International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Internet of Things (IoT) as a Driver of Domestic Automation Opportunities, Challenges, and Future Perspectives

Jitesh Khetan

Modern School, Barakhamba Road

Abstract

The Internet of Things (IoT) has become one of the most influential forces reshaping residential life, enabling households to move from isolated, manually operated appliances toward interconnected domestic ecosystems capable of sensing, communicating, and acting with minimal human intervention. This review synthesises secondary literature published largely between 2020 and 2026 to examine how IoT technologies, including sensors, actuators, communication protocols, cloud computing, and edge computing, have transformed key areas of household life such as security, energy management, appliances, cleaning and maintenance, health and assisted living, and entertainment. The review identifies substantial opportunities created by domestic IoT adoption, including improved convenience, operational efficiency, energy conservation, enhanced safety, and greater accessibility for elderly and disabled users, alongside emerging business models built around subscription services and home automation consulting. At the same time, the literature reveals persistent challenges, including cybersecurity vulnerabilities, privacy erosion, interoperability fragmentation, economic barriers to adoption, and the growing environmental burden of electronic waste. A recurring tension in the literature concerns the coexistence of studies that emphasise convenience and efficiency gains alongside others that highlight consumer distrust and security anxiety; this review argues that these contradictions largely stem from differences in methodology, geographic context, demographic sampling, and the specific category of IoT device under investigation. The review concludes that the long-term success of domestic automation depends on balancing technological innovation with privacy protection, affordability, interoperability standards, and environmentally responsible design, and it proposes a human-centred, policy-supported pathway for future research and development.

Keywords: Internet of Things, domestic automation, smart home, cybersecurity, privacy, sustainability, consumer adoption

Chapter 1: Introduction

1.1 Background of the Study

The Internet of Things refers to a network of physical objects embedded with sensors, software, and connectivity that allows them to collect and exchange data with minimal human input (Nizetic et al., 2020, as cited in Broad Perspective of Smart Home Technology, 2024). Since its conceptual origins in the late twentieth century, IoT has expanded from a niche engineering idea into a foundational layer of everyday digital life, connecting everything from industrial machinery to household lightbulbs. The growth of

connected devices has been especially visible inside the home, where wireless connectivity, falling sensor costs, and the proliferation of smartphones have made it possible for ordinary consumers, not just technologists, to automate parts of their daily routines (A Comprehensive Review of IoT Networking Technologies, 2023).

Historically, household technology evolved slowly: mechanical timers and single-function electrical appliances dominated domestic life for most of the twentieth century. The transition toward interconnected domestic ecosystems accelerated only once wireless sensor networks, cloud computing, and mobile interfaces converged, allowing previously isolated appliances such as thermostats, cameras, and washing machines to communicate with each other and with centralised control systems (A Comprehensive Review of IoT Networking Technologies, 2023). This shift has been reinforced by consumer demand for convenience, safety, and efficiency, as well as by demographic pressures such as ageing populations that require new models of independent living support (Stage-Wise IoT Solutions for Alzheimer's Disease, 2025).

1.2 Understanding Domestic Automation

Domestic automation can be defined as the application of electronic, computational, and networked technologies to control household functions such as lighting, climate, security, and appliances, typically with the goal of reducing manual effort while increasing comfort, safety, or efficiency. Early domestic automation relied on programmable timers and standalone controllers that operated according to fixed schedules, with no capacity to adapt to real-time conditions or communicate with other devices.

The evolution from these programmable systems to connected ecosystems reflects the broader trajectory of IoT itself: devices are no longer isolated but exist within a networked environment where data from one sensor can inform the behaviour of another appliance. For instance, an occupancy sensor can trigger both lighting adjustments and climate control simultaneously, a level of coordination that was not possible under earlier automation paradigms. This relationship between IoT and domestic automation is therefore not incidental but structural: IoT provides the connective and computational infrastructure that makes contemporary domestic automation possible (A low-cost IoT-based smart home automation system for urban sustainability in Mogadishu, Somalia, 2025).

1.3 Rationale of the Study

The rationale for this review rests on three interlocking observations. First, households are becoming increasingly reliant on connected technologies for core functions including security, comfort, and health monitoring, which raises the practical stakes of understanding how these systems perform and fail. Second, the home automation market has grown into a substantial economic sector; global smart home market valuations for 2024 and 2025 range from roughly USD 101 billion to USD 184 billion depending on methodology and market scope, with most forecasts projecting compound annual growth rates between 11 percent and 27 percent through the early 2030s (Grand View Research, 2026; SkyQuest, 2026; Databridge Market Research, 2024). Third, while the technical capabilities of domestic IoT are well documented, there remains a need to weigh these opportunities against the technical, ethical, and societal challenges that accompany them, including data privacy, cybersecurity, and equitable access.

