

The Role of Artificial Intelligence in Smart Home Automation

A study on Integration of Artificial Intelligence with IoT in Modern Home systems

Nidhi V Jain, Arpita Singh, Aaradhya Shrivastav
First-Third Undergraduate Student, School of CS & IT,
JAIN University (Deemed-to-be University), Bengaluru, Karnataka, India

Abstract - Artificial Intelligence and Internet of Things (IoT) have converted home into smart homes by facilitating better security and privacy, energy saving, automation and real-time tracking. Studies from year 2019-2025 highlights how AI helped in optimizing energy consumption and easier real-time decision making but also has several security and privacy threats due to weak security of devices, poor compatibility, system failures and user awareness. Edge computing and Machine learning are taking lead in the recent researches to improve protection of data and detect threats or attacks. However, merging of Artificial Intelligence with IoT improves energy efficiency and personalization, challenges like ethical designs, interoperability, security and privacy concerns requires consideration in future evolution.

Keywords- Artificial Intelligence (AI); Internet of Things (IoT); Energy Efficiency; Privacy; Security; Edge computing Real-time Decision making; Machine Learning; Personalisation; Interoperability.

I. INTRODUCTION

Over the past few years, Smart Home Automation has transformed lives of people by connecting everyday home devices with technology by making home more energy efficient, comfortable and safe through automation. Artificial intelligence plays a major role in smart home automation by allowing AI models to learn from user routine and make decisions and also improve security through smart security systems like facial recognition, computer vision and motion detection to detect and identify people or unusual activities. For example, smart lights can detect signals or motions and turn off lights when no one is around, reducing energy usage. However, as many devices are connected via internet, they may be endangered to cyber-attacks and data breach. AI powered cameras or monitoring devices collect personal data raising concerns about privacy and misuse of information. Also sometimes there are compatibility issues as devices from different companies might not work together well. Though the use of Artificial Intelligence and IoT is increasing but the challenges like user trust, high cost and long-term sustainability has limited research. This research study focuses on current technologies, developments, trends and challenges concerning smart home automation. Also focuses on enhancing threat detection, protecting user privacy and preventing cyber-attacks. In Conclusion, though there are certain challenges like privacy risks, cyber threats, data breach and ethical concerns Artificial

Intelligence has made smart home efficient, convenient and secure. In the future development concerns like data protection, data transparency and better device compatibility needs to be addressed.

A. Review of Literature

The study by Guo et al. [1] focused on smart technologies and their impact in the home automation area by focusing on technologies that have been used (or are being used) in smart homes such as federated learning, natural language processing, computer vision, etc., while also highlighting the relationship of smart home research to the theoretical and practical world, such as the need for further clinical and education collaboration between academics and industry.

According to the article Qashlan et al. [2], the authors proposed a method that creates a distributed ledger-based privacy model for smart home systems that; integrates policy-based access control; automates agreements; incorporates edge computing; and employs privacy-preserving methods with the goal of improving data security and protecting user privacy.

The FedHome System [3] provides an example of how to combine decentralized machine learning with a block-chain based solution to provide federated machine learning, ensure confidentiality, and allow for locally optimized automation in smart homes.

To detect patterns that are out of the ordinary in smart homes, Jiang et al. [4] have developed a method of detecting anomalous data points using time-gap analysis.

Buil-Gil et al. [5] identified several issues with smart home cybersecurity by performing standardized evaluations of various problems connected to smart home cyber security like contradictory security models, vulnerable encryption, inadequate user knowledge and inadequate device integration.

Zegeye et al. [6] Wrote about the examined protocols that had been assessed as responses to the issue of integration in smart homes as well as restrictiveness being replicated downwards (back to devices that support devices), and from those devices up (to the comprehensive support of testing).

[7] Proposed a hybridized deep learning network made up of a Combination of CONV-NET and some form of a structural approach to perform detection and face identification.

[8] outlined how an AI powered Smart Home System can improve a user's overall experience, automate user tasks, increase a user's safety through support of good decision-making, and improve the quality of communication between the user and devices.

[9] in this Paper studies some of the current threats to security and Privacy facing IoT within smart homes, and what risks exist as a result of some of the current practices and a lack of user understanding.

