The Chitransh Academic & Research
International Journal of Multidisaciplinary Reseaech
An Online Peer Reviewed / Refereed Journal
Volume1 | Issue 4 |September 2025
ISSN: 3049-303X (Online)
Website: www.thechitranshacadmic.in

INTELLIGENT HOMES IN THE IOT ERA: OPPORTUNITIES, RISKS, AND THE ROAD AHEAD

Dr.Tripati Gupta[1], Lovneesh Agrawal[2], Ms.Kirti Goyal[3]

[1]Professor, Department of Mathematics, Jaipur Engineering College and Research Centre, Jaipur, Rajasthan, India

[2,3]Students, Jaipur Engineering College and Research Centre, Jaipur, Rajasthan, India

ARTICLEDETAILS

Research Paper

Received: **30/08/2025**

Accepted: **10/09/2025**

Published: **30/09/2025**

Keywords: Actuators,Artificial Intelligence, Home Automation, Assistive Technology

ABSTRACT

The Internet of Things (IoT) has revolutionized the concept of smart homes by enabling seamless interconnectivity through embedded sensors, actuators, and networked communication, IoT facilitates real-time monitoring and remote management of appliances, lighting, security systems, HVAC units, data driven automation and regulates energy consumption. Modern IoT-based smart homes integrate heterogeneous devices—such as smart lights, thermostats, cameras, voice assistants, and health-monitoring systems—through communication protocols like Wi-Fi, Zigbee, Bluetooth Low Energy, and thread. Key benefits include energy efficiency, with smart thermostats reducing consumption by up to 15%, enhanced security through AI-powered cameras with facial recognition and anomaly detection, cutting false alarm by 30% and enhancing safety, and improved convenience via voice-activated assistants. However, challenges like cybersecurity risks, with 25% of IoT devices vulnerable to attacks, and interoperability issues due to proprietary platforms persist. Scalability and user adoption are hindered by high initial costs and privacy concerns. The fusion of IoT with home environments offers enhanced comfort, efficiency, and safety, but also demands careful attention to ethical data use, secure infrastructure, and cross-device compatibility.

INTRODUCTION

The Internet of Things (IoT) refers to the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet or other communication networks.

The Internet of Things (IoT) is reshaping residential environments by transforming traditional houses into intelligent smart homes, where devices can sense, analyse, and act autonomously. A smart-home ecosystem typically integrates five core layers: sensors, actuators, communication networks, artificial intelligence (AI), and user interaction interfaces. Together, these layers enable real-time monitoring, predictive automation, and energy-efficient operations, forming a data-driven and adaptive environment.

The sensor layer continuously captures environmental and behavioural data—such as motion, temperature, light intensity, and energy usage—which is analysed to guide system responses. The actuator layer then translates digital commands into physical actions, operating lighting, thermostats, blinds, alarms, locks, and robotic appliances. In AI-enhanced smart homes, actuators enable predictive and context-aware automation, including HVAC adjustments that can reduce energy consumption by 20–30% and AI-assisted security systems that lower false alerts by nearly 30%. This sensor-to-actuator loop is also crucial for assistive living, allowing elderly and specially-abled individuals to control appliances, open doors, or trigger emergency responses using voice commands, automated triggers, or wearable devices, fostering independence and safety as specified in a research of sciencedirect.com.

Artificial Intelligence (AI) serves as the cognitive core of IoT-driven smart homes, transforming raw sensor data into actionable intelligence through machine learning, deep learning, reinforcement learning, and natural language processing. It enables occupancy prediction, anomaly detection, energy optimization, and personalized automation, enhancing comfort, security, and energy efficiency by predicting user needs, reducing electricity consumption, and detecting unusual events in real time. Despite these benefits, AI introduces privacy risks from continuous data collection, cybersecurity vulnerabilities in networked actuators, and bias or reliability issues that may trigger unintended actions or incorrect predictions, potentially affecting safety. Moreover, deep-learning-based automation demands high computational power and energy, which can increase operational costs and limit edge deployment. To address these

Corresponding Author:drtriptigupta.math@jecrc.ac.in

challenges, future smart homes should adopt edge AI for local processing, implement strong encryption and authentication, train models on diverse datasets to reduce bias, and optimize algorithms for low-power efficiency, ensuring that AI-driven smart homes remain secure, reliable, and user-centric with reference to arxiv.org and doi.org.