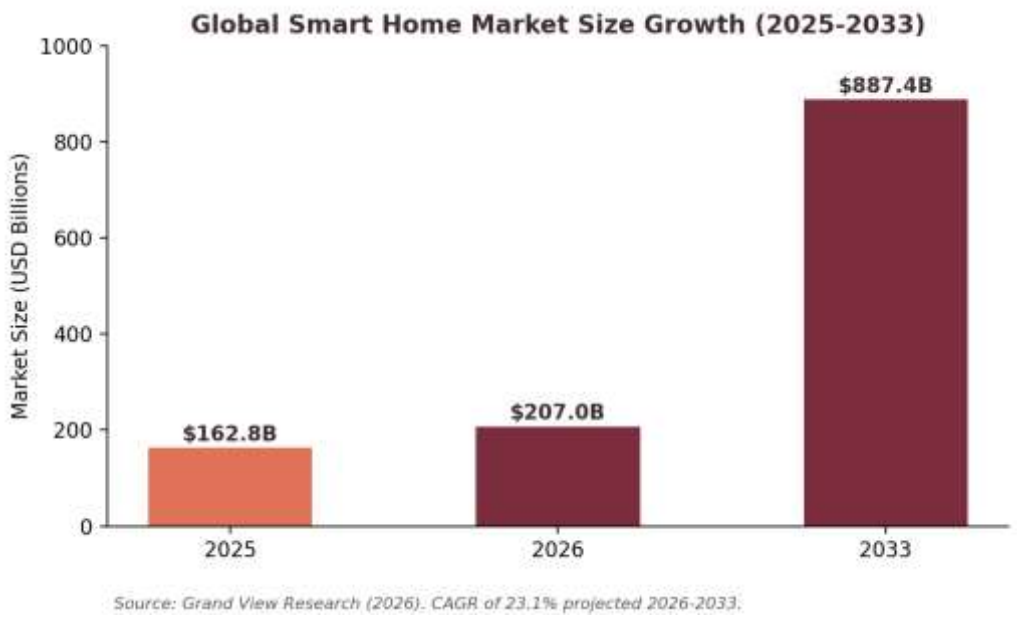

Figure 1.1. Global smart home market size growth, 2025-2033. Source: Grand View Research (2026).

1.4 Objectives of the Review

This review pursues five objectives: to trace the evolution of IoT within the context of domestic automation; to survey the principal household applications through which IoT is currently deployed; to appraise the benefits and constraints associated with IoT-based automation; to critically interrogate the challenges that continue to impede adoption; and to identify gaps and directions for future inquiry.

1.5 Research Questions

The review is guided by five research questions: How has IoT transformed domestic automation? What are the major applications of IoT in residential environments? What opportunities does IoT create for households and society? What challenges hinder widespread adoption? What future trends are likely to shape domestic automation?

1.6 Scope of the Review

This review is confined to residential applications of IoT and does not address industrial or commercial deployments except where they inform household-level insight. It relies exclusively on secondary research, drawing on peer-reviewed journal articles, conference proceedings, systematic reviews, and credible industry market research published predominantly between 2020 and 2026. The review addresses technological, consumer, operational, and societal dimensions in order to furnish a rounded account of domestic IoT rather than a narrowly engineering-focused one.

Chapter 2: Evolution and Foundations of IoT-Based Domestic Automation

2.1 Evolution of the Internet of Things

The historical development of IoT is closely tied to advances in networking and miniaturisation. Early machine-to-machine communication in the 1990s and 2000s laid the groundwork for what would later be branded the Internet of Things, but it was the falling cost of Micro Electro Mechanical Systems (MEMS) sensors and wireless communication chips that made mass deployment economically viable (A Comprehensive Review of IoT Networking Technologies, 2023). This period coincided with the broader

Industry 4.0 movement, in which manufacturing and infrastructure sectors began integrating networked sensing and automation, a trend that subsequently diffused into consumer markets and household products. By the early 2020s, IoT had become a mainstream feature of consumer technology rather than a specialist domain. Market analysts estimate that the number of connected devices in households worldwide surpassed 30 billion by late 2025, reflecting a dense and rapidly expanding ecosystem of domestic connectivity (Market Research Future, 2026).

2.2 Components of IoT Systems

IoT systems within the home are typically composed of six interacting layers. Sensors detect environmental conditions such as motion, temperature, humidity, or light. Actuators translate digital commands into physical actions, such as unlocking a door or adjusting a thermostat. Communication protocols, including Wi-Fi, Zigbee, Z-Wave, Bluetooth Low Energy, and the newer cross-manufacturer Matter standard, allow devices to exchange data reliably. Cloud computing provides centralised storage, processing, and remote accessibility, while edge computing increasingly complements the cloud by processing data locally on the device itself, reducing latency and limiting the amount of sensitive information transmitted externally. Finally, mobile interfaces, typically smartphone applications, give users a single point of control over an otherwise distributed set of devices (A Comprehensive Review of IoT Networking Technologies, 2023; A low-cost IoT-based smart home automation system for urban sustainability in Mogadishu, Somalia, 2025).

2.3 Evolution of Domestic Automation

Domestic automation has progressed through five broad stages. Manual household operations, in which all appliances required direct human control, gave way to electrical automation, where simple electromechanical devices such as timer-based irrigation or lighting systems reduced routine manual effort. Programmable automation followed, introducing digital logic that allowed users to schedule behaviours in advance. Connected automation then layered networking onto these programmable systems, enabling remote control and real-time monitoring via mobile applications. The current stage, integrated domestic ecosystems, is characterised by interoperability across manufacturers and device categories, centralised control hubs, and automation routines that respond dynamically to sensor data rather than fixed schedules (Broad Perspective of Smart Home Technology, 2024).

2.4 Theoretical Perspectives

Several theoretical frameworks help explain how and why consumers adopt domestic IoT technologies. The Technology Acceptance Model (TAM) proposes that perceived usefulness and perceived ease of use are the primary determinants of a user's intention to adopt a new technology; in the smart home context, research applying TAM has found that trust in the system and privacy concerns increasingly function as additional, and sometimes overriding, determinants of adoption decisions (Security and Privacy Concerns in the Adoption of IoT Smart Homes, 2024).

