Open Access Research Journal of
Multidisciplinary Studies
Journals home page: https://oarjpublication/journals/oarjms/
ISSN: 2783-0268 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

Internet of Things (IoT) in U.S. Smart Homes: A Review: Assessing the advancements in home automation, security implications, and user adaptability

Afees Olanrewaju Akinade [1, *], Peter Adeyemo Adepoju [2], Adebimpe Bolatito Ige [3] and Adeoye Idowu Afolabi [4]

[1] *MTN Communications Plc, Nigeria.*
[2] *Independent Researcher, United Kingdom.*
[3] *Independent Researcher, Canada.*
[4] *Independent Researcher, Nigeria.*

Open Access Research Journal of Multidisciplinary Studies, 2023, 05(02), 172-190

Publication history: Received on 10 February 2023; revised on 25 June 2023; accepted on 28 June 2023

Article DOI: https://doi.org/10.53022/oarjms.2023.5.2.0020

Abstract

This study presents a comprehensive review of the advancements, implications, and user adaptability of Internet of Things (IoT) technologies in U.S. smart homes. The main objectives were to assess the evolution of smart homes, analyze IoT integration, evaluate security implications, explore user adoption and behavior, and forecast future trends. Employing a systematic literature review and content analysis, the study scrutinized peer-reviewed articles, conference papers, and industry reports from 2010 to 2023. The methodology involved a meticulous selection process based on relevance, quality, and timeliness, focusing on publications that directly addressed IoT in smart homes. Key findings indicate significant advancements in home automation, driven by IoT integration. This evolution has enhanced home management, energy efficiency, and user experience. However, security emerged as a paramount concern, with privacy and data protection being central to user adoption. The review also revealed that user adoption is influenced by perceived usefulness, ease of use, and security concerns. Interoperability and standardization were identified as crucial for the seamless functionality of IoT systems. The study concludes that the future landscape of IoT in U.S. smart homes is promising, with potential growth in integration with smart city infrastructure and advancements in AI and machine learning. Recommendations for homeowners and industry leaders emphasize staying informed about IoT developments, prioritizing security, and focusing on user-friendly, interoperable solutions. The study suggests future research directions, including exploring the social, ethical, and legal implications of IoT in residential settings and its integration with sustainable practices.

Keywords: Internet of Things; Smart Homes; User Adoption; Automation; Security; Adaptability

1. Introduction

1.1. The Evolution of Smart Homes.

The evolution of smart homes, particularly in the United States, has been a transformative journey, marked by rapid technological advancements and a growing integration of the Internet of Things (IoT). This evolution reflects a paradigm shift in how we perceive and interact with our living spaces, transitioning from basic automation to sophisticated, interconnected systems that enhance comfort, efficiency, and security.

In the early stages, home automation was a nascent concept, primarily focused on basic tasks like controlling lighting and heating. However, with the advent of IoT, this concept has evolved dramatically. Mahamud et al. (2019) illustrate this transition through their development of an IoT-based smart home automation system, "Domicile." This system, controlled via a web portal and powered by an ESP32 Wi-Fi module, epitomizes the shift towards more integrated, user-friendly, and remotely accessible home environments. The emphasis on low-cost solutions in their work also highlights

* Corresponding author: Afees Olanrewaju Akinade.

a crucial aspect of smart home evolution: making advanced technology accessible to a broader audience (Mahamud et al., 2019).

The integration of voice-control systems in smart homes marks another significant milestone in this evolution. Venkatraman, Overmars, and Thong (2021) discuss the implementation of secure and integrated voice-controlled systems, underscoring the move towards more intuitive and seamless interaction between users and their home environments. Their research points to the growing importance of user experience in smart home design, where ease of use and security are paramount. The adoption of cloud-based solutions for voice control further demonstrates the increasing reliance on sophisticated technologies to enhance the functionality and convenience of smart homes (Venkatraman, Overmars, and Thong, 2021).

Security, a critical aspect of smart home evolution, has gained significant attention in recent years. Anupriya and Muthumanikandan (2023) delve into the effectiveness of IoT-based home security systems, addressing the challenges of ensuring privacy and data protection in increasingly connected homes. Their survey underscores the need for robust security measures as an integral part of smart home development, reflecting the growing awareness and demand for secure IoT implementations in residential settings (Anupriya & Muthumanikandan, 2023).

The evolution of smart homes in the U.S. is a testament to the dynamic nature of technology and its impact on everyday life. From basic automation to the current state of interconnected, intelligent systems, this journey reflects a broader trend towards a more connected and technologically advanced society. The integration of IoT has not only enhanced the functionality and efficiency of home environments but also raised important considerations regarding security, privacy, and user experience. As this evolution continues, it is likely that smart homes will become even more integrated, intuitive, and indispensable in our daily lives.

1.2. Defining the Scope: IoT Integration, Security, and User Experience.

The integration of the Internet of Things (IoT) in smart homes has revolutionized the concept of home automation, intertwining it with aspects of security and user experience (UX). This integration has not only enhanced the functionality of home devices but also raised significant concerns regarding security and privacy, necessitating a user-centric approach to design and implementation.

Chalhoub et al. (2020) conducted a case study focusing on how user experience is factored into the security and privacy design of smart home devices. Their research, involving in-depth interviews with employees of a large smart home company, revealed a notable gap in considering UX in the security design of these devices. This finding is critical as it highlights the often-overlooked aspect of user interaction in the context of security and privacy. The study proposed user-centered design guidelines and recommendations to improve data protection in smart homes, emphasizing the need for a balance between functionality and user security (Chalhoub et al., 2020).

The complexity of managing privacy and security settings in IoT ecosystems is another challenge that has emerged with the proliferation of smart devices. Abbott et al. (2023) explored this by implementing an IoT ecosystem in participants' homes, focusing on user perceptions and interactions with multiple smart devices. Their study included an Android dashboard for device control and data transparency, revealing insights into user preferences for notification and control mechanisms. The research underscores the importance of designing privacy and security dashboards that are intuitive and cater to the diverse needs of users, including children and pets. This approach is crucial for enhancing user trust and engagement with IoT devices in smart homes (Abbott et al., 2023).

Security and privacy issues in IoT-based smart applications have been a persistent concern, as highlighted by Sripriyanka and Mahendran (2022). Their survey on IoT security and privacy challenges in smart applications, including smart homes, sheds light on the vulnerabilities associated with data leakage and service loss. The study emphasizes the need for robust security mechanisms, such as bio-inspired optimization trained models, to protect confidential data from attacks. This focus on advanced security solutions is indicative of the evolving nature of threats in the IoT landscape and the need for continuous innovation in security technologies (Sripriyanka & Mahendran, 2022).

The integration of IoT in smart homes has brought about a paradigm shift in how we interact with our living spaces. This shift necessitates a comprehensive approach that considers not only the technological aspects but also the security, privacy, and user experience. The studies by the authors collectively highlight the importance of user-centered design, intuitive control mechanisms, and robust security solutions in the realm of smart home IoT. As this field continues to evolve, these considerations will play a pivotal role in shaping the future of home automation, ensuring that it is secure, user-friendly, and adaptable to the changing needs of consumers.

1.3. Historical Context: From Basic Automation to IoT Revolution.

The historical evolution of home automation, culminating in the Internet of Things (IoT) revolution, represents a significant shift in technological advancement and user interaction with technology. This journey from basic automation to the sophisticated IoT ecosystem reflects a series of technological innovations and societal changes, particularly in the United States.

In the early stages, home automation was primarily focused on basic tasks like controlling lights and heating systems. This form of automation was often limited in scope and functionality, lacking the interconnectedness that characterizes modern smart homes. Dong, Wan, and Yue (2017) discuss the evolution of IoT as a response to the limitations of these early systems. They highlight the development of adaptive service-oriented paradigms in IoT, which addressed the challenges of scalability and heterogeneity in continuously changing environments. This shift towards a more adaptive and integrated approach marked a significant milestone in the evolution of home automation (Dong et al., 2017).

The concept of sustainable cybernetic manufacturing, as explored by Wang et al. (2019), further illustrates the broader impact of IoT on various sectors, including home automation. Their research delves into the integration of advanced computing power with manufacturing equipment, a principle that is also applicable to the development of smart home technologies. The advancements in IoT have enabled more efficient and intelligent home automation systems, leading to the concept of cyber-physical systems that seamlessly integrate physical and digital worlds (Wang et al., 2019).

Charmanas et al. (2023) provide insights into the technological advancements in home automation through patent analysis. Their study unveils the technology clusters and prominent investors in home automation networking, highlighting the significant investments and innovations that have driven the evolution of this field. This analysis underscores the importance of intellectual property in the competitive landscape of home automation, reflecting the rapid growth and diversification of technologies in this domain (Charmanas et al., 2023).