[10] examined machine learning methods to address an increasing number of cyber threats, finding deep Learning and combined models contain the best solutions for addressing threats as they continue to evolve. This study presents an AI-based data architecture for IoT Data in a smart home, which provides customised automation to enhance the user's experience via the input of information generated based on the behavior and preferences of individual users as well as device usage, thereby providing for an increased level of user comfort and reduction in the amount of energy used by and response from the user.

The AI-IoT data framework to support adaptive automation is due to user behavior and feedback. The result is enhanced comfort, energy savings and reaction times [11].

Kumar and Singh [12] reviewed the implementation of AI-IoT in smart home security, based on smart monitoring and threat detection, while also presenting barriers for combining distributed edge computing, lower latency and ethical governance of data.

The study performed by Orłowski and Loh [13] takes a look at how to approach data privacy and management by using a privacy management assistant to provide users with a way to monitor compliance across various devices, thereby enhancing transparency and helping designers create user centric products.

Popoola et al. [14] assessed advances in smart homes and privacy systems, identifying advances in data encryption, verification, and usability; they recommend a policy driven, user centric approach in the adoption of these technologies.

Chen [21] examined the compatibility of integration of IoT enabled home systems and developed an efficient framework for devices to communicate while simultaneously addressing the

emerging issues of growing capacity, management of data and the establishment of security protocols.

Shakeri et al. [22] utilized advanced neural networks for intelligent energy management; energy savings in real time; decreased costs; and coordination with sustainable sources of energy.

Two studies have reviewed the implementation of AI and IoT in the home automation industry [23, 25]. They have looked into various parts such as its framework and the different elements of the design of automated home networks, data analytics, and tracking mechanisms. These studies have looked into how AI can improve the response time of systems, protection, platform, performance and usability.

[15] One study has documented how AI and machine learning have improved energy optimization and energy ownership through predictive energy usage by providing automatic control.

[17] Another study has described how AI has improved the functionality and usability of intelligent devices through the use of user modelling.

Ezugwu [18] In addition to these studies, another referenced an independent and autonomously controlled smart home with an integrated AI and IoT system and how this new approach provides for more reactive systems, security and energy management.

Inam Ul Haq et al. [19] In one study, information regarding the transformation of traditional automated homes to intelligent, data-driven homes was presented containing information regarding how AI can be leveraged to provide visionary maintenance and configurations, custom services and enhanced safety for the homeowner.

Al Rawahi [20] AI was again referenced in relation to the way the use of user-focused data can assist in automating the customization of systems as well as creating utility-based comfort for and/or with the user, thus enhancing productivity.

Alshehri [24] Lastly, the author mentioned that an AI solution can be developed to manage energy consumption and to design an AI-based system for reducing energy consumption and to balance comfort with discomfort.

