IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, December 2025
Impact Factor: 7.67

Smart Home Automation Using IoT and AI

Amol Darekar[1], Om Auti[2], Vedant Ghadge[3], Prof. P. B. Palve[4]
Student, Department of Computer Engineering[123]
Professor, Dept. of Computer Engineering[4]
Adsul Technical Campus, Chas, Ahilyanagar, Maharashtra, India

Abstract: *This research dives into the integration of Artificial Intelligence (AI) and the Internet of Things (IoT) into our living spaces, specifically in Smart Home Automation. We set out to understand this transformative technology's benefits, challenges, and ethics. Through a systematic review of sources (2023-2025), a clear duality emerged: The biggest benefits of AI-driven homes—like hyper-personalization, energy efficiency, and predictive safety—are deeply tied to their biggest risks. We found the main challenges are technical (interoperability), security-based (IoT botnets), and privacy-related (data surveillance). The paper also confronts the core ethical problems: loss of user autonomy, continuous surveillance, and data ownership. Our conclusion? A "set it and forget it" model isn't the answer. The future lies in a Human-in-the-Loop model, where local processing (Edge AI) and robust security protocols are the most valuable parts of the process. This paper frames these findings to help navigate this new landscape responsibly.*

Keywords: Smart Home Automation, Internet of Things (IoT), Edge AI, Energy Management, Data Privacy, Predictive Maintenance, Systematic Literature Review

I. INTRODUCTION

The Smart Home Paradigm Shift We are in the middle of a massive paradigm shift in how we live. We have moved from "Connected Homes"—where you simply use your phone as a remote control for lights—to "Cognitive Homes" that actively think, listen, and predict. Unlike traditional automation, which relied on rigid rules we had to program ourselves, modern AI-integrated systems learn our habits, anticipate our comfort, and optimize our environment without us lifting a finger. The universal adoption of protocols like Matter in late 2024 was a lightning rod for this industry, finally allowing devices to talk to each other and kicking off an unprecedented wave of innovation. This technology is no longer a futuristic concept; it is already woven into the fabric of our daily lives.

The Central Research Problem: Convenience vs. Control However, the speed of this adoption has left our understanding in the dust. We have a massive gap between what these devices can do and how we secure them. We are essentially in a race to fill our private spaces with "ever more intelligent sensors" that not even their manufacturers can fully secure against emerging threats. This race has split the conversation into two camps: those who see a utopia of effortless living and those who warn of a "panopticon" of constant surveillance.

This paper argues that the central problem isn't just a list of "pros and cons." It is that these factors are interdependent. The most powerful benefits of Smart Homes seem to be causally linked to their most significant harms.

• The amazing ability to "predict user needs" (like adjusting the heat before you arrive) is built on the ethically troubling foundation of "continuous behavioral profiling."

• The massive convenience of "seamless voice control" is the very thing causing the critical risk of "always-listening microphones" and potential eavesdropping.

• The benefit of "cloud-based processing" for heavy AI tasks is the direct cause of security threats like "data breaches," exposing sensitive footage to the world.

Objectives and Structure

This paper aims to cut through the hype. Using a Systematic Literature Review (SLR) and a critical analysis of the current 2024-2025 research, we will:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, December 2025 Impact Factor: 7.67

1. Analyze the documented benefits of AI-driven automation, focusing on energy efficiency, predictive maintenance, and health monitoring.
2. Examine the significant challenges to its use, including interoperability issues, latency, and the "black box" nature of AI decision-making.
3. Critically evaluate the core ethical implications, specifically algorithmic bias in security systems and the erosion of privacy within the home. The paper will conclude by pulling these findings into a framework for human-centric governance and identifying what we need to research next. The structure follows the standard academic format: a Literature Review, Methodology, Analysis of Findings, Discussion, and Conclusion.

II. LITUREATURE REVIEW

Defining the Technology: From Sensors to Brains So, what is the AIoT? It is the fusion of two powerful fields: IoT acts as the "nervous system" (collecting data via sensors), and AI acts as the "brain" (making decisions). It is built on "Edge Computing" and "Machine Learning" models. Traditional smart homes used simple IF-THEN logic (e.g., If motion is detected, turn on the light). Modern AIoT uses Predictive Analytics to understand context (e.g., If motion is detected at 2 AM, turn on lights at 10% brightness to avoid blinding the user).