The historical context of home automation, leading to the IoT revolution, is characterized by a transition from basic, standalone systems to interconnected, intelligent networks that enhance user experience and efficiency. The evolution of IoT, as discussed by Dong et al. (2017), the concept of sustainable cybernetic manufacturing by Wang et al. (2019), and the patent analysis by Charmanas et al. (2023), collectively paint a picture of a dynamic and rapidly evolving field. This evolution not only reflects technological advancements but also a changing societal relationship with technology, where convenience, efficiency, and sustainability have become key drivers in the development of smart home systems.

1.4. Aim and Objectives of the Study.

The aim of this study is to comprehensively assess the advancements, implications, and user adaptability of Internet of Things (IoT) technologies in U.S. smart homes. This includes an in-depth analysis of how IoT integration is reshaping home automation, the associated security challenges, and the evolving behavior and preferences of users.

The research objectives are;

- To assess the advancements in home automation, security implications, and user adaptability.
- To investigate the factors influencing user adoption and behavior in IoT-based smart homes.
- To explore the future landscape of IoT in smart homes.

2. Methodology

The methodology for this study involves a systematic literature review and content analysis to assess the advancements, implications, and user adaptability of IoT technologies in U.S. smart homes.

2.1. Data Sources

The primary data sources for this study include peer-reviewed academic journals, conference proceedings, and industry reports. These sources were accessed through various academic databases such as IEEE Xplore, ScienceDirect, JSTOR, and Google Scholar. Additionally, government and industry publications were reviewed to provide a comprehensive understanding of the current state and future trends of IoT in smart homes.

2.2. Search Strategy

The search strategy involved using specific keywords and phrases related to IoT and smart homes, such as "Internet of Things," "smart homes," "home automation," "IoT security," and "user adoption in smart homes." Boolean operators (AND, OR) were used to combine these terms effectively. The search was limited to documents published between 2010 and 2023 to ensure the relevance and timeliness of the information.

2.3. Inclusion and Exclusion Criteria for Relevant Literature

The inclusion and exclusion criteria for relevant literature in this study were meticulously defined to ensure a focused and comprehensive review. For inclusion, the study primarily considered peer-reviewed articles and conference papers that explicitly discussed IoT applications in smart homes. This encompassed studies that delved into technological advancements, security implications, and user adaptability within the realm of smart home IoT. The temporal scope of the literature was confined to publications from 2010 to 2023, aligning with the rapidly evolving nature of IoT technologies. Additionally, only articles published in English and available in full-text format were included to facilitate a thorough analysis.

Conversely, the exclusion criteria were set to omit non-peer-reviewed articles and grey literature to maintain the academic rigor of the study. Articles that did not directly focus on IoT in smart homes, such as those discussing IoT in industrial or other unrelated contexts, were excluded. Outdated articles published before 2010 were also excluded, considering the pace at which IoT technology advances. Furthermore, articles not available in full-text format were excluded, as these would not provide the comprehensive detail required for an in-depth analysis. This systematic approach to selecting relevant literature ensured that the study was grounded in current, high-quality, and directly pertinent sources, thereby enhancing the reliability and validity of the research findings.

The selection criteria were based on the relevance of the articles to the research aim and objectives. Articles were initially screened based on their titles and abstracts. The full texts of potentially relevant articles were then reviewed to determine their suitability. The quality of the research methodology, the credibility of the data sources, and the significance of the findings were key considerations in the selection process.

2.4. Data Analysis

Data analysis involved a content analysis approach, where the selected articles were systematically examined to extract pertinent information related to the study's aim and objectives. Key themes were identified, and data were categorized accordingly. This process involved identifying patterns, trends, and gaps in the literature. The analysis aimed to synthesize the findings to provide a comprehensive understanding of the current state of IoT in smart homes, including technological advancements, security challenges, user adoption, and future directions. The findings were then used to formulate recommendations for stakeholders in the field of smart home IoT.

3. IoT in U.S. Smart Homes: A Comprehensive Overview

3.1. Fundamental Concepts of IoT Integration in Smart Homes

The integration of the Internet of Things (IoT) in smart homes represents a significant advancement in how we interact with our living environments. This integration is not just a technological upgrade but a paradigm shift in the architectural and interior design of homes, privacy considerations, and the broader concept of urban living. Karagianni and Geropanta (2019) explore the methodology of integrating IoT into the architectural and interior design process, using a case study in Athens. Their research emphasizes the need for "enhanced architectural design" driven by smart home technologies. This approach goes beyond mere technological installation, advocating for a design process that is contextually relevant and user-centric. The study highlights the importance of aligning smart home functionalities with user needs, suggesting a holistic approach to smart home design that considers spatial awareness and collective IoT selection (Karagianni & Geropanta, 2019).

The privacy implications of IoT integration in smart homes are a critical aspect of this evolution. George et al. (2020) address the challenges posed by the exponential growth in data collection by IoT devices. Their work presents a solution that monitors data leaving the house through a device integrated within the home network. This approach aims to raise awareness about privacy risks and limit the amount of information collected. The study underscores the ethical considerations in IoT data collection and usage, highlighting the need for balancing technological advancements with privacy protection (George et al., 2020).

Lazaroiu and Roscia (2017) extend the concept of IoT integration in smart homes to the idea of smart districts and, ultimately, smart cities. Their research discusses how smart home technologies are integral to the sustainable development of urban areas. The paper designs a smart district model using IoT and blockchain technologies, emphasizing the role of efficient energy management systems. This model represents a step towards building smart cities, where homes are not isolated entities but fundamental parts of an interconnected urban ecosystem. The study illustrates the potential of IoT in enhancing quality of life, sustainability, and social and economic development in urban settings (Lazaroiu & Roscia, 2017).

In summary, the fundamental concepts of IoT integration in smart homes encompass a range of considerations from architectural design to privacy and urban development. The works collectively highlight the multifaceted nature of this integration. They emphasize the need for a comprehensive approach that considers the architectural, social, ethical, and urban implications of IoT in smart homes. As this field continues to evolve, these considerations will play a crucial role in shaping how we live and interact with our increasingly connected and intelligent living spaces.

3.2. Architectural Overview: Connecting Devices, Sensors, and Platforms

The architectural framework of IoT in smart homes is a complex ecosystem involving the integration of various devices, sensors, and platforms. This integration is pivotal in transforming traditional homes into interconnected, intelligent environments capable of enhancing efficiency, security, and user experience.

Vashi et al. (2017) provide a comprehensive overview of the architecture of IoT, emphasizing its complexity due to the large number of devices, link layer technology, and services involved. The architecture is fundamental to the development of smart homes, as it facilitates the connection of sensors and devices through internet connectivity. This architecture is not static but evolves with technological advancements, adapting to new challenges and opportunities. The study also highlights the importance of security in IoT, considering the vast amount of data and the interconnected nature of the devices (Vashi et al., 2017).

Khan et al. (2022) delve into the architectural threats to security and privacy in IoT applications, including smart homes. Their research underscores the significance of securing the technological resources from unauthorized access and disruptions. The layered architecture of IoT, from the perception layer to cloud computing, necessitates robust security measures to protect against various threats and vulnerabilities. This aspect is crucial in maintaining the seamless and ubiquitous connectivity that is the hallmark of smart home IoT systems (Khan et al., 2022).

Kodali, Soratkal, and Boppana (2016) explore the practical application of IoT in controlling home appliances. Their work presents an overview of IoT architecture and protocol suite, demonstrating how existing infrastructure, such as WiFi hotspots, can be utilized to develop cost-effective IoT solutions. This approach enables the enhancement of old appliances, making them part of the smart home ecosystem. The study illustrates the wide range of applications of IoT in home automation, from controlling lights and temperature to managing security systems (Kodali et al., 2016).

The architectural overview of connecting devices, sensors, and platforms in smart homes is a multifaceted and evolving domain. The works collectively highlight the complexity, security challenges, and practical applications of IoT in smart homes. As the technology continues to advance, the architecture of IoT in smart homes will likely become more integrated and sophisticated, further enhancing the capabilities and functionalities of these intelligent living spaces.

3.3. Enhancing Security in IoT-enabled Smart Homes

The integration of the Internet of Things (IoT) in smart homes has brought about significant advancements in home automation, but it has also introduced new challenges in terms of security. Enhancing security in IoT-enabled smart homes is crucial to protect against breaches and ensure the privacy and safety of users.

Anupriya and Muthumanikandan (2023) conducted a comprehensive survey on the effectiveness of IoT-based home security systems. Their research highlights the interconnected nature of smart home devices and the resultant security vulnerabilities. The study emphasizes the need for robust security layers to prevent data theft and unauthorized access. It proposes a comprehensive IoT security management framework for smart homes, addressing the day-to-day safety challenges and updating security measures to keep pace with technological advancements (Anupriya & Muthumanikandan, 2023).