The Diffusion of Innovation Theory explains adoption as a social process unfolding across categories of users, from early adopters through to laggards, and helps account for why smart home adoption rates vary substantially across regions and income groups. The Unified Theory of Acceptance and Use of Technology (UTAUT) extends TAM by incorporating social influence and facilitating conditions, and has been adapted into security-specific variants to evaluate how perceived risk affects technology adoption at a household or municipal level (Security and Privacy Concerns in the Adoption of IoT Smart Homes, 2024). Finally, Socio-Technical Systems Theory frames the smart home not merely as a collection of devices but as an interaction between technical infrastructure and social practices, family routines, and

household power dynamics, a perspective that has proven useful for understanding conflicts over control and surveillance within multi-occupant homes (Security and Privacy Perspectives of People Living in Shared Home Environments, 2024).

Chapter 3: Applications of IoT in Domestic Automation

3.1 Household Security

Security remains the most heavily adopted category of domestic IoT. Smart locks allow keyless entry and remote access management, surveillance systems and video doorbells provide continuous monitoring accessible from mobile devices, and motion detection sensors trigger alerts or automated responses when unexpected activity is detected. Surveillance cameras in particular have benefited from the incorporation of artificial intelligence and machine learning, which enable more accurate detection of suspicious activity, facial recognition, and object identification, thereby improving the responsiveness of home security systems to genuine threats while reducing false alarms (Smart Homes: A Meta-Study on Sense of Security and Home Automation, 2025). Market data confirm this emphasis: the security and access control segment held the largest single product share of the global smart home market in 2025, at just over 31 percent (Grand View Research, 2026).

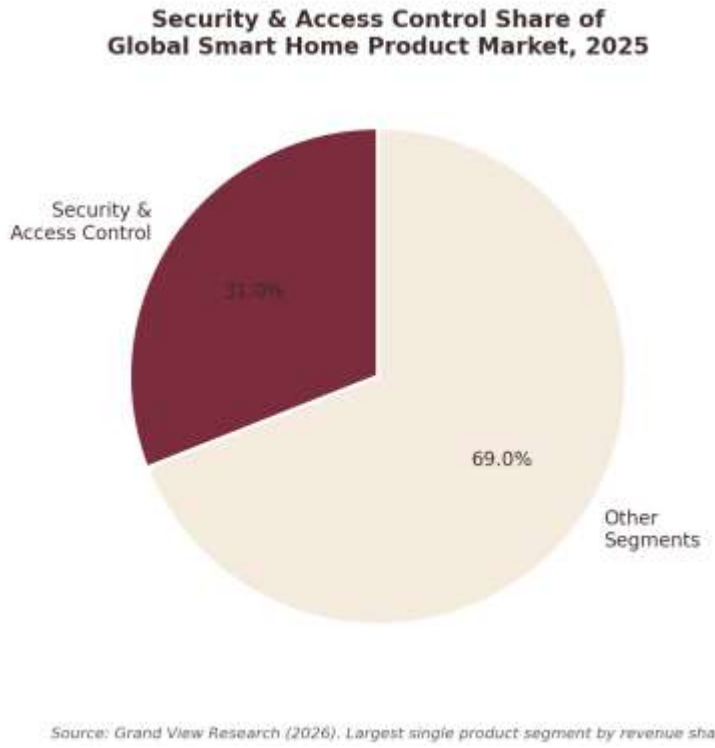

Figure 3.1. Security and access control as a share of the global smart home product market, 2025. Source: Grand View Research (2026).

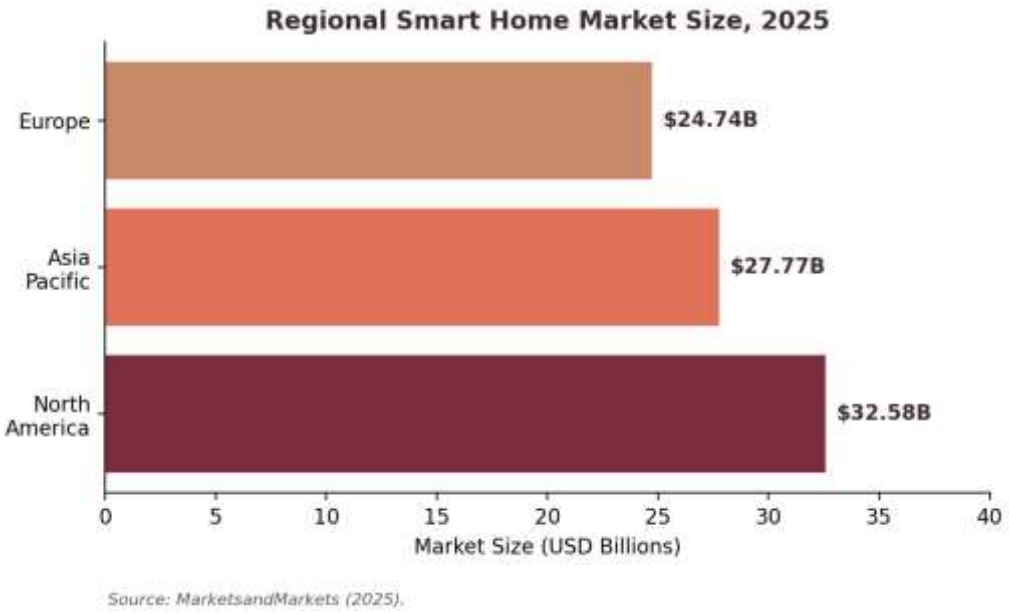

Figure 3.2. Regional smart home market size comparison, 2025. Source: MarketsandMarkets (2025).