B. Summary Table

Citation no. & Year	Techniques/ Methods approached	Objectives of research	Advantages/ key findings	Limitation/scope
[1] 2019	Machine learning, NPL and Computer vision	To analyse AI techniques enhancing smart-home automation and personalization	Identified AI's impact on personalized automation, predictive maintenance and adaptive energy management efficiency	Need for strong collaboration between academic research and commercial implementation. to accelerate the deployment of AI based smart home system
[2] 2021	Blockchain, attribute-based access control, Differential privacy, and edge computing	To improve data security and privacy concerns in IoT and smart home systems	Achieved data security, privacy and secure communication. Also, the proposed scheme is resilient against modification, DoS attacks, data mining and linkage attacks	Requires validation and implementation on large-scale and research to achieve better privacy and highly protected smart home with better data accuracy
[3] 2022	Federated Learning (FL) and Blockchain	To ensure decentralized and privacy-preserving intelligence in smart homes using BCFL	Requires, optimization of gas consumption, computation overheads and addressing vulnerabilities in smart contracts	Requires, optimization of gas consumption, computation overheads and addressing vulnerabilities in smart contracts
[4] 2022	Temporal learning model, scoring method and anomaly detection	To improve detection of abnormal patterns of smart home activity	Higher accuracy and fewer false alarms	
[5] 2022	Systematic review, PRISMA protocol	To review the overall IoT smart home security issues, concerns, harms and threats globally	Exposed inconsistencies insecurity standards, poor device interoperability and weak encryption mechanisms and limited user awareness	Unified standards and multidisciplinary collaborations to create secure, privacy-preserving smart home ecosystems
[6] 2023	Matter protocol, multi-network integration (WIFI, thread, Bluetooth)	To resolve device interoperability issues in smart home	Improved device compatibility and integration and on-boarding experience	Limited and incomplete legacy device support and large-scale security validation
[7] 2023	CNN models, LR and GBC	To exhibit Capabilities in detecting anomalies, face recognition and integrating them within smart home IoT devices	Has the potential to increase safety and dependability on smart home systems due to high accuracy and capacity and recall of face recognition	Deep Learning, Transfer learning and hybrid approaches.
[8] 2023	AI algorithms for authentication, device control and security enhancement	To integrate AI for home automation and safety	Enabled Real- time decisions and seamless device interaction	Limited to prototype, scalability not fully tested
[9] 2024	Multidisciplinary review	To analyse cyber security and privacy threats	Highlights risk from weak Standards and user ignorance	Need for regulatory and social frameworks
[10] 2024]	Deep learning, Ensemble techniques	To assess ML techniques for smart home malware detection	Identified Ensemble models and deep learning as most effective	Requires real world deployment and testing

[11] 2024	IoT Sensors with AI Algorithms	To enable context aware and adaptive automation systems	Improved safety, energy efficiency and responsiveness	Improved safety, energy efficiency and responsiveness
[12] 2024	Edge computing, AI Surveillance, facial recognition	To enhance smart home system security with real-time analysis	Improved system responsiveness and reduced latency	Interoperability and ethical data issues are still concern
[13] 2024	Centralised privacy management tool	To empower users with control over personal data	Enhanced transparency and user data autonomy	Needs standardization and limited adaption persists
[14] 2024	Review of Encryption, access control and authentication	To identify usability and technological gaps	User friendly designs and advocated regulations	Lacks user studies and real-world testing
[15] 2025	To analyse privacy risks in AI-IoT ecosystem	To analyse privacy risks in AI-IoT ecosystem	Provided standardised privacy-preserving techniques	Need for ethics Frameworks and universal privacy metrics
[16] 2025	Predictive Algorithms, Machine Learning models	To optimize power use and improve sustainability	Improved appliance performance and energy efficiency	Scalability and cost feasibility untested
[17] 2025	Artificial Intelligence for adaptive appliance control	To enhance appliance Sustainability and adaptability	AI learns user behaviour and improves satisfaction	Limited to controlled test environments
[18] 2025	AI driven decision-making integration, Autonomous learning systems	To explore next generation smart homes capable of autonomous adaptation and decision making	Instant response and optimized energy use	Integration complexity and data privacy concerns in adaptive systems
[19] 2025	AI algorithms, data-driven automation, predictive maintenance	To examine how AI enhances personalisation automation and service delivery	Enabled adaptive and Flexible smart home environments that boost safety and efficiency	Requires high quality data and reliable AI model performance
[20] 2025	AI-Analytic, behavioural Data Mining, personalisation models	To use behavioural data for improving automation and personalisation service	Enhanced user satisfaction, convenience, efficiency via adaptive automation	Ethical and privacy issues in behavioural data collection
[21] 2024	IoT communication protocols, device interoperability framework	To design an IoT based system that ensures smooth device communication and adaptability	Improved interoperability and user responsiveness	Challenges with scalability, data management and secure communication
[22] 2024	Deep Neural Networks, predictive energy optimization	To use DNNs for real-time prediction and optimization of energy use	Improved energy efficiency, reduced waste, aligned use with renewable resources	Needs large datasets and high computational power
[23] 2024	Review of system architecture, middleware and AI-IoT integration	To analyse progress and challenges in AI-integrated smart home designs	Highlights AI role in enhancing security, response time, and user adaptability	Real world implementation and interoperability challenges persist
[24] 2025	AI scheduling algorithms, real-time adaptive control	To optimize energy consumption while maintaining user comfort	Demonstrated cost savings and improved sustainability through AI scheduling	Limited scope for standardization and large-scale deployment

II. MATERIALS AND METHODS

This study follows Systematic review approach. Materials refers to the digital academic sources and software tools that were used to collect, organize and evaluate current articles of artificial intelligence in smart home automation from the year 2019-2025.

