Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 18 No. 21 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijim.v18i21.50217

PAPER

A Proposed Perspective for the Successful Deployment of Internet of Things in a Smart Home Environment

Galal Eldin Abbas Eltayeb(✉)

Department of Management Information Systems, College of Business and Economics, Qassim University, Buraydah, Saudi Arabia

g.eltayeb@qu.edu.sa

ABSTRACT

The Internet of Things (IoT) technology is used in smart homes to enhance comfort, security, and energy efficiency. This study outlines a theoretical framework for the deployment and dissemination of IoT technologies in intelligent residential environments. The framework of this study highlights the significance of many components that cater to people's individual needs. The study offers a systematic explanation of IoT principles, tangible devices, services, data creation, software, applications, and logistical needs. Furthermore, it contains an extensive table that assists users in choosing the most appropriate resources and components. The study points to smart home systems based on IoT, which utilize sensors, controllers, and cloud solutions to manage data and provide user control while ensuring privacy and confidentiality. The study addresses various needs of users by utilizing a semantic vision framework for smart house design that guarantees economic advantages, enhanced security, and user contentment, ultimately leading to enhanced community interactions and the overall welfare of residents.

KEYWORDS

Internet of Things (IoT), smart home, information technology, data analysis, networking, security

1 INTRODUCTION

The proposed perspective can lead to the successful deployment of the Internet of Things (IoT) in a smart home environment (SHE). This view encompasses several steps, including grouping IoT devices according to their hardware, identifying and preventing their use, and exploring their potential applications in a SHE. It also addresses security concerns by providing security level certificates (SLC), creating a communication plan, and connecting each other or connecting secure responses to legacy systems [1]. Additionally, proper network architecture and standard protocols should be used to connect devices to the internet, thereby ensuring the security of NetWare software [2]. Overall, because the successive deployment of IoT in a

Eltayeb, G.E.A. (2024). A Proposed Perspective for the Successful Deployment of Internet of Things in a Smart Home Environment. *International Journal of Interactive Mobile Technologies (iJIM)*, 18(21), pp. 117–133. https://doi.org/10.3991/ijim.v18i21.50217

Article submitted 2024-05-21. Revision uploaded 2024-08-24. Final acceptance 2024-08-26.

SHE typically follows a structured approach to ensure smooth integration and functionality, the proposed view aims to enhance the quality of life of users by providing a secure and convenient IoT-based smart-home system [3]. The proposed view emphasizes the importance of data privacy and security measures for IoT devices.

2 ENVIRONMENT OVERVIEW

2.1 Objectives

The integration of the IoT into a smart home aim to achieve multiple significant objectives, such as augmenting the convenience of device control via remote access, elevating energy efficiency via automation, fortifying security via intelligent monitoring systems, and furnishing enhanced insights into home usage patterns for optimization of the IoT into a smart home. By integrating IoT technology into a house, the goal is to improve the daily living conditions in terms of comfort, safety, and cost. As a variety of smart devices are used that generate or read different types of data, it is essential to investigate the complex relationship between smart devices and the data they gather, comprehend data management in a SHE, and understand its importance in improving the functionality of these systems.

2.2 Internet of Things smart home devices

To achieve the objectives of designing and furnishing a smart home, equipment, devices, connections, and software make it possible to do so. The following categories of devices need to be assigned to perform functions, to exercise remote control, and even to monitor the home in general:

- Thermal devices such as air conditioners have thermostats that regulate the temperature within buildings based on user preferences and behavioral patterns and allow users to adjust the temperature of their homes to a comfortable level.
- Lighting devices control remote or mechanical lighting systems to operate, stop, or modify brightness and color.
- Security cameras use motion sensors and real-time monitoring capabilities to enhance home security.
- Door locks allow users to lock and open their doors via smartphones. Doorbells and smart alarms enable users to view and contact visitors remotely.
- Smart appliances control kitchen equipment such as refrigerators, ovens, and dishwashers. They integrate communication features to improve efficiency, such as allowing users to start operating or preventing them from using their smartphones.
- Biometric detectors identify and analyze biometric data, including fingerprints, facial features, iris patterns, voiceprints, eye measurements, health and wellness indicators, and behavioral factors such as gait or typing habits.
- Smart speakers act as central voice commands to control other intelligent household appliances.
- Power management devices assist users in monitoring and managing the use of electricity or solar energy in their homes, controlling consumption, providing insights into reducing energy waste, and lowering service bills.