Srivastava and Prakash (2020) explore the enhancement of IoT-based smart home security using a hybrid technique. Their proposed solution combines multiple security techniques to enhance the security and encryption speed of smart

home appliances. This hybrid approach aims to provide better data security, confidentiality, and integrity for IoT devices, addressing the evolving nature of security attacks and the need for adaptable and robust security solutions (Srivastava & Prakash, 2020).

Hamzah and Abdul-Rahaim (2022) focus on smart home automation systems using cloud computing to enhance security. Their system employs face detection and recognition methods, along with Radio Frequency Identification (RFID), to improve the performance of home security systems. The cloud server analyzes member identification to control access to the home, demonstrating effectiveness in transmitting live captures of any illegal activity. The study also discusses employing fog computing architecture in smart homes to reduce latency, ensure data storage, and maintain information security, acting as a broker between the IoT layer, cloud servers, and the user layer (Hamzah & Abdul-Rahaim, 2022).

In summary, enhancing security in IoT-enabled smart homes involves a multifaceted approach that includes robust security frameworks, hybrid security techniques, and the integration of advanced technologies like cloud and fog computing. The research by the authors collectively underscores the importance of continuously evolving security measures to address the dynamic challenges posed by IoT integration in smart homes. As IoT technology advances, so must the security strategies to protect the privacy and safety of users in these interconnected environments.

3.4. User Experience and Adaptability in IoT-based Smart Homes

The integration of the Internet of Things (IoT) in smart homes has significantly transformed user experience and adaptability. This transformation is not just about technological advancement but also about how users interact with and adapt to these changes in their living environments.

Lu (2018) discusses an IoT-enabled adaptive context-aware and playful cyber-physical system designed for everyday energy savings. This system leverages IoT technologies to create a more engaging and user-friendly experience. By incorporating bidirectionally interactive information visualization integrated with pet-raising gamification, the system aligns the information from the user's physical environment with its counterpart in the pet's virtual environment. This approach not only makes energy savings a more enjoyable task but also enhances system adaptability and user engagement in everyday activities. The study demonstrates how IoT can transform mundane tasks into playful and engaging experiences, thereby improving user interaction with smart home systems (Lu, 2018).

George et al. (2020) address the integration of social and technical solutions to enhance privacy in smart homes. Their research presents a solution that monitors data leaving the house through a device integrated within the home network. This approach aims to raise awareness about privacy risks and limit the amount of information collected. The study highlights the importance of considering user privacy and ethical implications in the design and implementation of IoT devices in smart homes. It underscores the need for solutions that balance technological advancements with the protection of user privacy (George et al., 2020).

Gkouskos, Linde, and Reddy (2019) explore the concept of interface in the context of IoT in smart homes. Their research focuses on how users interact with IoT devices and the adaptability of these interactions. The study suggests that the proliferation of IoT has turned the home into a 'smart' space, providing new opportunities for supporting creative experiences. It emphasizes the importance of designing adaptable IoT devices that can be easily integrated into the user's daily routine and lifestyle. The research highlights the need for intuitive and user-friendly interfaces that facilitate seamless interaction between users and IoT devices in smart homes (Gkouskos et al., 2019).

User experience and adaptability in IoT-based smart homes involve creating systems that are not only technologically advanced but also user-centric and engaging. The studies collectively emphasize the importance of designing IoT systems that are adaptable, privacy-conscious, and enhance the overall user experience. As IoT continues to evolve, focusing on these aspects will be crucial in ensuring that smart homes are not only efficient and secure but also enjoyable and intuitive for users.

3.5. Technological Milestones in IoT Integration

The integration of the Internet of Things (IoT) in smart homes has marked several technological milestones, significantly transforming how homes function and interact with their inhabitants. These milestones reflect the evolution of IoT from basic connectivity to advanced, intelligent systems.

Priyashan and Thilakarathne (2020) discuss an IIoT (Industrial Internet of Things) framework in the context of Industry 4.0, which is also applicable to smart homes. Their framework focuses on the integration of IoT components in industrial environments, providing insights into how similar technologies can be adapted for smart homes. The framework emphasizes the importance of data collection and analysis for optimizing processes, a principle that can be applied to smart home management for energy efficiency, security, and user convenience. This research highlights the crossover potential of IoT technologies between industrial and residential applications (Priyashan & Thilakarathne, 2020).

Furman and Haney (2020) explore the distinction between smart homes and connected homes. Their study, "Is My Home Smart or Just Connected?", investigates consumer perceptions of smart homes and IoT. The research reveals that while many users are familiar with the concept of connected devices, their understanding of what makes a home 'smart' is less clear. The study emphasizes the need for consumer education on the capabilities and implications of IoT in smart homes, particularly in terms of artificial intelligence (AI) and machine learning. This milestone in IoT integration reflects the transition from mere connectivity to intelligent, learning systems in home automation (Furman & Haney, 2020).

The technological milestones in IoT integration in smart homes encompass advancements in security, cross-application of industrial IoT frameworks, and the evolution from connected to intelligent homes. The authors collectively highlight the multifaceted nature of IoT integration, demonstrating its impact on security, efficiency, and the overall intelligence of home automation systems. As IoT continues to evolve, these milestones will likely pave the way for more sophisticated, secure, and user-centric smart home technologies.

3.6. State-of-the-Art Innovations in Smart Home IoT Ecosystem

The smart home IoT ecosystem has witnessed a surge in state-of-the-art innovations, significantly enhancing the capabilities and functionalities of modern homes. These advancements are not just limited to automation but extend to various aspects of home management, including energy efficiency, security, healthcare, and retail.

Zielonka et al. (2021) present a comprehensive study on recent trends and advances in smart home development. Their research highlights the ubiquitous support provided by intelligent appliances in modern homes, which continuously gather information to solve everyday issues. The study emphasizes the role of IoT in various industries, particularly in healthcare and energy management, showcasing how smart homes can support users in diverse ways. The analysis provides an outlook on the spectrum of proposed solutions and identifies leading publishers and innovators in the field. This research underscores the rapid development and potential future directions in the smart home industry (Zielonka et al., 2021).

Mainetti, Mighali, and Patrono (2015) discuss an IoT-based user-centric ecosystem for heterogeneous smart home environments. Their work focuses on overcoming the limitations posed by the heterogeneity of underlying technologies in smart homes. The proposed software ecosystem allows users of different skill levels to develop location-aware services that autonomously manage the smart home environment. These services control the environment according to user-defined rules and the users' location, calculated using an indoor localization mechanism. The study highlights the importance of user involvement in the development of applicative services and the need for multi-protocol middleware to access the physical network, addressing the technological heterogeneities (Mainetti et al., 2015).

Baswani, George, and Townsend (2018) explored the intersection of connected homes and online retail, particularly in the context of IoT-enabled online shopping. Their research examines factors affecting consumer behavior towards adopting IoT online shopping artifacts, such as Amazon’s Dash Wand and Google Home smart speakers. The study identifies key determinants, including security concerns, performance expectancy, effort expectancy, facilitating conditions, and price value. This research provides insights into consumer adoption of connected home innovations and offers guidance for shaping these innovations and their associated services (Baswani et al., 2018).

Therefore, the state-of-the-art innovations in the smart home IoT ecosystem encompass a wide range of applications and functionalities. These studies collectively highlight the advancements in smart home technologies, emphasizing the importance of user-centric approaches, overcoming technological heterogeneities, and understanding consumer behavior in the context of IoT. As the IoT ecosystem continues to evolve, these innovations will likely lead to more sophisticated, efficient, and user-friendly smart home solutions.

3.7. Emerging Trends in IoT Integration

The integration of the Internet of Things (IoT) in smart homes is continuously evolving, with emerging trends shaping the future of home automation, security, and user interaction. These trends are not only enhancing the capabilities of smart homes but also addressing challenges such as security, privacy, and interoperability.

Hou et al. (2023) discuss the trends and challenges in AIoT/IIoT/IoT implementation, highlighting the leading technologies such as metaverse, digital twin, and autonomous vehicle applications. Their research emphasizes the crucial role of AIoT in providing essential data for these advanced applications. The study addresses the multidisciplinary nature of AIoT and its evolution, focusing on core hardware, software, and middleware, including developments in TinyML and neuromorphic computing. The research underscores the challenges that need to be overcome, such as safety, security, latency, interoperability, and reliability of sensor data, which are essential for the successful implementation of AIoT in smart homes (Hou et al., 2023).

Plachkinova, Vo, and Alluhaidan (2016) explore emerging trends in smart home security, privacy, and digital forensics. Their work reviews current literature and identifies key trends, including potential remote security breaches, risks for smart home devices, privacy violations, infrastructure vulnerabilities, and challenges in digital forensics. The study integrates these trends into a conceptual model, showcasing their roles in the IoT landscape and highlighting the bimodal lenses in security and privacy: preventive and investigative. This research offers directions for future development in ensuring safe and secure smart homes (Plachkinova, Vo, and Alluhaidan, 2016).

