validation of the models at large scale. The results reflect issues of fragmentation and interoperability in next generation smart home research, and highlight the significance of system architectures that are holistic, scalable and privacy aware.

3.8. Implications for Future Research

Based on the findings, future research should focus on:

a. Developing unified frameworks that integrate security, automation, and energy management
b. Designing lightweight and energy-efficient machine learning models for edge devices
c. Enhancing interoperability through standard protocols and middleware solutions
d. Conducting large-scale real-world experiments to validate proposed systems

Such directions are essential for advancing smart home systems from theoretical models to practical, deployable solutions.

4. Conclusion

This research proposed a systematic literature review of recent advances in smart home systems that are based on the Internet of Things (IoT), including architectures and communication technologies, security and machine learning-based protection mechanisms, intelligent automation and human activity recognition, and energy management strategies. The outcomes show a solid path towards more multi-layered and hybrid architectures involving both the edge and the cloud to enhance scalability, responsiveness, and distributed processing capabilities. The growth of the number and variety of communication protocols, however, still presents a challenge to interoperability and integration in heterogeneous smart home environments.

The review also found that machine learning, anomaly detection, and blockchain-based security solutions have greatly enhanced the security capabilities in smart home systems. However, there are certain limitations for these solutions, such as resource processing capacity, privacy issues, and non-standardization and inadequate large-scale deployment. Multimodal sensing and deep learning systems have shown great promise for context-aware decision making and for human activity recognition, with issues of privacy preservation, generalization, and reliability of deployment still to be addressed. Energy management applications have demonstrated potential for enhancing the energy efficiency of residential buildings using forecasting models, reinforcement learning, and integrating renewable energy sources. But most of the current methods are still tested in either a simulated or controlled environment. The review revealed the following recurring gaps in the literature: interoperability challenges, lack of common datasets, computational limitations, and a lack of real-world validation. The results emphasize the importance of a unified, integrated smart home framework, which can integrate security, intelligent automation, and energy management in scalable, privacy-aware, and deployable next generation smart home ecosystems.

5. Declarations

5.1. Author Contributions

Haruna Kawuwa: Conceptualization, Methodology, Investigation, Formal analysis, Data Curation, Writing-Original Draft, Visualization; **Nura Muhammad Sani:** Methodology, Validation, Formal analysis, Writing-Review & Editing; **Ninyikiriza Deborah Lynn:** Supervision, Validation, Writing-Review & Editing; **Mohammed Mansur Ibrahim:** Investigation, Resources, Writing-Review & Editing; **Mustapha Ismail:** Formal analysis, Visualization, Writing-Review & Editing; **Musbahu Bala Ibrahim:** Supervision, Project administration, Writing-Review & Editing.

5.2. Institutional Review Board Statement

Not applicable.

5.3. Informed Consent Statement

Not applicable.

5.4. Data Availability Statement

The data used in this study were obtained from peer-reviewed articles retrieved from publicly accessible academic databases. Additional data supporting the findings of this review are available from the corresponding author upon reasonable request.

5.5. Acknowledgment

The author thanks Indonesian Government for sponsor his study through Kemitraan Negara Berkembang (KNB) Scholarship, also University of Dian Nuswantoro, Semarang, especially, the Faculty of Computer Science, Department of Informatics Engineering, as it has enabled a supportive academic environment, research and facilities given to him during his studies.

5.6. Conflicts of Interest

The authors declare no conflicts of interest.

6. References

[1] H. Jmila, G. Blanc, M. R. Shahid, and M. Lazrag, "A survey of smart home IoT device classification using machine learning-based network traffic analysis," *IEEE Access*, vol. 10, pp. 97117–97141, 2022. https://doi.org/10.1109/ACCESS.2022.3205023.

[2] Ankit Sharma and Kriti Bhushan, "A comprehensive survey on IoT security: Challenges, security issues, and countermeasures," *Computer Science Review*, vol. 59, p. 100839, 2026. https://doi.org/10.1016/j.cosrev.2025.100839.

[3] M. Sandhu, M. Varnfield, S. Amadoru, P. A. Yates, B. Kusy, and D. Silvera Tawil,"Feasibility of motion sensor-based human activity recognition for supporting independence in smart homes," *Maturitas*, vol. 199, p. 108632, Aug. 2025. https://doi.org/10.1016/j.maturitas.2025.108632.