3.2 Energy and Resource Management

Intelligent lighting systems adjust brightness and scheduling based on occupancy or ambient light, while smart thermostats learn household routines and adjust heating and cooling accordingly. Water monitoring systems detect leaks and unusual consumption patterns, and smart metering provides households with granular, real-time visibility into energy use that was previously available only in aggregate monthly form. Industry reporting indicates that energy and water control is among the fastest-growing device segments, driven by rising utility costs and household interest in demonstrable sustainability gains (Fortune Business Insights, 2025).

3.3 Household Appliances

Connected refrigeration systems can track inventory and expiration, laundry appliances can be monitored and controlled remotely, and kitchen appliances increasingly integrate voice control and recipe-linked automation. Climate control systems, closely related to energy management, now commonly incorporate zone-based automation that adjusts conditions differently across rooms based on occupancy and preference.

3.4 Cleaning and Maintenance

Robotic vacuum cleaners represent one of the most commercially successful domestic IoT categories, having moved from novelty status to mainstream adoption over the past decade; industry analysis notes that smart vacuum manufacturers have increasingly focused on improving object recognition through AI alongside core cleaning functions (IDC, 2024). Related but less widely adopted categories include window-cleaning robots, automated lawn maintenance systems, and pool-cleaning devices, which extend the logic of automated indoor cleaning to outdoor and peripheral domestic spaces.

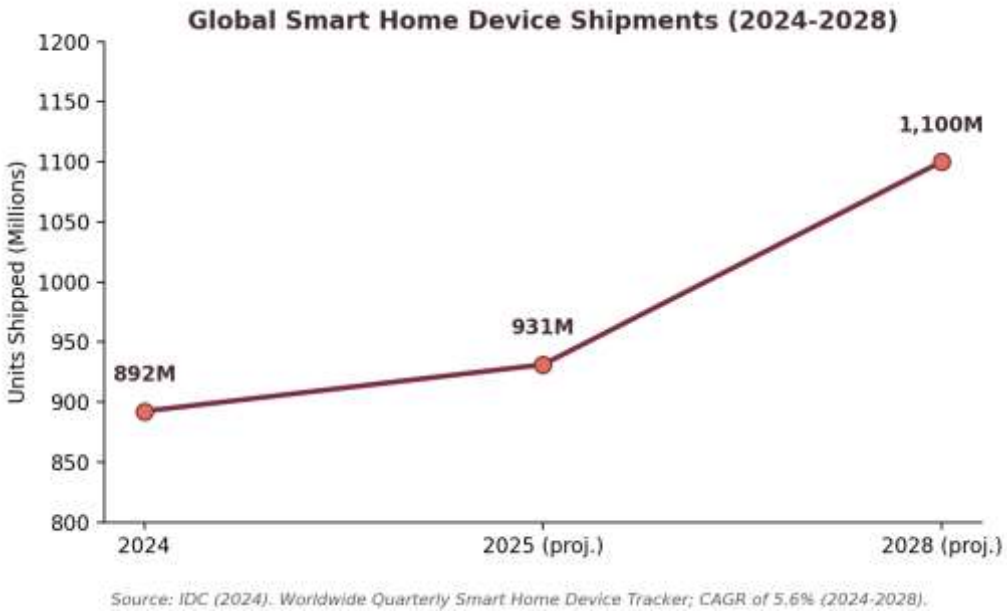

Figure 3.3. Global smart home device shipment growth, 2024-2028. Source: IDC (2024).

3.5 Health and Assisted Living

IoT-enabled health and assisted-living applications have grown particularly quickly in response to ageing populations. Systems for elderly monitoring track movement patterns and detect falls or prolonged inactivity, medication reminder devices support adherence to treatment schedules, indoor environmental monitoring tracks air quality and temperature relevant to respiratory or cardiovascular conditions, and emergency response systems can automatically alert caregivers or emergency services. A systematic review of IoT-enabled systems for Alzheimer's disease care, synthesising 236 studies published mostly between 2020 and 2025, found that wearable biosensors, cognitive monitoring tools, and smart home automation combined with AI-driven analytics are increasingly used for early diagnosis, continuous monitoring, and assistive care of patients with dementia (Stage-Wise IoT Solutions for Alzheimer's Disease, 2025). The home healthcare segment is projected to be the fastest-growing product category in the smart home market through the early 2030s, with compound annual growth exceeding 32 percent (Grand View Research, 2026).

3.6 Entertainment and Lifestyle

Voice-controlled systems, led by assistants such as Amazon Alexa and Google Home, have become central hubs for controlling other domestic devices as well as for media consumption. Multimedia integration allows entertainment systems, including smart televisions, to serve as control points for household automation, while connected entertainment devices increasingly incorporate generative AI features that personalise content recommendations and enable more natural voice interaction (Grand View Research, 2026).

3.7 Integrated Domestic Ecosystems

The most advanced form of domestic IoT deployment involves genuine device interoperability, in which products from different manufacturers communicate through shared standards. The Matter protocol, an IP-based open-source connectivity standard developed by the Connectivity Standards Alliance and championed by Apple, Google, and Amazon, exemplifies this industry effort to reduce fragmentation. The global market for Matter-compatible devices was valued at approximately USD 14.8 billion in 2025 and

is projected to reach USD 52.6 billion by 2034, a trajectory that reflects rapid manufacturer commitment across categories including lighting, energy management, and water sensing (Matter Smart Home Device Market Research Report, 2026). Empirical evaluation of the standard has found that it meaningfully enhances device interoperability and security, producing a more cohesive user experience, although integrating legacy, pre-Matter devices and achieving truly universal manufacturer adoption remain unresolved obstacles (Innovative IoT Solutions: A Comprehensive Study of the MATTER Standard, 2025). Automation routines, in which multiple devices respond together to a single trigger, such as a morning routine adjusting lighting, temperature, and music simultaneously, exemplify the cross-device communication that distinguishes integrated ecosystems from earlier generations of standalone smart devices (Grand View Research, 2026).