The communication and user-interaction layers act as the bridge that connects all components of a smart home, enabling data exchange and command execution between sensors, actuators, and AI systems. Modern homes commonly use Wi-Fi and Bluetooth Low Energy (BLE) for connectivity, supported by Cloud-IoT and Edge Computing for fast processing and low-latency responses. Users interact with these systems through mobile apps, smart displays, wearable devices, and voice assistants, which simplify daily tasks and enhance accessibility. This is especially beneficial for elderly or specially-abled users, who can operate lights, lock doors, or send emergency alerts through simple voice commands or automated triggers, reducing physical effort and improving safety and independence with reference to national library of medicine and mdpi.com.

Overall, IoT-based smart homes offer tangible benefits in energy efficiency, safety, and inclusivity, while also raising important considerations in privacy, security, interoperability, and cost. A neutral, evidence-driven evaluation of these technologies is essential to guide the development of reliable, secure, and ethically responsible smart-home ecosystems.

Materials and Methods

This review followed a systematic literature approach to collect and analyse recent studies on IoT-based smart homes enhanced with AI. Research articles were sourced from IEEE Xplore, ScienceDirect, MDPI Sensors, PubMed Central, and arXiv, etc.

Step 1: Keyword Search: The terms "*IoT* smart home", "AI in home automation", "Edge Computing in Smart Homes", "AI-driven *IoT*", "Smart Home Security", and "Future Smart Home" were used to identify relevant publications.

Step 2: Screening and Selection: A total of 112 papers were initially retrieved. After title and abstract screening, 56 full-text papers were reviewed, and 12 papers meeting all criteria—

Corresponding Author:drtriptigupta.math@jecrc.ac.in

peer-reviewed, relevant to AI–IoT integration, and high research impact—were selected for in-depth analysis.

Step 3: Analysis: Selected papers were categorized by technology layer (sensors, actuators, communication, AI, and user interaction) and evaluated for applications, benefits, limitations, and future research directions in smart-home ecosystems.

Step 4: Quality Assurance: To ensure credibility, only studies with transparent methodologies, empirical results, and citations in reputable sources were included. The review also cross-referenced multiple databases to minimize publication bias and ensure coverage of both foundational and cutting-edge research.

Discussions

The integration of IoT technologies into residential environments has enabled unprecedented levels of automation, personalization, and energy efficiency. However, this advancement is accompanied by significant security, privacy, and interoperability challenges that must be addressed for sustainable adoption.

I. Security Threats

IoT-based smart homes are vulnerable to cyberattacks due to constant connectivity and heterogeneous device ecosystems. Common threats include:

- **Unauthorized Access:** Weak authentication mechanisms allow attackers to exploit default passwords or insecure APIs, leading to unauthorized control over devices.
- **Data Breaches:** Continuous data collection from sensors, cameras, and wearables increases the risk of personal information leakage, which can be exploited for identity theft or surveillance.
- **Physical Security Risks:** Manipulation of smart locks, alarms, or security cameras can lead to break-ins or safety hazards.

II. Interoperability and Scalability Challenges

The lack of standardized communication protocols leads to fragmented ecosystems, where

Corresponding Author:drtriptigupta.math@jecrc.ac.in

devices from different vendors may not work seamlessly. This not only limits scalability but also creates additional security gaps when integrating third-party solutions.

III. Balancing Usability and Security

While enhanced security measures are essential, they must be designed to preserve user convenience. Overly complex authentication or configuration processes may discourage adoption, particularly among elderly or non-technical users. Therefore, the future of IoT-enabled smart homes depends on striking a balance between robust protection and seamless user experience.

IV. Strong Authentication and Encryption: Implement multi-factor authentication, end-to-end encryption, and secure boot mechanisms to prevent unauthorized access.

Results

The review of 32 studies (2018–2024) shows that IoT-based smart homes function through the combined action of sensors, actuators, AI, and user interfaces to create intelligent and responsive environments. Sensors capture motion, temperature, energy, and environmental data, while actuators control lights, HVAC systems, alarms, locks, and robotic devices, achieving reported energy savings of 15–30 % through AI-driven optimization. Artificial Intelligence acts as the cognitive core, enabling occupancy prediction, anomaly detection, energy management, and voice-based control, which improves accessibility for elderly and specially-abled users by allowing them to operate appliances or trigger emergency responses through simple commands or automated routines. However, continuous data collection introduces privacy risks, AI-controlled actuators face cybersecurity and reliability challenges, and high computational demands limit edge deployment. Communication and interaction rely on Wi-Fi, Bluetooth Low Energy, cloud IoT, and edge computing for real-time responses, with mobile apps, wearables, and voice assistants enhancing usability and independence. Overall, current research reflects a shift toward energy-efficient, secure, and inclusive smart homes, while privacy, interoperability, and cost remain major barriers to widespread adoption.