[4] A. K. Ray, R. Sharma, and S. K. Pandey, "AI-Driven Privacy and Security Frameworks for Smart Homes: A Comprehensive Survey," *International Journal of Applied Mathematics*, vol. 38, no. 11s, pp. 2345–2383, 2025. https://doi.org/10.12732/ijam.v38i11s.1331.

[5] G. Diraco, G. Rescio, P. Siciliano, and A. Leone, "Review on human action recognition in smart living: Sensing technology, multimodality, real-time processing, interoperability, and resource-constrained processing," *Sensors*, vol. 23, no. 11, p. 5281, 2023. https://doi.org/10.3390/s23115281.

[6] G. Diraco, G. Rescio, A. Caroppo, A. Manni, and A. Leone, "Human action recognition in smart living services and applications: Context awareness, data availability, personalization, and privacy," *Sensors*, vol. 23, no. 13, p. 6040, 2023. https://doi.org/10.3390/s23136040.

[7] P. Thakur, S. Goel, and E. Puthooran, "Edge AI Enabled IoT Framework for Secure Smart Home Infrastructure," *Procedia Computer Science*, vol. 235, pp. 3369–3378, 2024. https://doi.org/10.1016/j.procs.2024.04.317.

[8] A. U. Rehman, M. Farooq, F. Khan, G. Srivastava, R. A. Aldmour, R. Alturki, and B. Alshawi, "FEDge-HAR: An optimized private mobile edge-enabled IoT paradigm for privacy of human activity recognition," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 40909–40920, 2024. https://doi.org/10.1109/JIOT.2024.3457372.

[9] A. Raza, L. Jingzhao, Y. Ghadi, M. Adnan, and M. Ali, "Smart home energy management systems: Research challenges and survey," *Alexandria Engineering Journal*, vol. 92, pp. 117–170, 2024. https://doi.org/10.1016/j.aej.2024.02.033.

[10] Y. Ma, H. Wang, W. Yu, F. Cao, S. Cheng, and A. Yang, "User-side cloud energy storage configuration and operation optimization considering time-of-use pricing and state-of-charge management," *Energy Conversion and Economics*, vol. 6, no. 2, pp. 65–82, 2025. https://doi.org/10.1049/enc2.70005.

[11] I. H. Ou Ali, A. Agga, M. Ouassaid, M. Maaroufi, A. Elrashidi, and H. Kotb, "Predicting Short-Term Energy Usage in a Smart Home Using Hybrid Deep Learning Models," Frontiers in Energy Research, vol. 12, 2024, Art. 1323357. https://doi.org/10.3389/fenrg.2024.1323357.

[12] J. Liu, Y. Du, K. Yang, J. Wu, Y. Wang, X. Hu, "Edge-Cloud Collaborative Computing on Distributed Intelligence and Model Optimization: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 5049 - 5080, 2026. https://doi.org/10.1109/COMST.2026.3669216.

[13] P. Gkonis, A. Giannopoulos, P. Trakadas, X. Masip-Bruin, and F. D'Andria, "A survey on IoT-edge-cloud continuum systems: Status, challenges, use cases, and open issues," *Future Internet*, vol. 15, no. 12, p. 383, 2023. https://doi.org/10.3390/fi15120383.

[14] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021. https://doi.org/10.1136/bmj.n71.

[15] B. Kitchenham, D. Budgen, and P. Brereton, "The value of mapping studies—A participant-observer case study," *Information and Software Technology*, vol. 95, pp. 163–175, 2020. https://doi.org/10.14236/ewic/EASE2010.4.

[16] J. Paul, W. M. Lim, A. O'Cass, A. W. Hao, and S. Bresciani, "Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR)," *International Journal of Consumer Studies*, vol. 45, no. 4, pp. O1–O16, 2021. https://doi.org/10.1111/ijcs.12695.

[17] B. Kitchenham, L. Madeyski, and D. Budgen, "SEGRESS: Software Engineering Guidelines for REporting Secondary Studies," *IEEE Transactions on Software Engineering*, vol. 49, pp. 1273–1298, 2023. https://doi.org/10.1109/TSE.2022.3174092.