Chapter 4: Opportunities Created by IoT-Based Domestic Automation

4.1 Improved Convenience

The most consistently reported benefit of domestic IoT is convenience: the ability to control, monitor, and automate household functions remotely reduces the cognitive and physical burden of routine domestic management. Case study evidence from residential smart home deployments has demonstrated improved comfort alongside measurable energy savings when lighting, heating, and ventilation systems are automated (Song et al., 2021, as cited in Smart Homes of the Future, 2023).

4.2 Operational Efficiency

Beyond individual convenience, IoT systems improve the operational efficiency of the household as a unit by coordinating multiple devices and reducing redundant or wasteful behaviour, such as heating unoccupied rooms or leaving lights on in empty spaces.

4.3 Energy Conservation

Smart thermostats, lighting, and metering systems allow households to reduce energy consumption through automated, data-driven adjustments rather than manual vigilance. This capability has become increasingly significant given rising energy costs and household sustainability goals, and it is a primary driver of consumer investment in smart HVAC and lighting products (MarketsandMarkets, 2025).

4.4 Enhanced Safety and Security

AI-enhanced surveillance, automated locks, and real-time alerts collectively improve household safety by enabling faster detection and response to intrusions, fires, or medical emergencies compared to traditional, non-connected systems (Smart Homes: A Meta-Study on Sense of Security and Home Automation, 2025).

4.5 Improved Accessibility

Elderly users

For elderly users, IoT-enabled monitoring and assistive technologies support independent living by reducing reliance on continuous in-person supervision while still enabling rapid intervention when needed (Stage-Wise IoT Solutions for Alzheimer's Disease, 2025).

Persons with disabilities

For persons with disabilities, voice control and automated environmental adjustment reduce physical barriers to interacting with the home environment, extending functional independence in ways that were not previously possible with manually operated systems.

4.6 Sustainability Benefits

Efficient resource utilisation, reduced energy consumption, and water conservation are frequently cited sustainability benefits of domestic IoT, achieved through automated monitoring and adjustment rather

than reliance on manual conservation habits. However, as discussed in Chapter 5, these benefits must be weighed against the environmental costs of manufacturing and disposing of the devices themselves.

4.7 Emerging Business Opportunities

The growth of domestic IoT has created new commercial categories beyond device manufacturing itself, including subscription-based services for monitoring and cloud storage, maintenance and repair services, digital platforms that aggregate device data, and home automation consulting services that help households design and integrate multi-vendor systems. Corporate activity in this space has accelerated: recent product launches include Amazon's Alexa+ AI assistant, Schneider Electric's AI-powered energy management feature, and LG's ThinQ AI Home Hub, each reflecting the commercial convergence of generative AI with domestic automation (Grand View Research, 2026).

Chapter 5: Challenges and Critical Evaluation

5.1 Cybersecurity Risks

Domestic IoT devices are frequently vulnerable to compromise due to weak default credentials, infrequent firmware updates, and inconsistent security engineering across manufacturers. A large-scale empirical study of 93 IoT devices and their companion mobile applications found extensive previously undisclosed local network security and privacy issues, demonstrating that vulnerabilities exist not only in cloud-connected functions but in local device-to-device communication as well (Girish et al., 2023). In response, government bodies including the United States National Institute of Standards and Technology (NIST) have developed baseline cybersecurity requirements for consumer IoT products, culminating in the voluntary U.S. Cyber Trust Mark labelling programme announced in 2023 (NIST, 2025).

5.2 Privacy Concerns

The continuous data collection inherent to IoT devices, ranging from occupancy patterns to voice recordings, raises significant privacy concerns. Research on shared home environments has shown that privacy and control mechanisms are often poorly understood by users, with awareness and consent frequently limited to the primary account holder rather than all household occupants (Tabassum & Lipford, 2023, as cited in Security and Privacy Perspectives of People Living in Shared Home Environments, 2024). Surveillance-adjacent functions, such as cameras and voice assistants, are particularly implicated in these concerns because they capture data about individuals who may not have consented to monitoring, including guests, children, or domestic workers.

5.3 Interoperability Issues

Compatibility among manufacturers remains a persistent impediment to fully integrated domestic ecosystems. Despite the emergence of unifying standards such as Matter, many households continue to operate fragmented collections of devices that require separate applications and cannot communicate directly with one another. Industry commentary tracking the rollout of Matter through 2024 and 2025 notes that inconsistent specification turnaround times and incomplete manufacturer buy-in have slowed the standard's ability to fully supersede proprietary ecosystems, prompting some vendors, such as Nanoleaf, to develop parallel proprietary protocols even while nominally supporting Matter (Matter Alpha, 2025). Standardisation efforts continue but have not yet fully resolved the practical friction this fragmentation creates for average consumers (Ozadowicz, 2024, as cited in A low-cost IoT-based smart home automation system for urban sustainability in Mogadishu, Somalia, 2025).

5.4 Economic Barriers

Initial investment costs remain a meaningful barrier to adoption, particularly in lower-income households

and developing economies. Estimates place the cost of installing a full-featured smart home system with AI capabilities in the United States between USD 2,000 and USD 10,000 depending on device count and system complexity (Statista, 2024, as cited in Smart Home Market Size Report, 2024). Beyond upfront costs, ongoing subscription fees for cloud storage and monitoring, along with maintenance and eventual replacement costs, compound the affordability challenge over a device's lifecycle.