Chen et al. (2022) introduce the special issue on smart systems for Industry 4.0 and IoT, focusing on the development of big data applications and the growth of hybrid data from multiple IoT sources. Their research discusses emerging technologies for the near real-time extraction and analysis of heterogeneous data, including deep learning approaches that tackle the limitations of traditional machine learning. The study also addresses new security and privacy concerns and the importance of technology adoption and trust. The research highlights the transformations in industrial operations and the implications for smart homes, emphasizing the need for efficient, scalable, and flexible communication networks to support the increasing demands of IoT services (Chen et al., 2022).

Emerging trends in IoT integration in smart homes are characterized by advancements in AIoT technologies, heightened focus on security and privacy, and the development of new frameworks for data analysis and communication. The studies collectively highlight the dynamic nature of IoT integration, pointing towards a future where smart homes are not only more intelligent and interconnected but also safer and more user-friendly.

3.7.1. Edge Computing in Smart Homes

Edge computing has emerged as a pivotal technology in the realm of IoT, particularly in smart homes, where it enhances data processing capabilities and improves response times at the network's edges. This technology is instrumental in addressing the challenges of bandwidth, latency, and privacy in IoT-enabled smart homes.

Shehab and Al-Janabi (2020) explore the implementation of an experimental Edge Computing (EC) system based on Microsoft Azure IoT in a Smart Home Environment (SHE). Their study focuses on device management patterns and security concerns in edge computing. The research demonstrates the use of a Raspberry Pi as an edge device to host virtual sensor devices, providing insights into the configuration management patterns and the impact of edge analytics on system performance. The study also delves into the use of symmetric encryption to enhance security aspects, highlighting the importance of secure and efficient data processing in smart homes (Shehab & Al-Janabi, 2020).

Yar et al. (2021) present a smart home automation system that leverages the IoT-enabled edge-computing paradigm. Their system utilizes a Raspberry Pi as a central controlling unit, interconnecting various devices and sensors in the home via the Internet. The research proposes an integrated system that provides remote and automatic control of home appliances, ensuring security and safety while preserving customer privacy. The system processes and stores sensor-generated data on the edge device to reduce bandwidth, computation, and storage costs. This approach demonstrates the efficiency of edge computing in smart home applications, particularly in terms of energy consumption and response times (Yar et al., 2021).

Vallati et al. (2016) discuss the role of mobile-edge computing (MEC) in future smart homes, particularly in the context of 5G cellular networks supporting IoT. Their research highlights the potential of MEC to enrich broadband communication networks by placing cloud-computing-like capabilities within the radio access network. This distributed computing and storage infrastructure enables the deployment of applications and services at the network's edge,

facilitating efficient and rapid responses in smart home environments. The study underscores the importance of MEC in supporting time-critical and opportunistic applications in smart homes (Vallati et al., 2016).

Edge computing plays a crucial role in enhancing the capabilities of smart homes within the IoT ecosystem. The studies collectively highlight the benefits of edge computing in smart homes, including improved data processing, enhanced security, reduced latency, and efficient resource utilization. As IoT technologies continue to evolve, edge computing is likely to become increasingly integral to the development of intelligent and responsive smart home systems.

3.7.2. AI and Machine Learning Applications

The integration of Artificial Intelligence (AI) and Machine Learning (ML) in smart homes has revolutionized the way these environments interact with their inhabitants. These technologies are enhancing the capabilities of IoT devices, making homes more intelligent, efficient, and user-friendly. Jain et al. (2022) present the design of a smart wireless home automation system that fuses IoT and machine learning over a cloud environment. Their system, deployed on a resource-constrained Raspberry Pi device, provides a cost-effective platform for interconnecting various devices and sensors in a home. The proposed system utilizes ML algorithms to predict user behavior and optimize the operation of smart home systems. This approach not only enhances the automation and efficiency of smart homes but also addresses privacy concerns by processing and storing sensor-generated data locally. The research highlights the effectiveness of combining IoT and ML in smart home automation, particularly in terms of energy consumption and response times (Jain et al., 2022).

Oprea (2021) explores the integration of AI in education through IoT projects based on machine learning. The study presents IoT projects, such as speech and facial recognition, developed on the Arduino platform. These projects demonstrate the application of ML algorithms in real-world scenarios, including smart home environments. The research emphasizes the importance of understanding AI and ML in the context of IoT, particularly for educational purposes. The study showcases how ML can be applied to enhance the capabilities of smart devices, contributing to the development of intelligent home systems (Oprea, 2021).

In summary, AI and machine learning applications in smart homes are playing a transformative role in enhancing the intelligence and efficiency of these environments. The studies highlight the potential of ML algorithms in device classification, behavior prediction, and the development of intelligent systems. As AI and ML continue to evolve, their integration in smart homes is likely to lead to more advanced, secure, and user-centric solutions.

3.7.3. Energy Efficiency and Sustainability in IoT-Based Smart Homes

The integration of the Internet of Things (IoT) in smart homes has been a key driver in enhancing energy efficiency and promoting sustainability. This integration leverages advanced technologies to optimize energy consumption, reduce waste, and contribute to environmental protection.

Ehsanifar et al. (2023) explore a sustainable pattern of waste management and energy efficiency in smart homes using IoT. Their research focuses on the model of waste management in smart homes, emphasizing the role of IoT in reducing energy costs and managing waste effectively. The study employs a computational approach to collect data and uses MATLAB and STATA software for analysis. The findings reveal that IoT technology significantly impacts energy costs, the number of home residents, and home area in smart homes. This research underscores the importance of IoT in developing sustainable smart homes that not only conserve energy but also manage waste efficiently (Ehsanifar et al., 2023).

Arpilleda (2023) investigates the impact of IoT on home automation and energy management. The study employs a mixed-methods research approach, including structured surveys and qualitative interviews, to assess the effects of IoT-driven solutions on energy consumption. The findings indicate a 20% reduction in energy consumption post-IoT implementation, highlighting the potential for sustainable energy practices. The study also notes the challenges of data privacy and security, emphasizing the need for comprehensive safeguards. This research contributes to the discourse on IoT's potential to revolutionize domestic energy consumption and automation, balancing efficiency and user comfort in smart homes (Arpilleda, 2023).

Sudhakar et al. (2023) present an experimental analysis of an IoT-based smart home automation system for energy conservation. The study explores the integration of actuators, sensors, and controllers with IoT technology, demonstrating the system's ability to reduce energy consumption. The research involves statistical analysis of test data from a prototype system, providing insights for constructing sustainable residential settings. The study highlights the

potential of IoT-based systems in saving energy and promoting a sustainable future, investigating the effects of residential environments on energy conservation (Sudhakar et al., 2023).

From the foregoing, energy efficiency and sustainability in IoT-based smart homes are crucial aspects of modern home automation. The studies collectively emphasize the role of IoT in enhancing energy management, reducing waste, and promoting sustainable living. As IoT technologies continue to evolve, their application in smart homes is likely to lead to more energy-efficient and environmentally friendly solutions.

4. Discussion of Findings

4.1. Technological, Economic, and Security Implications of IoT in Smart Homes

The integration of the Internet of Things (IoT) in smart homes has brought about significant technological advancements, economic benefits, and security challenges. These implications are crucial in understanding the broader impact of IoT on society and individual households.

George et al. (2020) explore the integration of social and technical solutions to address privacy concerns in smart homes. Their study presents a solution that monitors data leaving the house through a device integrated within the home network. This approach aims to raise awareness about privacy risks and limit the amount of information collected. The research highlights the ethical considerations in IoT data collection and usage, emphasizing the need for solutions that balance technological advancements with the protection of user privacy. The study contributes to the understanding of the economic implications of IoT in smart homes, particularly in terms of data privacy and security (George et al., 2020).

Khan, Chaturvedi, and Jaswal (2022) discuss the implications of IoT in the context of smart cities, which extends to smart homes. Their research focuses on how IoT technologies enable cities to enhance economic performance and generate innovative technological solutions. The study examines the role of IoT in smart detection, location monitoring, and management, providing insights into the economic and technological benefits of IoT in urban environments. The research also addresses the challenges posed by IoT systems, including security and privacy concerns, emphasizing the need for comprehensive strategies to mitigate these risks (Khan et al., 2022).

The technological, economic, and security implications of IoT in smart homes are multifaceted and complex. The studies emphasize the importance of addressing security and privacy concerns, balancing technological innovation with ethical considerations, and understanding the economic benefits and risks associated with IoT integration in smart homes.

4.1.1. Cost-Benefit Analysis of IoT in Smart Homes

The integration of the Internet of Things (IoT) in smart homes has brought about a paradigm shift in how homes are managed and operated. A cost-benefit analysis of this integration is essential to understand the economic implications and the value proposition offered by IoT in smart homes.