- Smart USB ports control, operate, and extinguish household energy systems and continuous supply capacities such as uninterrupted power (USB) and follow-up on consumption.
- Water coolers and heaters can remotely change water temperature in terms of heat or cold.
- Emergency response devices integrate systems to provide quick access to emergency assistance, such as fire stations, police, and hospitals, contacting them when needed.
- Voice-activated assistants such as Amazon Echo (Alexa), Google Home (Google Assistant), and Apple HomePod (Siri) allow users to control smart home devices using voice commands.
- Smart blinds and curtains are motorized and can be controlled remotely or scheduled to open and close based on preferences or external factors, such as sunlight.
- The services for the elderly and disabled include providing and installing devices and accessibility tools for easy access to different parts of the home and integrating health-monitoring devices according to their needs.

3 DATA DIVERSITY

Undoubtedly, the wide variety of devices and equipment required for establishing and furnishing a smart home generates copious amounts of data, necessitating the implementation of specialized software to manage them. The diverse types of software and apps and their unique processing and interaction methods are presented in Table 1.

Table 1. Smart home devices and their function and data prediction

Use	Devices	Function	Nature of Data	Example
Entertainment	TV, Radio, Players, reminders	Voice-control	Multimedia (Text, audio, image, file transfer, Sensor Data)	Amazon Alexa and Google Assistant
Home Kits	Phone, Smartphone, Alarm	Mobile control	Bluetooth, Bluetooth RS232 data	Apple HomeKit
Thermostat	Air conditioners, water temperature and BLE Devices, Thermometers, Heaters and coolers	Adjusting the entire temperature	Multimedia, Temperature Sensor energy consumption readers	Nest Thermostat
Lighting	Switches, Bulbs	control lighting color, brightness, and schedules.	Multimedia, Bluetooth	Philips Hue
Cameras	motion detector, night vision camera, and two-way audio camera	monitoring indoor and outdoor spaces	Video footage, motion events, camera status	Arlo and Wyze Cameras
Door	Doorbell, alarm, smart lock	Open and Close doors or move up and down or Secure the door with a password	Multimedia, Bluetooth	Android App BLE Devices, Danalock Bluetooth
Emergency	Phone, Smartphone, Alarm	Detect fire, Detect gas spreading	Arduino Board	switches or sensors
Electric powers	Switch-on/Off, counters, consumption readers	Switching on/Off	Temperature Sensor	switches or sensors
Biometric	Finger-printer, eye captures, human reactions readers	Controlling and passing security gates	WiFi Devices	Multimedia
Appliances	Refrigerators, ovens and dishwashers	Switching on/Off	BLE Devices	switches or sensors

4 DATA MANIPULATION

Data manipulation involves altering or transforming data to achieve a desired outcome or objective. With the "rush of data," which typically refers to the massive amount of data generated and processed within smart home systems, data management in smart homes entails the collection, analysis, and utilization of information generated by various devices and sensors to improve living conditions, improve energy efficiency, and provide residents with convenience and security.

Smart home systems, which generate and utilize large amounts of data for various purposes, rely heavily on data manipulation techniques. The essential data-processing duties used in smart homes are as follows:

- Smart home devices collect data from sensors, user interactions, and external sources such as weather forecasts. These data include temperature, humidity, energy consumption, and occupancy information.
- The collected data is stored in databases or cloud platforms. To store and manage data efficiently, techniques are used such as database management systems (DBMS), data lakes, and cloud storage.
- Data cleaning involves identifying and rectifying mistakes, anomalies, and missing values in raw data. To ensure the correctness and consistency of the data, data cleaning procedures are utilized, including filtering, normalization, and imputation.
- Smart homes combine data from multiple sources to gain comprehensive insights. Data integration techniques include data fusion, warehousing, and API integration with third-party services.
- Aggregating data allows for summarization and analysis at different levels of granularity. Techniques such as averaging, summing, and counting are used to aggregate the data for reporting and visualization.
- Data analysis involves applying analytical tools, such as statistical analysis, machine learning (ML), and data mining, to identify significant patterns, trends, and correlations in smart home data. This study facilitates comprehension of user behavior, enhances energy utilization optimization, and enhances automation.
- Some smart home applications require real-time data processing for immediate action or decision-making. Stream processing techniques, event processing, and real-time analytics enable rapid responses to changing conditions in a smart home environment.
- Data processing in smart homes must prioritize security and privacy. Data encryption, access control, and anonymization protect sensitive information and ensure compliance with privacy regulations.