5.5 Consumer Adoption Challenges

Digital literacy and technology anxiety continue to constrain adoption among older and less technically confident users. A qualitative study of UK families' engagement with smart home cybersecurity found that most participants simply assumed adequate protection was already built into their devices, rather than actively verifying or configuring security settings themselves (Turner et al., 2022). A related empirical study similarly reported that fewer than half of surveyed participants were conversant with the procedures needed to secure their own IoT devices, underscoring a persistent gap between perceived and actual security competence among household users (Examining the Security Essences of Internet of Things, 2024). This discrepancy between assumed and actual security understanding illustrates a broader trust and ease-of-use problem that extends beyond any single technical vulnerability.

The digital divide compounds these adoption challenges. Survey research on U.S. technology ownership indicates that roughly a quarter of adults in households earning under USD 30,000 annually do not own a smartphone, and a comparable proportion lack home broadband, both of which are prerequisite infrastructure for most contemporary domestic IoT products (Pew Research Center, 2021). Field-trial evidence further suggests that smart home adoption itself risks widening this divide, since early adopters tend to share socio-demographic characteristics with adopters of earlier information and communication technologies, meaning the same households that lag in general digital access are also likely to lag in smart home adoption (Chicago Policy Review, 2023).

5.6 Environmental Concerns

The rapid proliferation of IoT devices carries a growing environmental cost. Estimates suggest the number of active IoT connected devices could reach 30 to 50 billion by 2030, and industry analysts note that a meaningful proportion of these devices are discarded annually as they become obsolete or malfunction (Securis, 2024). Because IoT devices often have shorter functional lifespans than traditional appliances, driven by rapid technological turnover and software compatibility issues, they contribute disproportionately to global electronic waste streams, which already exceeded 62 million tonnes annually as of the mid-2020s (Expert Assessment: The Systemic Environmental Risks of Artificial Intelligence, 2025). Many IoT devices also contain hazardous materials, including heavy metals and brominated flame retardants, that pose environmental and public health risks when disposed of improperly rather than recycled (Securis, 2024; Quantum Lifecycle, 2025).

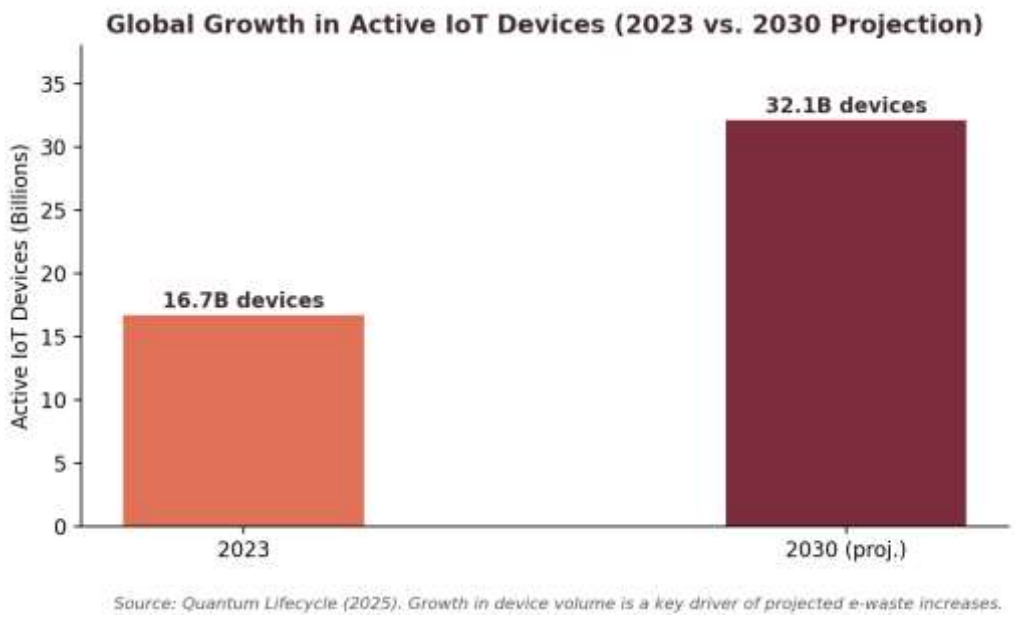

Figure 5.1. Growth in active global IoT devices, 2023 vs. 2030 projection, a key driver of rising e-waste volumes. Source: Quantum Lifecycle (2025).

5.7 Ethical Considerations

Ethical questions surrounding domestic IoT centre on data ownership, that is, who ultimately retains authority over the data generated by household devices, the manufacturer, the platform, or the resident, as well as on responsible innovation practices that anticipate rather than merely react to misuse. Digital inclusion is a closely related ethical concern, since the concentration of IoT benefits among higher-income, urban, and digitally literate households risks compounding existing inequalities in domestic safety, efficiency, and independence. This concern is not speculative: national survey data show that lower-income households already lag substantially in ownership of the broadband and smartphone infrastructure that domestic IoT products typically require, meaning the digital divide observed in general internet access is likely to be reproduced, and potentially amplified, in the distribution of smart home benefits (Pew Research Center, 2021).

Chapter 6: Critical Review of Existing Literature

6.1 Areas of Scholarly Consensus

Across the literature reviewed, several conclusions recur with relative consistency. Researchers broadly agree that IoT-based domestic automation improves convenience and reduces the manual burden of household management (Smart Homes of the Future, 2023). There is similarly strong agreement regarding operational efficiency gains, particularly in energy and resource management applications. Market and adoption data further confirm sustained growth potential and increasing consumer acceptance, evidenced by the consistent upward trajectory of smart home market valuations across independent research firms, despite some variation in the precise figures reported (Grand View Research, 2026; Fortune Business Insights, 2025; SkyQuest, 2026).