Current State of Research (2024-2025) Lately, the research has shifted. We have moved past just proving that we can connect devices to the internet; now we are studying the impact of doing so. The big theme in recent literature is balancing efficiency with profound security responsibilities.

This brings us to a central "Autonomy Paradox." On one side, 2025 data shows that AI-optimized homes reduce energy consumption significantly (approx. 30%). But there's a catch. The same studies found this automation had a negative effect on user control; users often felt "powerless" when the house made decisions they didn't understand. Other researchers back this up, noting AI's tendency to "misinterpret irregular human behavior" (like a party or a sick day) as an anomaly to be corrected. This paper is built around that core paradox: The Smart Home helps us manage life, but it may be eroding our privacy and sense of control.

III. METHODOLOGY

A Framework for Synthesis To tackle this, we used a Systematic Literature Review (SLR) combined with a Critical-Conceptual Analysis. This hybrid approach was necessary because this field moves incredibly fast and crosses many disciplines—computer science, electrical engineering, and sociology. A simple technical review wouldn't capture the connected legal and ethical impacts.

Data Collection and Analysis The sources we reviewed were curated to represent a high-quality, 2023-2025 snapshot of the field. This corpus included academic databases (IEEE, ACM), industry analysis (IoT Analytics reports), and security white papers.

• Stage 1 (Coding): We reviewed sources to tag concepts like "interoperability," "energy efficiency," "data leakage," and "Edge AI."
• Stage 2 (Synthesis): We grouped these into Benefits, Challenges, and Ethical Implications.
• Stage 3 (Critical Synthesis): We looked for causal links (e.g., how cloud dependency causes latency and privacy risks).

IV. SYSTEM ARCHITECTURE (FINDINGS)

The New Engine of Living: Benefits of AI/IoT Integration The literature overwhelmingly paints AIoT as a powerful engine for sustainability and health.

1. Efficiency and Sustainability: The most obvious benefit is Energy Management. AI thermostats don't just hold a temperature; they "learn the thermal properties" of a house. They know how long it takes to heat up and cool down, and they cross-reference this with weather forecasts to optimize HVAC usage. This creates huge reductions in electricity bills and carbon footprints.

2. Hyper-Personalization and Health: AI is getting us closer to the "holy grail" of Ambient Assisted Living (AAL). For elderly users, the home becomes a caregiver. Wearables and wall sensors use "gait analysis" to predict falls before they

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, December 2025 Impact Factor: 7.67

happen. The home can "interpret vital signs" and alert doctors in real-time, allowing seniors to maintain independence for longer.

3. Predictive Maintenance: Just as AI predicts car engine failures, Smart Homes now predict appliance failure. By analyzing the "vibration and power draw" of a washing machine or fridge, the AI can alert the user to a part needing replacement before the appliance breaks.

Case Studies in Practice This isn't just theory; the literature highlights successful real-world implementations of AIoT.

• Google Nest: The integration of AI learning algorithms in Nest thermostats has been shown to save customers an estimated 10-12% on heating and 15% on cooling bills by automatically adjusting to user schedules.

• Samsung SmartThings: Their AI Energy Mode monitors energy consumption in real-time and automatically switches appliances to low-power modes when not in use.

• Amazon Alexa: The "Hunches" feature uses predictive AI to alert users if they left a door unlocked or a light on, demonstrating the shift from passive control to active, predictive safety.

Points of Friction: Challenges in Implementation The review also identified major technical and economic roadblocks.

1. Interoperability and Fragmentation: Despite the launch of the Matter protocol to unify devices, "legacy environments" still exist. A home might have 50 devices from 10 different brands (cameras, bulbs, locks) that struggle to communicate. This requires complex "bridge" hardware and creates a fractured user experience.

2. Latency and Bandwidth: Cloud-based AI requires sending data to a server, processing it, and sending a command back. This introduces Latency. In critical scenarios (like a smart lock detecting an intruder or a fire alarm), milliseconds matter. "Cloud dependency" also means if the internet goes down, the "smart" home becomes "dumb."

3. Security Vulnerabilities: The "attack surface" of a home expands with every new device. Cheap smart bulbs often have "weak firmware security," acting as an entry point for hackers to access the entire network.