To address these concerns, one study focuses on the practices and ethical considerations of data collection, which are critical in smart homes because of the sensitive nature of personal data [4]. Also, Weilu proposed an innovative blockchain architecture with a hierarchical proof of work (PoW) mechanism, which is used in this work as a reference for data security considerations [5]. Another study [6] proposed a new framework for enhancing data gathering from wireless sensor networks. This study employed an uncrewed aerial vehicle (UAV) and ground vehicle with additional batteries. The objective was to optimize the duration of the data collection mission. González presented a compelling case for the effectiveness of data augmentation in improving the accuracy of classification algorithms [7]. This facilitated the understanding of how to use advanced analytical techniques to look at smart home data by examining how well convolutional neural networks (CNNs) worked with data augmentation techniques. Another study looked at the risks of road accidents for vehicles according to the computer vision object study and analysis [19].

There are several techniques available to manipulate the generated data, such as:

- Machine learning uses algorithms that learn and adapt to user preferences and behavioral patterns.
- Data analytics analyze data to derive insights into energy optimization, security enhancements, and user comfort.
- Voice processing interprets voice commands to ensure seamless interaction with smart home devices.
- Automation scripts are predefined to automate routine tasks and responses.
- Cloud computing stores and processes data on remote servers for scalability and accessibility.

5 RAPID GROWTH

The rapid growth of smart home technologies can be attributed to technological advancements, increased consumer demand for convenience and efficiency, and a broader adoption of connected devices. Technological advancements encompass several cutting-edge developments such as IoT, artificial intelligence (AI), ML, speech recognition, and natural language processing. Consumer demand has risen due to convenience, efficiency, energy savings, security, and safety. The increased use of connected devices is driven by compatibility, interoperability, affordability, accessibility, and integration with existing ecosystems. Market growth and economic drivers encompass investment, innovation, marketing, consumer education, and worldwide expansion. The COVID-19 pandemic has also impacted the expansion of smart home devices owing to the increased time spent at home and the surge in remote work and automation. Standard smart home technologies include smart speakers, thermostats, lighting fixtures, security systems, and household appliances. Upcoming developments encompass improved AI capabilities, more integration, the adoption of 5G connections, and a heightened emphasis on sustainability. The smart home market is expected to sustain its growth owing to technical improvements, consumer preferences, and market dynamics.

In 2020, the worldwide smart home market had a value of approximately $79.12 billion; this is expected to reach $313.95 billion by 2026 [8]. The Asia-Pacific region has witnessed the most rapid expansion, while North America has maintained its position as the largest market globally. Technological innovations, including integrating IoT, AI, and 5G connections, are crucial in driving market expansion. Consumer demand is driven by convenience, efficiency, energy management, and security. Economic aspects encompass affordability, investment, and innovation [9]. Standard smart home devices include smart speakers and assistants, smart security systems, smart lighting, climate controls, and smart appliances. Market trends include incorporation, compatibility, improved user satisfaction, and long-term viability. Problems and considerations encompass privacy, security, and market fragmentation. Prospects entail expanding in developing economies, utilizing cutting-edge technologies, and incorporating health and wellness [10].

The smart home market is not just growing; it is evolving rapidly, driven by advancements in technology, consumer demand, and investment. The future looks promising with continuous innovation and expansion into new markets, although challenges such as privacy and compatibility need to be addressed. IoT, a game-changer, is reshaping our daily lives, and effective data management strategies are crucial in this ecosystem. Real-time data processing and decision-making are vital for smart homes, and the market is expected to continue to grow, making IoT devices an integral part of households worldwide.

Moreover, the ability to process data in real time and make immediate decisions is not just a feature but a necessity for smart homes. Therefore, studies often focus on post hoc analysis rather than real-time interventions, highlighting the importance of this aspect in the smart home market.