6.2 Contradictory Findings

Despite this consensus on core benefits, the literature contains genuine contradictions on several dimensions. The most prominent is the tension between privacy and convenience: studies focused on user

experience and efficiency tend to report high satisfaction and adoption intent, while studies focused specifically on security and privacy report substantial consumer anxiety and, in some cases, avoidance of certain device categories altogether (Security and Privacy Concerns in the Adoption of IoT Smart Homes, 2024). A related contradiction concerns automation versus consumer control, where some research frames automation as empowering because it removes routine burdens, while other research, particularly from a socio-technical systems perspective, frames the same automation as a loss of granular control, especially for secondary household members who did not configure the system (Security and Privacy Perspectives of People Living in Shared Home Environments, 2024).

A further contradiction concerns cost versus long-term savings. Industry-oriented literature emphasises the long-term financial benefits of energy-efficient automation, while consumer-adoption literature emphasises the high upfront cost as a primary barrier, particularly in emerging economies (Smart Home Market Size Report, 2024). Finally, an innovation versus sustainability contradiction runs through the literature: technological innovation is generally treated as unambiguously positive in market-oriented sources, whereas environmental and e-waste literature raises significant concern about the sustainability implications of a device ecosystem built on rapid replacement cycles (Quantum Lifecycle, 2025; Expert Assessment: The Systemic Environmental Risks of Artificial Intelligence, 2025).

6.3 Limitations of Existing Research

Several limitations recur across the reviewed literature. Much of the existing research places heavy emphasis on technical development, device performance, and system architecture, with comparatively limited attention to long-term consumer behaviour once initial adoption has occurred. Longitudinal consumer studies remain scarce, meaning most conclusions about satisfaction, trust, and habituation are drawn from single-point-in-time surveys rather than sustained observation. Developing countries are also underrepresented in the literature relative to their share of projected future IoT growth, with the bulk of empirical studies originating from North America, Europe, and parts of East Asia. Interdisciplinary research that meaningfully integrates technological, business, and behavioural science perspectives remains limited, and few studies assess the long-term societal implications of widespread domestic automation beyond the household unit itself.

6.4 Research Gaps

Building on these limitations, several research gaps warrant attention. Consumer behaviour within multi-device ecosystems, as opposed to single-device studies, remains underexplored, despite the fact that most real households now operate several interacting IoT products simultaneously. Accessibility in low-income households is another significant gap, given that most adoption research implicitly assumes a baseline level of disposable income and digital infrastructure. Sustainable lifecycle management of IoT devices, including repairability, recyclability, and extended producer responsibility, requires further empirical study, as does the development of business models that could support more affordable adoption without compromising security. Finally, policy and regulatory frameworks specific to connected domestic technologies remain underdeveloped in much of the world, even as national initiatives such as the U.S. Cyber Trust Mark begin to establish precedents (NIST, 2025).

Chapter 7: Future Perspectives

7.1 Evolution of Connected Domestic Ecosystems

Future domestic ecosystems are likely to move further toward seamless, cross-manufacturer interoperability as standards such as Matter mature and gain broader industry adoption. The integration of

generative AI into domestic hubs, exemplified by products such as Amazon's Alexa+ and Google's expanding Home APIs platform, suggests that future systems will increasingly function as autonomous agents capable of multi-step task execution rather than simple command-response devices (Grand View Research, 2026; SkyQuest, 2026).

7.2 Sustainable Domestic Automation

Given the environmental concerns documented in Chapter 5, future domestic automation will likely need to prioritise modular, repairable device design, extended producer responsibility schemes, and consumer education on responsible disposal, in order to prevent the projected growth in connected devices from translating directly into proportional growth in electronic waste (Quantum Lifecycle, 2025).

7.3 Human-Centred Design

Future systems will need to move beyond purely technical optimisation toward human-centred design that accounts for the needs of all household members, not only the primary account holder who configures the system. This includes more transparent consent mechanisms for shared and multi-occupant homes, and interfaces that make data collection and automated decision-making visible and understandable to non-technical users (Security and Privacy Perspectives of People Living in Shared Home Environments, 2024).

7.4 Standardisation and Interoperability

Continued progress on unifying communication standards is likely to reduce the fragmentation that currently limits integrated domestic ecosystems, lowering both the technical and cognitive barriers to adoption for average consumers.

7.5 Role of Public Policy and Regulation

Public policy is expected to play an increasingly active role in shaping domestic IoT, particularly around minimum cybersecurity standards, data protection, and labelling schemes that allow consumers to compare the security posture of different products before purchase, following the precedent set by frameworks such as NIST's IoT Core Baseline and the associated U.S. Cyber Trust Mark (NIST, 2025).

7.6 Future Research Directions

Future research should prioritise longitudinal, cross-cultural studies of household adoption and trust; empirical evaluation of sustainable device lifecycle models; investigation of accessibility and affordability in low- and middle-income households; and interdisciplinary work that connects engineering, behavioural science, and policy analysis to produce a more complete account of how domestic automation is actually lived and experienced, rather than only how it is designed and marketed.

Chapter 8: Conclusion

8.1 Summary of Major Findings

This review has shown that IoT has fundamentally transformed domestic automation, moving households from isolated, manually operated appliances toward interconnected ecosystems capable of coordinated, data-driven behaviour. Applications of this technology now extend well beyond simple convenience into efficiency, sustainability, accessibility, and safety, spanning security, energy management, appliances, cleaning, health monitoring, and entertainment. Adoption continues to grow briskly, reflected in consistent upward market projections across independent research organisations, despite the persistence of well-documented technical and societal challenges.