The Glass House: Core Ethical Implications

1. Privacy and Surveillance: Here is that paradox again: Personalization requires Surveillance. To work effectively, the house must know when you sleep, what you eat, and who visits you. This is a system of "intimate surveillance." The risk is the "monetization of behavioral data"—where device manufacturers sell your living habits to advertisers or insurance companies.

2. Autonomy and Dependence: As algorithms increasingly influence home decisions (locking doors, dimming lights), the impact falls on human agency. Users may become "over-reliant" on the system, losing the ability to manage their home manually. Furthermore, if an AI "hallucinates" a threat (e.g., falsely identifying a family

3. member as an intruder), it can cause physical lockouts or false police alarms.

V. DISCUSSION

The Inescapable Interlock: Reconciling Benefits and Risks The findings show us this isn't a simple "upgrade." It's a trade-off. The core value of the Smart Home—its ability to anticipate needs—is the same mechanism that produces its core risk: the erosion of privacy. We can't just "install IoT" as a simple tool. We have to treat it as a sensitive ecosystem.

The Privacy-by-Design Imperative Our review leads to one critical conclusion: Cloud-centric architectures are too risky for the future. The future lies in Edge AI (processing data locally on the device). If a camera analyzes a face, it should do so on the chip, not by sending the video to a server. This minimizes data leakage.

Table 1: Synthesis of Challenges, Risks, and Solutions

Domain	Identified Challenge / Risk	Causal Factor	Proposed Mitigation Strategies
Privacy	Data Leakage / Surveillance	Cloud-based processing of sensitive video/audio.	Edge Computing: Process data locally on the device (On-device AI).
Security	IoT Botnets / Hacking	Weak default passwords; unpatched firmware.	Network Segmentation: Keep IoT devices on a separate Wi-Fi

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, December 2025 Impact Factor: 7.67

Domain	Identified Challenge / Risk	Causal Factor	Proposed Mitigation Strategies
			network (VLAN).
Interoperability	Fragmented Ecosystems	Proprietary protocols (locking users to one brand).	Matter Protocol: Adoption of universal open-source standards.
Reliability	Internet Dependency	AI logic lives in the cloud.	Local Fallback: Critical functions (locks, lights) must work offline.

VI. CONCLUSION

Principal Conclusions This review set out to make sense of AI and IoT in the home. We found that the Smart Home is not just a collection of gadgets; it is an intelligent entity. It offers transformative benefits in energy efficiency, elderly care, and convenience. However, these benefits are inextricably linked to significant technical and ethical challenges. The technology's reliance on data creates inherent risks of surveillance, and its complexity creates security holes for hackers.

Our central conclusion is that the successful integration of Smart Home technology is not a technical problem, but a trust problem. The future of home automation will be defined by Local Intelligence. In this new paradigm, the most valuable systems will be those that offer the benefits of AI (prediction/automation) without the privacy cost of the Cloud.

Directions for Future Research

1. Edge AI Efficiency: Research must accelerate into smaller, more efficient models (TinyML) that can run on low-power chips inside lightbulbs and switches.
2. Standardized Security Labels: We need a "Nutrition Label" for IoT security, helping consumers understand what data a device collects before they buy it.
3. Long-term Psychological Impacts: We need studies on the long-term cognitive effects of living in fully automated environments—does it reduce stress, or increase anxiety about surveillance?

REFERENCES

[1]. Stojkoska, B. L. R., & Trivodaliev, K. V. (2024). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production.
[2]. Matter Alliance. (2024). The State of Smart Home Interoperability: 2025 Report. Connectivity Standards Alliance.
[3]. Gartner, Inc. (2025). Emerging Trends in IoT and Edge AI. Gartner Research.
[4]. Islam, S. M. R., et al. (2023). Internet of Things (IoT) and AI in Energy Management: A Survey. IEEE Access.
[5]. Mozilla Foundation. (2024). Privacy Not Included: A Guide to Connected Gadgets.
[6]. DarkReading. (2025). The Rise of IoT Botnets: Security Challenges in the Modern Smart Home.
[7]. McKinsey & Company. (2024). The Connected Home Market: Opportunities and Risks in 2025.
[8]. U.S. NIST. (2023). IoT Device Cybersecurity Capability Core Baseline. NISTIR 8259.