Some popular brands of smart home productivity tools and applications (ordered alphabetically) [6, 7] are presented in Figure 1 [11, 12]:

- Alexa is Amazon's virtual assistant that powers various smart devices, such as echo speakers and shadow screens. Through voice commands, it can control smart home devices, answer questions, play music, set reminders, etc.
- Apple HomeKit is Apple's ecosystem for smart home devices, which allows users to control compatible products, such as lights, locks, and thermostats, using Siri voice commands or a home application on iOS devices.
- Arlo specializes in wireless security cameras with features such as HD video recording, motion detection, and night vision. The Arlo app enables remote access to and control of cameras.
- August Smart Lock specializes in smart locks that enable keyless entry, remote access, and integration with other smart home systems for enhanced security and convenience.
- Danalock offers Bluetooth-operated smart locks. Their services include keyless entry, remote access, and integration with smart home platforms to boost security.
- Known for their smart thermostats, Eco bee provides remote-controllable energy-efficient solutions that integrate voice assistants, such as Alexa and Google Assistant.
- Eufy provides smart home devices such as security cameras, robot vacuums, and smart bulbs. They focused on simplicity, affordability, and user-friendliness.
- Google Assistant is Google's virtual assistant available on various devices, such as smartphones, smart speakers, and smart displays. It can control smart home devices, answer questions, provide weather updates, etc.
- Known for its Nest thermostats, cameras, and smart speakers, Google Nest offers a range of products that enhance home productivity through automation and voice control.
- While not a brand, If This Then That (IFTTT) is a platform that allows users to create custom automation rules (applets) to connect and control various smart home devices and services.
- Kangaroo offers affordable home security solutions, including motion sensors, door/window sensors, and security cameras. Kangaroo products are designed for easy set-up and DIY installation.
- LG Smart TV has built-in Wi-Fi connectivity and support for streaming applications such as Netflix, Hulu, and Amazon Prime Video. Smart home systems can integrate voice control and automation.
- Philips Hue is a well-known smart lighting solution. The Philips Hue app and platforms such as Alexa and Google Assistant enable remote control of their products, which include smart bulbs, light strips, and accessories.
- Ring is popular because its video doorbells and security cameras provide real-time monitoring and alerts, enhancing home security and convenience.
- Samsung SmartThings is a platform that integrates various smart home devices, such as lights, sensors, and cameras, enabling users to create automated routines and control their home environment using a single app.

- Vivint provides professionally installed smart home systems, including security cameras, smart locks, and thermostats. The Vivint app allows remote control of their systems and provides 24/7 monitoring.
- Wemo provides a variety of smart plugs, switches, and light controllers that allow remote control and integration with voice assistants for hands-free operation.
- Wyze offers affordable smart home products, including security cameras, smart bulbs, plugs, and sensors. They focus on affordability without compromising features such as HD video recording and smartphone integration.

Fig. 1. Some popular brands of smart home productivity tools and smart home applications

6 SECURITY CONSIDERATIONS

Smart home security is crucial because devices are interconnected and handle sensitive data. Key security considerations include data privacy, device and network security, access control, vulnerability management, physical security, incident response, user education, regulatory compliance, and awareness of emerging threats.

Personal data security is essential because smart home devices collect vast amounts of data, such as usage patterns, preferences, and video and audio recordings. Encryption techniques such as Secure Sockets Layer/Transport Layer Security (SSL/TLS) are essential for securing data transmission. Data minimization involves collecting only the necessary data and avoiding storing sensitive information longer than required.

Device and network security are crucial, including secure network configurations, robust authentication mechanisms, firmware and software updates, user-access management, and remote access. Regular security audits and vulnerability assessments are necessary to identify and mitigate potential risks. Third-party integration should be evaluated to ensure that it adheres to strict security standards.

Physical security involves placing devices in secure locations, implementing tamper-detection mechanisms, and establishing continuous monitoring and real-time alerts for unusual activities or potential security breaches. An apparent incident response plan should be developed to quickly address and mitigate the impact of security incidents.

User education and awareness are also important, as is education about security practices such as creating strong passwords, recognizing phishing attempts, and regularly updating devices. User manuals and support should be provided for security settings and best practices.

Regulatory compliance is essential, as smart home devices comply with relevant data protection and privacy regulations. Industry standards such as ISO/IEC 27001 should also be followed. Emerging threats such as botnets and DDoS attacks must be addressed to protect devices and networks from hijacking.

Alheeti paper proposes a deep learning-based detection system for IoT devices to secure sensitive information. The system, tested on normal and fuzzification datasets, achieved an accuracy rate of 99.30% and 99.42% respectively, demonstrating its robustness, reliability, and efficiency in providing a secure environment for IoT devices [20].