Methods is the process followed to find, screen, extract, sort, compare and arrange data from the selected research papers.

A. Materials:

1. Digital Databases

This review is mainly based on academic papers from big science

databases and platforms that heavily cover AI, IoT, security and smart home tech. We used the following sources to find relevant articles: IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, ACM Digital Library, MDPI journals, Google Scholar, Scopus indexed journals and arXiv preprint server. For these platforms combined, we had access to peer-reviewed journal posts, meeting papers and good preprints in computer science, engineering and new tech areas. Access required for full systematic review of this area.

2. Software and Tools

For this study some software helped with paperwork, and looking at the articles and no lab work or gear was made. Tools like Microsoft Word, Microsoft Excel, Google Sheets, and Google Docs were used to write, change and prepare the report, like the summary chart and description. Reference tool Mendeley was used for gathering paper info, removing copies and made citations and reference list in a standard way. Writing tools like Grammarly and other proofreading software were used to improve the writing style and avoiding copying.

3. Selection Material

25 peer-reviewed papers were used for this study using keywords like Artificial Intelligence, Machine Learning, Deep learning, IoT, and Smart home automation. Also, words like security, privacy, energy use, automation and connection were used to find the study materials. We only used articles that matches the topic and used sufficient methods or technology info.

B. Methods:

1. Literature Identification

We used specific keyword combos like “Artificial Intelligence”, “IoT”, “Smart Home”, “Security”, “Privacy”, “Blockchain”, etc. Limited results to peer-reviewed papers were used by applying date filters to show studies only from the year 2019 to 2025. non-academic sources were excluded. For further review studies clearly about AI/ML in smart homes were focused.

2. Screening and Eligibility

Papers were reviewed by following three steps: title, abstract and full text review. Titles that were not related to smart homes or Artificial Intelligence or IoT were excluded. Academic papers that had clear techniques and methods with results were included. Irrelevant papers or studies from blogs, magazines, etc. were excluded.

3. Data Extraction

A standard method was used to collect key details from each study such as methods related to AI, Smart home, IoT, research aim, results and limitations/gap. We created a summary table for better and easy analysis of the study.

4. Categorization and Thematic analysis

After analyzing the study, we figured out five topics like:

- AI Security in Smart Homes
- AI privacy and ethical considerations
- Energy consumption
- Legal platforms/software and connectivity
- User friendly.
- Comparison of each topic were made to find advantages,

disadvantages and drawbacks from the study.

5. Comparative Method

Comparison of models, data types, technology, methods, test results and use cases in terms of AI were made to analyse what gaps were present in the current solutions and what worked best. The comparison also highlighted how technology like IoT models work in smart home automation.

6. Synthesis and Interpretation

After the overall comparisons of studies, findings were combined to give an overall view of AI works in smart home, challenges faced like compatibility, cost, privacy and security, and how current technologies can be implied like deep learning, edge computing, privacy-preserving methods). we also highlighted future scopes for further research directions.

7. Ethical Considerations

Ethics were followed through the research by using the research in the right way and being honest in the review. No people or personal data were used. All the sources were cited and used only licensed or public academic materials. We followed the research ethics by avoiding plagiarism or any duplication of data.

III. RESEARCH METHODOLOGY

This study follows a descriptive and exploratory research methodology to understand how artificial intelligence is being used in smart home automation. Instead of creating a new system or conducting technical experiments, this research focuses on examining existing academic studies in this field.

1. Research Design

The research is of a qualitative and descriptive design. The aim of this design is to acquire an explicit understanding of the role of Artificial Intelligence in smart home automation. The study was focused mainly on areas including home security, energy efficiency and user convenience. This research is based on previously published studies; hence no surveys, experiments, or primary data collection methods were used. The analysis is based on review and interpretation of existing research findings (not new research).