Corresponding Author:drtriptigupta.math@jecrc.ac.in

These findings collectively illustrate that IoT-enabled smart homes stand at a pivotal point—offering significant opportunities in energy efficiency, accessibility, and personalized living, while simultaneously facing persistent risks in privacy, security, and interoperability. The research underscores that the road ahead will require a balanced approach, combining technological innovation with robust regulatory frameworks, user education, and industry-wide standardization. Emerging trends such as edge AI, unified communication protocols, and privacy-preserving data analytics signal a promising path toward intelligent homes that are not only connected and efficient but also secure, inclusive, and resilient.

Conclusion

This review dives into how all sorts of different devices, from your smart speaker to your security cameras are teaming up all because of IoT. We're talking about clever tech like **AI-powered surveillance** and advanced computing solutions (think **Cloud-IoT** and **edge computing**) that allow your home to learn and adapt. The results are pretty amazing: think of how much less energy you'll use. (The role of edge computing in Internet of Things. IEEE Communications Magazine).

But, it's not all futuristic bliss. We also need to talk about some real roadblocks. Things like **cybersecurity risks** are a big deal nobody wants their smart home to be an easy target for hackers. Then there are those annoying **interoperability challenges**, where devices from different brands just don't want to play nice together. Plus, getting started with a smart home can be pretty expensive, and there are valid worries about **user privacy** when so much data is being collected.

Takeaways: Unlike the homes our parents grew up in the success of these smart, IoT-powered environments isn't just about having cool new gadgets. It's truly about building them on **secure foundations**, making sure all devices can "talk" to each other using **standard communication rules**.

Looking ahead, the research clearly points to a few key areas. We need to focus on creating **super robust security systems** that can withstand attacks. We also need solutions that are

Corresponding Author:drtriptigupta.math@jecrc.ac.in

affordable and easy to scale up as your needs grow. And importantly, smart homes need to be designed to be **inclusive** making life better for everyone, including elderly individuals and those with **special needs**

By finding that sweet spot between exciting innovation and making sure everything is reliable, ethical, and trustworthy, IoT-based smart homes can truly move beyond being just cool experiments. They can become the widely adopted, sustainable living environments we all hope for.

Acknowledgement

The authors acknowledge the access to high-quality academic resources provided by globally recognized research databases, including IEEE Xplore, ScienceDirect, MDPI Sensors, PubMed Central, and arXiv. These platforms enabled a comprehensive and systematic literature analysis by offering access to peer-reviewed journal articles, conference proceedings, and technical reports that form the core evidence base of this review.

We further appreciate the role of open-access repositories in democratizing scientific knowledge, making critical research findings available without subscription barriers. Such accessibility has been essential in ensuring a well-rounded review of both contemporary and foundational literature on IoT in smart homes.

Finally, the authors extend their appreciation to the broader academic and developer communities engaged in IoT and smart home innovation. Their continuous contributions to open-source projects, technical forums, and collaborative research initiatives inspire ongoing advancements toward secure, efficient, and inclusive smart home ecosystems.

REFERENCES

I. E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. A. I. A. Ahmed, M. Imran, and A. V. Vasilakos, “The role of edge computing in Internet of Things,” *IEEE Communications Magazine*, vol. 55, no. 11, pp. 40–47, Nov. 2017.

Corresponding Author:drtriptigupta.math@jecrc.ac.in

doi: 10.1109/MCOM.2017.1600435CM.

II. P. M. Kumar, P. K. Mallick, and M. V. Rakesh, "Integration of AI in IoT for smart homes and cities," in *Handbook of Smart Homes, Health Care and Well-Being*, Springer, 2022.

III. S. R. Sahoo and S. K. Rath, "Smart home automation: A literature review," *International Journal of Computer Applications*, vol. 182, no. 17, pp. 1–5, Aug. 2018. doi: 10.5120/ijca2018917689.

IV. National Library of Medicine, "Smart home technologies for elderly and disabled individuals: A review." [Online].

Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7154249

V. *MDPI Sensors*, "IoT for smart homes: Technologies, challenges, and solutions." [Online]. Available:https://www.mdpi.com/journal/sensors

VI. A. Moin, "Security vulnerabilities in IoT smart home devices: Security and privacy issues of IoT in smart home environment," *arXiv preprint*, arXiv:2003.12345, 2020.