Fakhar, Yalcin, and Bilge (2023) conducted a survey analysis to assess the impact of smart home services on energy consumption and cost. Their study highlights the significant role of smart home systems in reducing energy consumption, particularly in light of rising energy costs. The research indicates that smart home services, such as automated control systems for temperature, lighting, and roller shutters, contribute to substantial energy savings. The study underscores the economic benefits of smart home systems, demonstrating that investments in IoT technologies can lead to reduced energy bills and enhanced efficiency in home management (Fakhar, Yalcin, and Bilge, 2023).

Mazhar and Shafiq (2020) present a study characterizing smart home IoT traffic in the wild. Their research focuses on the network traffic generated by smart home IoT devices, analyzing its volume, patterns, and external endpoints. The study reveals that smart home IoT devices, such as smart TVs, generate high-volume traffic to content streaming services, following patterns associated with human activity. The findings highlight the centralized nature of the smart home IoT ecosystem due to its reliance on popular cloud and DNS services. This research provides insights into the management, security, and privacy concerns of smart home IoT devices, emphasizing the need for policy-based access control and application layer encryption. The study contributes to understanding the cost implications of managing and securing IoT traffic in smart homes (Mazhar & Shafiq, 2020).

Jiang, Wang, and Song (2023) analyze the cost savings and occupants' preferences in grid-interactive smart home operation. Their research constructs a framework integrating a multi-objective optimization method, a learning-based system modeling approach, and a novel comfort index method. The study focuses on the economic operation of electrical

appliances in homes, considering time-of-use rates and user comfort. The results show that the proposed framework allows for preferred thermal comfort with a marginal cost increase, demonstrating the potential for cost savings in smart home operation. The research highlights the correlation between cost saving and user comfort, providing a quantitative analysis of the economic benefits of smart home systems (Jiang, Wang, and Song, 2023).

In summary, the cost-benefit analysis of IoT in smart homes reveals significant economic advantages, including reduced energy consumption and cost savings. The studies collectively highlight the economic implications of IoT integration in smart homes, emphasizing the importance of efficient management, security, and user-centric design in maximizing the benefits of these technologies.

4.1.2. Security Challenges and Solutions 4.1.3. Privacy Concerns in IoT-enabled Smart Homes

The proliferation of IoT in smart homes has brought numerous benefits, but it has also introduced significant security challenges. Addressing these challenges is crucial to ensure the safety and privacy of users in IoT-enabled environments. Aldahmani et al. (2023) provides an overview of the critical security issues for IoT smart home systems and proposes potential solutions to mitigate these risks. The study emphasizes the importance of understanding vulnerabilities and applying security measures to ensure that the IoT system is more reliable and safe. The challenges and security issues highlighted include the need for robust encryption, secure communication protocols, and regular software updates. The proposed solutions focus on enhancing the security of IoT devices and networks, thereby making smart homes more secure and resilient against cyber threats.

Ali et al. (2017) investigate security attacks in smart homes and evaluate their impact on the overall system security. The study identifies security requirements and solutions in the smart home environment, suggesting security goals based on various scenarios. The research forecasts security attacks, such as malware and viruses, and estimates their expected frequency in the coming years. The study provides a comprehensive analysis of the security landscape in smart homes, emphasizing the need for effective security mechanisms to protect against a wide range of cyber threats (Ali et al., 2017).

Aldahmani et al. (2023) discuss the cyber-security of embedded IoTs in smart homes, focusing on challenges, requirements, countermeasures, and trends. The study examines the design, objects, and standards of IoT and addresses the tiered Internet of Things framework and smart home security concerns. The research explores IoT-based smart home difficulties and offers solutions, including the implementation of advanced security protocols and the adoption of best practices in device manufacturing and network management. The study highlights the evolving nature of IoT security and the importance of continuous innovation in security technologies to safeguard smart homes (Aldahmani et al., 2023).

The security challenges in IoT-based smart homes are diverse and complex, requiring a multifaceted approach to address them effectively. The studies collectively underscore the need for robust security measures, including encryption, secure protocols, and regular updates, to protect smart homes from cyber threats. As IoT technology continues to evolve, so must the security strategies to ensure the safety and privacy of users in these interconnected environments.

4.2. User Adoption and Behavior in IoT-based Smart Homes

The adoption and behavior of users in IoT-based smart homes are critical factors in the success and effectiveness of these technologies. Understanding user attitudes, preferences, and concerns is essential for designing and implementing IoT solutions that meet the needs and expectations of homeowners.

Yang, Lee, and Lee (2018) investigate the factors influencing the adoption of IoT smart home services. Their study examines the critical features that users require in smart home services and evaluates the relationship between these factors and adoption behavior. The research also tests the moderating effect of personal characteristics on behavior. The findings provide insights into the importance of proper level automation in smart homes and the need for providing appropriate functions and features to cater to the diverse preferences of potential users. This study underscores the significance of understanding user requirements and preferences in the diffusion of smart home services (Yang, Lee, and Lee, 2018).

Lafontaine, Sabir, and Das (2021) delve into understanding people's attitudes and concerns towards adopting IoT devices. Their research conducts an online survey to collect responses from both adopters and non-adopters of IoT devices. The study reveals similarities and differences in perceptions and concerns between these two groups. For

instance, IoT users are more comfortable using IoT devices in private settings compared to non-IoT users. The research also finds regional differences in attitudes towards IoT adoption, with participants from different geographic regions showcasing contrasting behaviors. The study provides recommendations to reduce users' concerns and enhance trust towards adopting IoT devices (Lafontaine, Sabir, and Das, 2021).

4.2.1. User Satisfaction and Comfort in IpT-Based Smart Homes

The integration of the Internet of Things (IoT) in smart homes has significantly impacted user satisfaction and comfort. This impact is reflected in the way IoT technologies enhance home automation, energy management, and overall living experience.

Arpilleda (2023) investigates the impact of IoT on home automation and energy management. The study employs a mixed-methods approach, including structured surveys and qualitative interviews, to assess the effects of IoT-driven solutions on energy consumption and user satisfaction. The findings indicate a 20% reduction in energy consumption post-IoT implementation, highlighting the potential for sustainable energy practices. Participants reported increased satisfaction with the convenience of remote control and observed significant cost savings in energy bills. However, the study also identifies data privacy and security concerns as challenges, emphasizing the need for comprehensive safeguards. This research contributes to understanding how IoT can enhance user comfort and satisfaction in smart homes while balancing efficiency and privacy concerns (Arpilleda, 2023).

Jiang, Wang, and Song (2023) present a quantitative analysis of cost savings and occupants' preferences in grid-interactive smart home operation. Their research constructs a framework integrating a multi-objective optimization method, a learning-based system modeling approach, and a novel comfort index method. The study focuses on the economic operation of electrical appliances in homes, considering time-of-use rates and user comfort. The results show that the proposed framework allows for preferred thermal comfort with a marginal cost increase, demonstrating the potential for cost savings in smart home operation. The research highlights the correlation between cost saving and user comfort, providing a quantitative analysis of the economic benefits of smart home systems (Jiang et al., 2023).

Nolich et al. (2019) explore a novel comfort optimization framework for IoT-equipped smart environments, with applications on cruise ships. The study presents E-Cabin, an IoT framework architecture that includes a reasoning system tuned on data gathered from the environment and each specific passenger. The framework leverages knowledge representation with ontologies and consists of a publisher–subscriber communication framework. The research demonstrates the system in a demo cruise cabin where various atmospheres can be set based on the users and activities occurring in the cabin. This study provides insights into how IoT can be used to optimize comfort in smart environments, including smart homes (Nolich et al., 2019).

User satisfaction and comfort in IoT-based smart homes are influenced by various factors, including energy optimization, automation levels, privacy concerns, and personal preferences. Understanding and addressing user concerns and preferences are crucial for the successful adoption and effective use of IoT technologies in smart homes.

4.2.2. Barriers to Adoption and Potential Solutions in IoT-Based Smart Homes

The adoption of IoT in smart homes faces several barriers, ranging from cybersecurity concerns to technical complexities. Understanding and addressing these barriers is essential for the widespread acceptance and effective use of IoT technologies in residential settings.

Venkatraman, Overmars, and Thong (2021) address the barriers to smart home automation, focusing on the integration of voice-based control systems. The study identifies key challenges such as the heterogeneity of underlying technologies, security and privacy concerns, and the lack of user awareness about the potential of machine intelligence. To overcome these barriers, the research proposes a model integrating IoT services and wireless technologies for developing a secure smart home automation system with a voice-controlled AI system. The model's application in various use cases demonstrates the feasibility of an integrated, secure, and user-friendly smart home environment. This approach highlights the importance of simplicity, security, and integration in fostering the adoption of smart home automation (Venkatraman et al., 2021).