2. Data sources

The data in this study is secondary data sources. Research papers and journal articles were collected from well-known academic databases and digital libraries. These are the journals indexed in IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, MDPI journals, Google Scholar, arXiv and Scopus.

3. Search Strategy

The suitable research papers were identified for the study by a keyword-based search strategy. keywords used in the search process included: Artificial intelligence in smart homes, privacy and security. Search results were filtered to include only research articles published from 2019 to 2025

IV. .DATA ANALYSIS

In this study 25 research papers were reviewed and selected to understand the uses and challenges of Artificial Intelligence in smart home systems. The main aim of this study was to note the

key challenges faced, results, advantages and disadvantages and drawbacks for the better understanding of the study.

1. Thematic analysis

After analyzing the selected research papers, the information was grouped into several major themes for better understanding of the role of Artificial Intelligence in smart home automation. The main themes identified in the literature include security, privacy, energy efficiency, device compatibility, and user experience.

2. AI techniques Identified in the Literature

The literature review shows that different Artificial Intelligence techniques are used in smart home systems.

- Machine learning algorithms are commonly used to support decision-making and automate device control.
- CNN/Deep learning models are widely applied in smart cameras and facial recognition systems to improve security.
- LSTM/Time based models help in understanding user behaviour and detecting unusual activities.
- Federated learning for training AI models and also ensuring protection of user data from data breaching.
- Block-chain AI to enhance security through decentralized control and logging.

3. Findings

The analysis of the studies reviewed shows that Artificial Intelligence plays an important role in improving the performance of smart home systems. AI-based technologies can help improve home security by detecting unusual activities and reducing false alarms. They also help in energy consumption management, by controlling the household appliances automatically according to the user behavior and environmental conditions.

4. Outcome of the literature review

The review of the research points out that Artificial Intelligence has the potential for a substantial improvement in the functioning of modern homes. AI technologies enable us to automate numerous daily activities, enhance security systems and optimize energy consumption. Therefore, smart homes can be more efficient, Convenient and comfortable for users.

5. Key insight

The studies reviewed show that AI-based smart home systems function well in experimental or controlled environments. But there are still some limitations to their practical use in everyday home situations. There is a need for further improvements in areas such as data protection, interoperability between devices and system stability.

V. CONCLUSION

The study highlights that Artificial Intelligence is increasingly being integrated into modern smart home systems. AI can improve home security, help people consume less energy and make daily life easier for users. Machine learning, Deep Learning, and other AI techniques and technologies can be used to train smart devices to learn user behavior and automatically respond to it. Merging of Artificial Intelligence with IoT helps

different devices in home to operate, connect and communicate in a smarter, easier and responsive to use and manage. There are certain challenges like data privacy, breaching of data, cyber threats and compatibility between different devices that needs to be addressed and improvised for better adaptation with the changing technologies in smart home automation. However, there are also real time scalability testing issues as most testing's are done in controlled environments instead of real-time home testing. In conclusion, Artificial intelligence will play a major role in future development of smart home automation. Smart home systems can become more reliable with better and stronger privacy and security measures and improved device compatibility and device adaptability.