8.2 Critical Conclusions

Domestic automation, as it has evolved through IoT, constitutes a genuine transition toward interconnected living rather than a mere accumulation of isolated technological solutions. However, this review's

synthesis of the literature indicates that the long-term viability and social value of domestic automation hinge on the extent to which innovation is reconciled with privacy protection, affordability, cybersecurity, interoperability, and environmental sustainability. Where these factors are neglected, as current evidence on e-waste and consumer distrust suggests they too often are, the advantages of domestic IoT risk being eroded by the very technologies meant to deliver them.

8.3 Final Remarks

As IoT continues to embed itself more deeply into residential life, the central challenge facing manufacturers, policymakers, and researchers is not whether domestic automation will continue to grow, since market and adoption data make that trajectory clear, but whether it can grow in a manner that is secure, equitable, and environmentally sustainable. Addressing the research gaps identified in this review, particularly around long-term consumer behaviour, affordability, and sustainable device lifecycle management, will be essential to ensuring that the next generation of domestic automation delivers on its considerable promise.

References

1. A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications. (2023). Journal of Sensor and Actuator Networks, 12(2), 30. https://doi.org/10.3390/jsan12020030
2. A low-cost IoT-based smart home automation system for urban sustainability in Mogadishu, Somalia. (2025). Discover Internet of Things. https://doi.org/10.1007/s43926-025-00207-4
3. Broad Perspective of Smart Home Technology in 2024. (2024). ResearchGate.
4. Chicago Policy Review. (2023). How can policymakers increase the adoption of smart home technologies? https://chicagopolicyreview.org/2019/05/15/how-can-policymakers-increase-the-adoption-of-smart-home-technologies/
5. Databridge Market Research. (2024). Global smart home market report. https://www.databridgemarketresearch.com/reports/global-smart-home-market
6. Examining the security essences of Internet of Things (IoT) for adoption and use. (2024). Issues in Information Systems, 25(1), 279-292. https://iacis.org/iis/2024/1_iis_2024_279-292.pdf
7. Expert assessment: The systemic environmental risks of artificial intelligence. (2025). arXiv. https://arxiv.org/pdf/2512.11863
8. Fortune Business Insights. (2025). Smart home market size, share and forecast report, 2032. https://www.fortunebusinessinsights.com/industry-reports/smart-home-market-101900
9. Girish, A., Hu, T., Prakash, V., Dubois, D. J., Matic, S., Huang, D. Y., Egelman, S., Reardon, J., Tapiador, J., Choffnes, D., & Vallina-Rodriguez, N. (2023). In the room where it happens: Characterizing local communication and threats in smart homes. Proceedings of the 2023 ACM on Internet Measurement Conference, 437-456. https://doi.org/10.1145/3618257.3624845
10. Grand View Research. (2026). Smart home market size, share and growth report, 2026-2033. https://www.grandviewresearch.com/industry-analysis/smart-homes-industry
11. IDC. (2024). Smart home market on track for rebound thanks to emerging regions. https://my.idc.com/getdoc.jsp?containerId=prUS52632124
12. Innovative IoT solutions: A comprehensive study of the MATTER standard in smart home integration. (2025). IEEE Xplore. https://ieeexplore.ieee.org/document/11119901/

13. Market Research Future. (2026). Smart home market size, trends, industry report - 2035. https://www.marketresearchfuture.com/reports/smart-home-market-974
14. MarketsandMarkets. (2025). Smart home market size report, 2026-2032. https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html
15. Matter Alpha. (2025). 2024: The year smart home interoperability began to matter. https://www.matteralpha.com/explainer/2024-the-year-smart-home-interoperability-began-to-matter
16. Matter smart home device market research report 2034. (2026). MarketIntelo. https://marketintelo.com/report/matter-smart-home-device-market
17. National Institute of Standards and Technology. (2025). Consumer IoT cybersecurity. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity
18. Pew Research Center. (2021). Digital divide persists even as Americans with lower incomes make gains in tech adoption. https://www.pewresearch.org/short-reads/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/
19. Quantum Lifecycle. (2025). The impact of IoT devices on e-waste volumes. https://quantumlifecycle.com/en_CA/blog/the-impact-of-iot-devices-on-e-waste-volumes/
20. Securis. (2024). IoT devices will lead to more e-waste in the future. https://securis.com/blog/iot-devices-will-lead-to-more-future-e-waste/
21. Security and privacy concerns in the adoption of IoT smart homes: A user-centric analysis. (2024). ResearchGate.
22. Security and privacy perspectives of people living in shared home environments. (2024). arXiv. https://arxiv.org/pdf/2409.09363
23. SkyQuest. (2026). Smart home market size, share, forecast and trends [2033]. https://www.skyquestt.com/report/smart-home-market
24. Smart home market size report, 2026-2032. (2024). https://www.databridgemarketresearch.com/reports/global-smart-home-market
25. Smart homes of the future: A comprehensive review of IoT-based home automation. (2023). International Journal of Novel Research and Development, 8(5). https://www.researchgate.net/publication/371666903
26. Smart homes: A meta-study on sense of security and home automation. (2025). Sensors, 13(8), 320. https://doi.org/10.3390/wevj13080320
27. Stage-wise IoT solutions for Alzheimer's disease: A systematic review of detection, monitoring, and assistive technologies. (2025). PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12431156/
28. Turner, S., Pattnaik, N., Nurse, J. R. C., & Li, S. (2022). "You just assume it is in there, I guess": Understanding UK families' application and knowledge of smart home cyber security. Proceedings of the ACM on Human-Computer Interaction, 6(CSCW2), Article 269. https://doi.org/10.1145/3555159