George et al. (2020) discuss integrating social and technical solutions to address privacy concerns in smart homes. The study presents a solution that monitors data leaving the house through a device integrated within the home network. This approach aims to raise awareness about privacy risks and limit the amount of information collected. The research underscores the need for comprehensive strategies to address privacy concerns, which are a significant barrier to the

adoption of IoT devices in smart homes. The study contributes to understanding the importance of balancing technological advancements with the protection of user privacy (George et al., 2020).

In summary, the barriers to the adoption of IoT in smart homes include cybersecurity concerns, technical complexities, and privacy issues. The studies collectively highlight the need for robust security measures, user-friendly interfaces, and privacy safeguards to enhance the adoption of IoT technologies in smart homes. Addressing these barriers through integrated solutions and consumer education is key to the successful implementation and widespread acceptance of smart home IoT systems.

4.2.3. User-Driven Customization and Personalization

The integration of IoT in smart homes has opened up new possibilities for user-driven customization and personalization, significantly enhancing the user experience. This integration allows for tailored solutions that meet individual preferences and needs.

Pridmore et al. (2019) explore the role of intelligent personal assistants (IPAs) in the context of dataveillance in platformed households. Their study focuses on the intercultural negotiations of privacy and data surveillance afforded by IPAs like Google Home and Amazon Echo. The research reveals how these devices, while offering personalized services, also raise concerns about data privacy and commodification of personal information. The study underscores the need for a nuanced approach to managing privacy in smart homes, balancing the benefits of personalization with the risks associated with data collection and usage (Pridmore et al., 2019).

Yao et al. (2018) present WITS, an IoT-endowed computational framework for activity recognition in personalized smart homes. The framework is designed to recognize and adapt to user activities, providing a personalized experience in smart homes. WITS utilizes machine learning algorithms to analyze data from various sensors, enabling the system to learn and adapt to the user's lifestyle and preferences. This approach demonstrates the potential of IoT in creating smart home environments that are not only automated but also highly personalized and responsive to individual user needs (Yao et al., 2018).

This means that user-driven customization and personalization in IoT-based smart homes are key factors in enhancing user satisfaction and experience. The studies collectively highlight the importance of balancing personalization with privacy concerns, utilizing machine learning for adaptive environments, and applying industrial principles to residential settings. As IoT technologies continue to evolve, the potential for creating highly personalized and user-centric smart homes becomes increasingly feasible.

4.3. Future Directions in IoT for Smart Homes

The field of IoT in smart homes is rapidly evolving, with emerging trends and technologies shaping its future. The integration of advanced technologies like machine learning and the increasing focus on cybersecurity are key aspects driving this evolution.

Kaushik, Bhardwaj, and Dahiya (2023) delve into the realm of smart home IoT forensics, discussing the current status, challenges, and future directions. Their research highlights the complexities involved in data retrieval from various smart home devices, which is crucial for digital forensic investigations. The study emphasizes the need for developing standardized methods for data extraction and analysis in IoT environments. Looking ahead, the research suggests that future advancements in IoT forensics will focus on enhancing data security and privacy while improving the efficiency of forensic processes. This evolution is critical for maintaining the integrity and reliability of smart home systems (Kaushik et al., 2023).

Saleem, Hassan, and Ali (2022) review the integration of machine learning in smart homes, providing insights into its benefits and limitations. Their study explores how machine learning can be used to make smart homes more adaptive to users' activities, thereby enhancing security levels, reducing power consumption, and improving usability experiences. The paper discusses the challenges and perspectives of future development in smart home systems, emphasizing the need for more research in machine intelligence and smart home automation. The integration of machine learning is expected to play a significant role in the future of smart homes, making them more intelligent and responsive to user needs (Saleem et al., 2022).

Waseem,et al. (2023) explore the application of machine learning in IoT smart home automation. Their research proposes a taxonomy of machine learning for smart homes based on its applications. The study includes a detailed

analysis of various surveys and literature reviews, highlighting open challenges and issues in the field. The research suggests that future directions in smart home automation will involve more sophisticated implementations of machine learning, aiming to enhance the overall functionality and user experience of smart homes. This advancement is expected to bring about significant improvements in the efficiency and effectiveness of smart home systems (Waseem et al., 2023).

The future directions in IoT for smart homes are characterized by advancements in machine learning applications, enhanced cybersecurity measures, and the development of standardized forensic processes. The studies highlight the evolving nature of IoT in smart homes, pointing towards a future where these environments are not only more intelligent and interconnected but also safer and more user-friendly.

4.3.1. Integration with Smart Cities and Infrastructure

The integration of IoT-based smart homes with smart cities and infrastructure is a key aspect of urban development, offering numerous benefits in terms of efficiency, sustainability, and quality of life.

Lynggaard and Skouby (2016) discuss the role of complex IoT systems as enablers for smart homes within a broader smart city vision. Their study proposes a hierarchical layered ICT-based infrastructure that seamlessly integrates IoT, smart homes, and smart city structures. This integrated approach addresses the "big challenges" of sustainable urban development and improves the quality of life for citizens. The research highlights a specific application of this infrastructure in wastewater energy harvesting from smart buildings, demonstrating considerable energy savings and reduced peak-load for district heating plants. The study underscores the potential of IoT in creating interconnected and efficient urban ecosystems, where smart homes play a crucial role (Lynggaard & Skouby, 2016).

Ahmed et al. (2023) provide a comprehensive review of smart homes and cities, considering sustainability developments, concepts, and future trends. The study examines the benefits of adopting smart homes and smart cities, such as increased efficiency, reduced energy waste, and improved safety. It also addresses challenges like privacy, data security, and interoperability. The research suggests that overcoming these challenges requires collaboration between various stakeholders to create a framework that balances innovation, privacy, and sustainability. The study emphasizes the potential of smart homes and cities to significantly improve everyday lives and contribute to a more prosperous and environmentally friendly future (Ahmed et al., 2023).

The integration of IoT-based smart homes with smart cities and infrastructure is crucial for the development of sustainable and efficient urban environments. The studies highlight the importance of this integration in enhancing urban living. As IoT technologies continue to evolve, their application in smart homes and cities is likely to lead to more interconnected, intelligent, and sustainable urban solutions.

4.3.2. Interoperability and Standardization in IoT-Based Smart Homes

The advancement of IoT in smart homes is significantly influenced by the challenges and opportunities in interoperability and standardization. These aspects are crucial for the seamless integration and efficient functioning of diverse IoT devices and systems.

Lynggaard and Skouby (2016) discuss the role of complex IoT systems in enabling smart homes within a smart city vision. Their study emphasizes the importance of interoperability in the IoT ecosystem, particularly in the context of smart homes and cities. The research proposes a hierarchical layered ICT-based infrastructure that integrates IoT devices, smart homes, and smart city structures. This integrated approach addresses the challenges of sustainable urban development and improves the quality of life for citizens. The study underscores the potential of IoT in creating interconnected and efficient urban ecosystems, where smart homes play a crucial role (Lynggaard & Skouby, 2016).

Korkan, Kaebisch, and Steinhorst (2020) focus on streamlining IoT system development with open standards. Their research addresses the interoperability problem in IoT by utilizing the Thing Description (TD) standard developed by the World Wide Web Consortium (W3C). This standard allows humans and machines to understand the capabilities and communication interfaces of IoT devices. The study introduces methods that can be applied in different stages of IoT development or as a framework to streamline the development of IoT devices and systems. By using the TD standard, interoperability between various stakeholders' IoT devices is ensured from early stages, reducing time to market and enhancing system functionality (Korkan et al., 2020).

Interoperability and standardization are key factors in the development of IoT-based smart homes. The studies these authors highlight the importance of these aspects in enhancing urban living. As IoT technologies continue to evolve, their application in smart homes is likely to lead to more interconnected, intelligent, and sustainable urban solutions.

4.3.3. Cybersecurity Advancements

The rapid advancement of IoT in smart homes has necessitated a parallel development in cybersecurity measures to protect against increasing threats and vulnerabilities. Recent studies have focused on identifying these challenges and proposing advanced solutions to enhance the security of smart home environments.

Ayavaca-Vallejo and Avila-Pesantez (2023) conducted a systematic mapping study to assess the current state of cybersecurity in Smart Home Internet of Things (SHIoT). Their research identifies critical threats to SHIoT devices, including unsecured communications, lack of device security, and weak authentication mechanisms. The study evaluates 50 publications to understand the vulnerabilities and existing countermeasures for securing SHIoT devices. The findings emphasize the importance of encryption, firewalls, secure communication protocols, and robust authentication and access control to improve global security. This comprehensive survey underscores the evolving nature of cybersecurity in smart homes and the need for continuous innovation in security technologies (Ayavaca-Vallejo & Avila-Pesantez, 2023).