VI. REFERENCES

- [1]. F. Guo, L. Zhu, and X. Wang, "Artificial Intelligence in Smart Homes: A Comprehensive Review of Applications, Techniques, and Challenges," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 3, pp. 1157–1175, 2019.
- [2]. A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021. doi: 10.1109/ACCESS.2021.3098795
- [3]. R. Reis and R. Seródio, "Federated Learning for Privacy-Preserving Smart Home Systems," *arXiv preprint arXiv:2012.07450*, 2022.
- [4]. C. Jiang, C. Fu, Z. Zhao, X. Du, and Y. Ji, "Effective Anomaly Detection in Smart Home by Integrating Event Time Intervals," *arXiv preprint arXiv:2201.07954*, 2022.
- [5]. M. Buil-Gil, J. Miró-Llinares, and E. Moneva, "Cybersecurity Challenges in Smart Homes: A Systematic Literature Review," *Computers & Security*, vol. 120, p. 102845, 2022.
- [6]. W. Zegeye, A. Jemal, and K. Kornegay, "Connected Smart Home over Matter Protocol," in *Proc. IEEE Int. Conf. Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2023, pp. 1–7.
- [7]. A. Alshamsi, R. Almarzooqi, and K. Alnaqbi, "Machine Learning Approaches for Malware Detection in Smart Home Environments: A Systematic Review," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1450–1465, 2024.
- [8]. "Design and Implementation of an AI-Powered Smart Home System," *Res. Inventy: Int. J. Eng. Sci.*, vol. 13, no. 6, 2023.
- [9]. M. Fauzi, A. Rahman, and N. A. Zulkifli, "Privacy and Security Challenges in IoT-Based Smart Homes: A Comprehensive Review," *IEEE Access*, vol. 12, pp. 45678–45695, 2024.
- [10]. A. Alshamsi, R. Almarzooqi, and K. Alnaqbi, "Machine Learning Approaches for Malware Detection in Smart Home Environments: A Systematic Review," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 1450–1465, 2024.
- [11]. M. N. Varadarajan, C. Viji, N. Rajkumar, and A. Mohanraj, "Integration of AI and IoT for Smart Home Automation," *SSRG Int. J. Electron. Commun. Eng.*, vol. 11, no. 5, pp. 37–43, 2024.
- [12]. S. Kumar and T. Singh, "AI and IoT Integration for Smart Home Security: A Review of Emerging Techniques and Challenges," *Int. J. Adv. Computer. Sci. Appl.*, vol. 15, no. 5, pp. 88–96, 2024.
- [13]. J. Orłowski and P. Loh, "Privacy Meta-Assistant: Enhancing User Autonomy in Smart Home Environments," *IEEE Trans. Consume. Electron.*, vol. 70, no. 1, pp. 34–45, 2024.
- [14]. O. Popoola et al., "A Critical Literature Review of Security and Privacy in Smart Homes," *ScienceDirect*, 2024.
- [15]. A. Sharma and R. Verma, "Privacy Information Disclosure in AI-Integrated IoT Systems: A Systematic Literature Review," *IEEE Access*, vol. 13, pp. 2245–2268, 2025.
- [16]. A. C. Ikegwu et al., "Investigating the Impact of AI/ML for Monitoring and Optimizing Energy Usage in Smart Home," *Adv. Inf. Eng.*, Jan. 2025.
- [17]. "A Study on Smart Home Appliances Based on Artificial Intelligence," *J. Inf. Syst. Eng. Manag.*, Jan. 2025.
- [18]. A.E. Ezugwu, "Smart Homes of the Future," *Transactions on Emerging Telecommunications Technologies*, 2025.
- [19]. M. Inam Ul Haq, M. Naveed, A. Ahmad, and S. Kumar, "Shaping the Next Generation of AI-Integrated Smart Homes," *Scholars Journal of Engineering and Technology*, vol. 13, no. 8, pp. 644–656, Aug. 2025
- [20]. A. Al Rawahi, "Analyze user behavior to improve Smart Home services," *Procedia Computer Science*, vol. 228, pp. 788–796, 2025.
- [21]. Y. Chen, "Design and implementation of smart home system based on IoT,"

- Internet of Things and Cyber-Physical Systems, vol. 8, pp. 105–116, 2024.
- [22] R. Shakeri, S. Hosseinian, and M. Damghani, "Smart energy management: real-time prediction and optimization for smart home and grid with DNN," Cogent Engineering, vol. 11, no. 1, Dec. 2024.
- [23] P. Sutar, N. Kulkarni, and S. Nayak, "A Review on IoT-Enabled Smart Homes Using AI," in Proc. 15th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), Kamand, India, Jun. 24–28, 2024, Art. no. 10723321.
- [24] M. Alshehri, "Artificial intelligence-driven energy optimization in smart homes and buildings," Heliyon, vol. 11, no. 5, May 2025.
- [25] M. Inam Ul Haq, M. Naveed, A. Ahmad, and S. Kumar, "Maximizing energy savings in smart homes through artificial neural networks," Computational Engineering, vol. 9, no. 2, pp. 140–155, Feb. 2025.