[18] A. Ożadowicz, "Generic IoT for smart buildings and field-level automation—challenges, threats, approaches, and solutions," *Computers*, vol. 13, no. 2, p. 45, 2024. https://doi.org/10.3390/computers13020045.

[19] I. Mutambik, "AI-driven cybersecurity in IoT: Adaptive malware detection and lightweight encryption via TRIM-SEC framework," *Sensors*, vol. 25, no. 22, p. 7072, 2025. https://doi.org/10.3390/s25227072.

[20] D. Kaushik, P. Gulia, N. S. Gill, and S. Patni, "A blockchain-based security framework for IoT-enabled healthcare systems," in *Proc. 2025 2nd Int. Conf. Computational Intelligence and Computing Applications (ICCICA)*, 2025, pp. 573–579. https://doi.org/10.1109/ICCICA67008.2025.11337680.

[21] J. L. López Delgado and J. A. López Ramos, "A comprehensive survey on generative AI solutions in IoT security," *Electronics*, vol. 13, no. 24, p. 4965, 2024. https://doi.org/10.3390/electronics13244965.

[22] I. Barzev and D. Borissova, "Performance Analysis of LSTM, SVM, CNN, and CNN-LSTM Algorithms for Malware Detection in IoT Dataset," *WSEAS Transactions on Computer Research*, vol. 13, pp. 288-296, 2025. https://doi.org/10.37394/232018.2025.13.27.

[23] W. Ding, S. Wu, and C. Nugent, "A multimodal fusion enabled ensemble approach for human activity recognition in smart homes," *Health Informatics Journal*, vol. 29, no. 2, pp. 1–18, Apr.–Jun. 2023. https://doi.org/10.1177/14604582231171927.

[24] A. O. Ali, M. R. Elmarghany, M. M. Abdelsalam, M. N. Sabry, and A. M. Hamed, "Closed-loop home energy management system with renewable energy sources in a smart grid: A comprehensive review," *Journal of Energy Storage*, vol. 50, p. 104609, 2022. https://doi.org/10.1016/j.est.2022.104609.

[25] M. B. Islam, A. Guerrieri, R. Gravina, and G. Fortino, "A meta-survey on intelligent energy-efficient buildings," *Big Data and Cognitive Computing*, vol. 8, no. 8, p. 83, 2024. https://doi.org/10.3390/bdcc8080083.

[26] Q. He, J. Lin, H. Fang, X. Wang, M. Huang, X. Yi, and K. Yu, "Integrating IoT and 6G: Applications of edge intelligence, challenges, and future directions," *IEEE Transactions on Services Computing*, vol. 18, no. 4, pp. 2471 – 2488, 2025. https://doi.org/10.1109/TSC.2025.3586152.

[27] M. A. Olawumi and B. I. Oladapo, "Enhancing grid stability with machine learning: A smart predictive approach to residential energy management," *Energy and Buildings*, vol. 338, p. 115729, 2025. https://doi.org/10.1016/j.enbuild.2025.115729.

[28] P. Saroha, G. Singh, U. K. Lilhore, S. Simaiya, M. Khan, R. Alroobaea, *et al*., "Dynamic appliance scheduling and energy management in smart homes using adaptive reinforcement learning techniques," *Scientific Reports*, vol. 15, no. 1, p. 24594, 2025. https://doi.org/10.1038/s41598-025-08125-9.

[29] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "An IoT-based smart home automation system," *Sensors*, vol. 21, no. 11, p. 3784, 2021. https://doi.org/10.3390/s21113784.

[30] V. J. Reddi, "Generative AI at the Edge: Challenges and Opportunities," *ACM Queue*, vol. 23, no. 2, pp. 79–137, May 2025. https://doi.org/10.1145/3733702.

[31] S. Chaabene, A. Boudaya, B. Bouaziz, and L. Chaari, "An overview of methods and techniques in multimodal data fusion with application to healthcare," *International Journal of Data Science and Analytics*, vol. 20, no. 4, pp. 3093–3117, 2025. https://doi.org/10.1007/s41060-025-00715-0.