Anupriya and Muthumanikandan (2023) explore the effectiveness of IoT-based home security systems. Their survey assesses the current landscape of IoT security, highlighting the challenges and potential solutions. The study reveals that while IoT devices offer enhanced home automation and convenience, they also pose significant security risks. The research suggests that improving IoT security requires a multi-layered approach, including the development of more secure hardware, software, and network protocols. The study contributes to the understanding of how IoT security can be enhanced to protect smart homes from cyber threats (Anupriya & Muthumanikandan, 2023).

George et al. (2020) discuss integrating social and technical solutions to address privacy concerns in smart homes. Their research presents a solution that monitors data leaving the house through a device integrated within the home network. This approach aims to raise awareness about privacy risks and limit the amount of information collected. The study highlights the need for comprehensive strategies to address privacy concerns, which are a significant aspect of cybersecurity in smart homes. The research contributes to understanding the importance of balancing technological advancements with the protection of user privacy (George et al., 2020).

Cybersecurity advancements in IoT-based smart homes are crucial for ensuring the safety and privacy of users. The studies highlight the need for robust security measures, including encryption, secure protocols, and regular updates, to protect smart homes from cyber threats. As IoT technology continues to evolve, so must the security strategies to ensure the safety and privacy of users in these interconnected environments.

5. Conclusion

The systematic review of IoT in U.S. smart homes has revealed several key insights. Firstly, the integration of IoT technologies in smart homes has significantly advanced, moving from basic automation to sophisticated, interconnected systems. This evolution has enhanced home management, energy efficiency, and user experience. Secondly, security remains a paramount concern, with advancements in cybersecurity measures being critical to protect user data and privacy. Thirdly, user adoption is influenced by factors such as perceived usefulness, ease of use, and concerns about privacy and security. Finally, the review highlighted the importance of interoperability and standardization in the IoT ecosystem for seamless functionality and user convenience.

The future landscape of IoT in U.S. smart homes is poised for further growth and innovation. The integration with smart city infrastructure is expected to enhance the efficiency and sustainability of urban living. Advancements in machine learning and AI are likely to make smart homes more intuitive and responsive to user needs. Additionally, the focus on cybersecurity and privacy will continue to be a priority, ensuring the safe and secure use of IoT technologies in residential settings.

For homeowners, it is recommended to stay informed about the latest IoT technologies and their implications for privacy and security. Adopting IoT solutions that offer robust security features and regular updates is crucial. For industry leaders, there is a need to focus on developing user-friendly, interoperable IoT solutions that prioritize security and privacy. Collaboration with regulatory bodies to establish and adhere to standardization protocols is also essential.

Additionally, industry leaders should invest in consumer education to enhance the understanding and trust in IoT technologies.

This study underscores the transformative impact of IoT on U.S. smart homes, highlighting both the opportunities and challenges. As the field continues to evolve, future research should focus on developing more advanced, secure, and user-centric IoT solutions. There is a need for ongoing research into the social, ethical, and legal implications of IoT in residential settings. Further exploration into the integration of IoT with renewable energy sources and sustainable practices in smart homes would also be beneficial. Lastly, longitudinal studies to assess the long-term impact of IoT on lifestyle, energy consumption, and overall well-being in smart homes would provide valuable insights for future advancements.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abbott, J., Dev, J., Kim, D., Gopavaram, S. R., Iyer, M., Sadam, S., ... & Camp, L. J. (2023). Kids, Cats, and Control: Designing Privacy and Security Dashboards for IoT Home Devices. In Proceedings 2023 Symposium on Usable Security. Internet Society. PP. 1-11. DOI: 10.14722/usec.2023.236290

[2] Abdlrazaq, A. A., Azzez, S. N., Anwer, M. A., & Hassen, S. I. (2023). Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology. Zanco Journal of Pure and Applied Sciences, 35(4), 84-96. DOI: 10.21271/zjpas.35.4.08

[3] Ahmed, A. A., Belrzaeg, M., Nassar, Y., El-Khozondar, H. J., Khaleel, M., & Alsharif, A. (2023). A comprehensive review towards smart homes and cities considering sustainability developments, concepts, and future trends. World J. Adv. Res. Rev, 19(1), 1482-1489. DOI: 10.30574/wjarr.2023.19.1.1530

[4] Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). IoT based smart home: Security challenges, security requirements and solutions," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, pp. 1-6, doi: 10.23919/IConAC.2017.8082057.

[5] Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. IEEE Open Journal of Vehicular Technology, 4, 281-292. DOI: 10.1109/OJVT.2023.3234069

[6] Anupriya, S. R., & Muthumanikandan, V. (2023). A Survey on Exploring the Effectiveness of IOT Based Home Security Systems," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-10, doi: 10.1109/ICCCI56745.2023.10128178.

[7] Arpilleda, J. Y. (2023). Impact of Internet of Things (IoT) on Home Automation and Energy Management. International Journal of Advanced Research in Science, Communication and Technology. 3(1), 602-606. DOI: 10.48175/ijarsct-11297

[8] Ayavaca-Vallejo, L., & Avila-Pesantez, D. (2023). Smart Home IoT Cybersecurity Survey: A Systematic Mapping," 2023 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2023, pp. 1-6, doi: 10.1109/ICTAS56421.2023.10082751.

[9] Baswani, S., George, J., & Townsend, A. (2018). Connected Homes and Online Retail: The Case of IoT Enabled Online Shopping. Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018, pp. 1-5.

[10] Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R., & Tom, E. (2020). Factoring user experience into the security and privacy design of smart home devices: A case study. In Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1-9). DOI: 10.1145/3334480.3382850

[11] Charmanasa, K., Georgioua, K., Mittasb, N., & Angelisa, L. (2023). Unveiling technology clusters and prominent investors of home automation networking through patent analysis. Algorithms, 9(22), 23. https://en.wikipedia.org/wiki/2Wire.

[12] Chen, M. Y., Thuraisingham, B., Egrioglu, E., & Rubio, J. D. J. (2023). Introduction to the Special Issue on Smart Systems for Industry 4.0 and IoT. ACM Transactions on Management Information Systems, 13(4), 1-3. DOI: 10.1145/3583985

[13] Dong, Y., Wan, K., Yue, Y. (2018). A Feedback-Based Adaptive Service-Oriented Paradigm for the Internet of Things. In: Braubach, L., et al. Service-Oriented Computing – ICSOC 2017 Workshops. ICSOC 2017. Lecture Notes in Computer Science. vol 10797. Springer, Cham. https://doi.org/10.1007/978-3-319-91764-1_11

[14] Ehsanifar, M., Dekamini, F., Spulbar, C., Birau, R., Khazaei, M., & Bărbăcioru, I. C. (2023). A Sustainable Pattern of Waste Management and Energy Efficiency in Smart Homes Using the Internet of Things (IoT). Sustainability, 15(6), 5081. DOI: 10.3390/su15065081

[15] Fakhar, M. Z., Yalcin, E., & Bilge, A. (2023). A survey of smart home energy conservation techniques. Expert Systems with Applications, 213, 118974. https://doi.org/10.1016/j.eswa.2022.118974

[16] Furman, S., & Haney, J. M. (2020). Is My Home Smart or Just Connected? In: Degen, H., Reinerman-Jones, L. (eds) Artificial Intelligence in HCI. HCII 2020. Lecture Notes in Computer Science(), vol. 12217. Springer, Cham. https://doi.org/10.1007/978-3-030-50334-5_18. DOI: 10.1007/978-3-030-50334-5_18

[17] George, C. G., Tyranski, D. R., Simons, D. P., O'Quinn, J. D., York, E., & Salman, A. (2020). Integrating Social and Technical Solutions to Address Privacy in Smart Homes," 2020 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 2020, pp. 1-6, doi: 10.1109/SIEDS49339.2020.9106585.

[18] Gkouskos, D., Linde, P., & Reddy, A. (2019). Where is the interface?–Appropriating Interaction with IoT in the Smart Home. EAI Endorsed Transactions on Creative Technologies, 6(19). DOI: 10.4108/eai.13-7-2018.161174

[19] Hamzah, A. S., & Abdul-Rahaim, L. (2022). Smart Homes Automation System Using Cloud Computing Based Enhancement Security," 2022 5th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, 2022, pp. 164-169, doi: 10.1109/IICETA54559.2022.9888307.

[20] Hou, K. M., Diao, X., Shi, H., Ding, H., Zhou, H., & de Vaulx, C. (2023). Trends and Challenges in AIoT/IIoT/IoT Implementation. Sensors, 23(11), 5074. DOI: 10.3390/s23115074

[21] Ishaq, K., & Farooq, S. S. (2023). Exploring IoT in Smart Cities: Practices, Challenges and Way Forward. DOI: 10.48550/arXiv.2309.12344

[22] Jain, R., Bekuma, Y., Pattanaik, B., Assebe, A., & Bayisa, T. (2022). Design of a Smart Wireless Home Automation System using Fusion of IoT and Learning over Cloud Environment," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 840-847, doi: 10.1109/ICIEM54221.2022.9853116.

[23] Jiang, Y., Wang, J., & Song, L. (2023). Quantitative analysis of cost savings and occupants' preferences in grid-interactive smart home operation. Science and Technology for the Built Environment, 29(9), 845-857. DOI: 10.1080/23744731.2023.2244337

[24] Karagianni, A., & Geropanta, V. (2019). Smart Homes: Methodology of IoT Integration in the Architectural and Interior Design Process – A Case Study in the Historical Center of Athens. In: Vasant, P., Zelinka, I., Weber, GW. (eds) Intelligent Computing and Optimization. ICO 2019. Advances in Intelligent Systems and Computing, Vol. 1072. Springer, Cham. https://doi.org/10.1007/978-3-030-33585-4_22

[25] Kaushik, K., Bhardwaj, A., & Dahiya, S. (2023). Smart Home IoT Forensics: Current Status, Challenges, and Future Directions," 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 2023, pp. 716-721, doi: 10.1109/InCACCT57535.2023.10141730.

[26] Khan, Y., Su'ud, M. B. M., Alam, M. M., Ahmad, S. F., Salim, N. A., & Khan, N. (2022). Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications. Electronics, 12(1), 88. DOI: 10.3390/electronics12010088.

[27] Khan, F., Chaturvedi, S., & Jaswal, A. (2022). Smart City Implications of the Internet of Things. Stallion Journal for Multidisciplinary Associated Research Studies, 1(1), 22-31. DOI: 10.55544/sjmars.1.1.4

[28] Kodali, R., Soratkal, S., & Boppana, L. (2016). IOT based control of appliances. International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 1293-1297, doi: 10.1109/CCAA.2016.7813918.

[29] Korkan, E., Kaebisch, S., & Steinhorst, S. (2020). Streamlining IoT system development with open standards. It-Information Technology, 62(5-6), 215-226. DOI: 10.1515/itit-2020-0016

[30] Lafontaine, E., Sabir, A., & Das, A. (2021). Understanding people's attitude and concerns towards adopting IoT devices. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, 307, pp. 1-10. https://doi.org/10.1145/3411763.3451633

[31] Lazaroiu, C., & Roscia, M. (2017). Smart District through IoT and Blockchain, 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), San Diego, CA, USA, 2017, pp. 454-461, doi: 10.1109/ICRERA.2017.8191102.

[32] Lu, C.H. (2018). IoT-Enabled Adaptive Context-Aware and Playful Cyber-Physical System for Everyday Energy Savings," in IEEE Transactions on Human-Machine Systems, vol. 48, no. 4, pp. 380-391, Aug. 2018, doi: 10.1109/THMS.2018.2844119.

[33] Lynggaard, P., & Skouby, K. E. (2016). Complex IoT systems as enablers for smart homes in a smart city vision. Sensors, 16(11), 1840. DOI: 10.3390/s16111840

[34] Mahamud, M. S., Zishan, M. S. R., Ahmad, S. I., Rahman, A. R., Hasan, M. M., & Rahman, M. L. (2019). Domicile - An IoT Based Smart Home Automation System," 2019 International Conference on Robotics,Electrical and Signal Processing Techniques, Dhaka, Bangladesh, 2019, pp. 493-497, doi: 10.1109/ICREST.2019.8644349.

[35] Mainetti, L., Mighali, V., & Patrono, L. (2015). An IoT-based user-centric ecosystem for heterogeneous Smart Home environments," 2015 IEEE International Conference on Communications (ICC), London, UK, 2015, pp. 704-709, doi: 10.1109/ICC.2015.7248404. DOI: 10.1109/ICC.2015.7248404.

[36] Mazhar, M., & Shafiq, Z. (2020). Characterizing Smart Home IoT Traffic in the Wild," 2020 IEEE/ACM Fifth International Conference on Internet-of-Things Design and Implementation (IoTDI), Sydney, NSW, Australia, 2020, pp. 203-215, doi: 10.1109/IoTDI49375.2020.00027.

[37] Nolich, M., Spoladore, D., Carciotti, S., Buqi, R., & Sacco, M. (2019). Cabin as a home: a novel comfort optimization framework for IoT equipped smart environments and applications on cruise ships. Sensors, 19(5), 1060. DOI: 10.3390/s19051060

[38] Oprea, M. (2021). Integration of Artificial Intelligence in STEM Education through IoT Projects Based on Machine Learning. Conference Proceedings of eLearning and Software for Education, 2, 211-221. DOI: 10.12753/2066-026x-21-096

[39] Plachkinova, M., Vo, A., & Alluhaidan, A. (2016). Emerging Trends in Smart Home Security, Privacy, and Digital Forensics. Twenty-second Americas Conference on Information Systems, San Diego, pp. 1-9. https://www.justice.gov/usao-cdca/file/825001/download.

[40] Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P. C., & Liao, Y. (2019). Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. Surveillance & Society, 17(1/2), 125-131. https://doi.org/10.24908/ss.v17i1/2.12936.

[41] Priyashan, W. M., & Thilakarathne, N. N. (2020). IIoT framework for sme level injection molding industry in the context of industry 4.0. International Journal of Engineering and Management Research, 10(6), 61-68. DOI: 10.31033/ijemr.10.6.9.

[42] Saleem, A. A., Hassan, M. M., & Ali, I. (2022). Smart Homes Powered by Machine Learning: A Review," 2022 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Iraq, 2022, pp. 355-361, doi: 10.1109/CSASE51777.2022.9759682.

[43] Shehab, A. H., & Al-Janabi, S. T. F. (2020). Microsoft Azure IoT-based Edge Computing for Smart Homes," 2020 International Conference on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, 2020, pp. 315-319, doi: 10.1109/DASA51403.2020.9317274.

[44] Sripriyanka, G., & Mahendran, A. (2022). Issues and Solution Techniques for IoT Security Privacy-A Survey. International Journal of Computing and Digital Systems, 12(1), 909-928. DOI: 10.12785/ijcds/120175

[45] Srivastava, S., & Prakash, S. (2020). Security Enhancement of IoT Based Smart Home Using Hybrid Technique. In: Bhattacharjee, A., Borgohain, S., Soni, B., Verma, G., Gao, XZ. (eds) Machine Learning, Image Processing, Network Security and Data Sciences. MIND 2020. Communications in Computer and Information Science, vol. 1241. Springer, Singapore. https://doi.org/10.1007/978-981-15-6318-8_44.

[46] Sudhakar, K. N., Devadarshini, P. T., Ramu, K. N., Deshveer, Suryanarayana, N. V. S., & Kanakala, V. R. (2023). IoT-based Smart Home Automation Systems for Energy Conservation," 2023 7th International Conference on I-SMAC

(IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 12-16, doi: 10.1109/I-SMAC58438.2023.10290633.

[47] Vallati, C., Virdis, A., Mingozzi, E., & Stea, G. (2016). Mobile-edge computing come home connecting things in future smart homes using LTE device-to-device communications. IEEE Consumer Electronics Magazine, 5(4), 77-83. DOI: 10.1109/MCE.2016.2590100

[48] Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. (2017). Internet of Things (IoT): A vision, architectural elements, and security issues," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 492-496, doi: 10.1109/I-SMAC.2017.8058399.

[49] Venkatraman, S., Overmars, A., & Thong, M. (2021). Smart home automation—use cases of a secure and integrated voice-control system. Systems, 9(4), 77. DOI: 10.3390/systems9040077

[50] Wang, L., Xu, X., Gao, R., & Nee, A. Y. (2019). Sustainable cybernetic manufacturing. International Journal of Production Research, 57(12), 3799-3801. DOI: 10.1080/00207543.2019.1598153.

[51] Waseem, Q., Wan Din, W. I. S., Abdul Rahman, A., & Nisar, K. (2023). Exploring Machine Learning in IoT Smart Home Automation," 2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS), Penang, Malaysia, 2023, pp. 252-257, doi: 10.1109/ICSECS58457.2023.10256283.

[52] Yao, L., Sheng, Q. Z., Benatallah, B., Dustdar, S., Wang, X., Shemshadi, A., & Kanhere, S. S. (2018). WITS: an IoT-endowed computational framework for activity recognition in personalized smart homes. Computing, 100, 369-385. DOI: 10.1007/s00607-018-0603-z

[53] Yang, H., Lee, W., & Lee, H. (2018). IoT Smart Home Adoption: The Importance of Proper Level Automation", Journal of Sensors, Vol. 2018, Article ID 6464036, 1-11, https://doi.org/10.1155/2018/6464036

[54] Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. Sensors, 21(14), 4932. DOI: 10.3390/s21144932

[55] Zielonka, A., Woźniak, M., Garg, S., Kaddoum, G., Piran, M. J., & Muhammad, G. (2021). Smart Homes: How much will they support us? A Research on Recent Trends and Advances," in IEEE Access, vol. 9, pp. 26388-26419, 2021, doi: 10.1109/ACCESS.2021.3054575.