Therefore, the following security methods and tools are required:

6.1 Encryption methods

- Communication protocols use advanced encryption standard (AES).
- Device-level encryption is provided for cameras, door locks, and sensors.
- End-to-end encryption (E2EE) aims to secure data transmission from one endpoint to another.
- Secure Shell Protocol (SSH) is used for secure remote access to devices.
- Transport Layer Security is used to secure communication over networks.
- Virtual private network (VPN) is a secure and encrypted connection between a smart home network and an external server.

6.2 Authentication methods

- Password-based authentication utilizes a combination of a username and a password.
- Biometric authentication allows secure login and data access by fingerprints, facial, or voice recognition [21].
- Token-based authentication involves using a smart card, a Radio Frequency Identification (RFID) tag, a Near Field Communication (NFC)-enabled device, and a one-time passcode.
- Certificate-based authentication uses trusted digital certificates.

- Open authorization (OAuth) grants secure access to third-party applications.
- Device pairing is a secure device pairing gateway.

6.3 Secure Wi-Fi

- It is essential to change the service set identifier (SSID) network name and password periodically.
- Wi-Fi service should enable Wi-Fi Protected Access 3 (WPA3) or WPA2 [18].
- Use virtual local area networks (VLANs) or network segmentation.
- Update the Wi-Fi router's firmware periodically.
- Enable MAC address filtering.

7 DELICATE BALANCE

Before improving smart home operations, protecting user privacy and keeping data functional must be balanced because privacy and security have become essential in smart home data ecosystems. There are many possible weaknesses and ways to lower the risks associated with smart home operations, in addition to the known control mechanisms. Rahim explored intelligent approaches that further enrich the domain of smart-home IoT security. LogitBoost techniques were studied to create multiclass classification models that distinguish between normal and abnormal network traffic, an essential skill for keeping smart home data safe and private [8]. Puri's work from 2022 on AI-based botnet attack classification and detection in IoT devices also provided a complete plan for using ML and deep learning models to protect against complex cyber threats [9].

8 METHODS

In implementing a smart home system, it is crucial to establish the aims and objectives, evaluate the current infrastructure, and select the proper IoT devices. Actuators and sensors can categorize these wired or wireless devices. These devices' hardware configuration, testing, and optimization depend on the system's compatibility with the existing infrastructure, ease of integration, security measures, and potential for scaling. Mobile devices are essential for controlling, monitoring, and managing smart homes; they offer remote control, voice control, and monitoring. Integration with virtual assistants and AI algorithms can enhance security. Security considerations include robust authentication methods, encryption, regular updates, and secure network configurations. Future trends in mobile integration include AI integration, personalized automation experiences, predictive maintenance, and blockchain technology. Integration and automation of smart home devices have improved significantly in recent years, offering functionalities such as remote access, security measures, and real-time meteorological updates.

8.1 Implications

To choose and operationalize smart home services at this point, the aims and objectives of IoT system implementation in a home must first be established. Subsequently, the current infrastructure must be evaluated, including the hardware and networks already in place and linkage options. A dissemination strategy plan must be created that considers the needs, timeline, and budget.

8.2 Selection of Internet of Things devices

Choose IoT devices that align with goals and criteria. Typically, a wired or wireless network interconnects multiple devices throughout the house to form a smart-house system. At a node, a computer system acts as a server that controls all information flows within the network. The server system requires a middleware device manager [10] to facilitate the connection of the primary application to various device controllers through a single or minimal number of interfaces. The devices in this home can include three distinct groups:

1. Actuator devices include alarms, lights, windows, and doors.
2. Sensor devices can detect heat, gas, movement, and health care data. Robots and air conditioners are examples of actuators and sensors, respectively.
3. The IoT enables connectivity between several devices, as shown in Figure 2 [13].

Both the sensors and actuators can communicate their states through their controllers. They can communicate whether they are on or off and the specific tasks they are currently performing, such as closing a door. Consider elements such as the system's compatibility with the current infrastructure, ease of integration, security measures it provides, and potential to scale.

INTERNET OF THING
Ai
VR

Fig. 2. The Internet of Things enables connectivity between several devices

8.3 Hardware configuration

Internet of Things devices are installed and configured according to the manufacturer's guidelines to configure each device, including connecting them to the home network, setting up user accounts, and adjusting settings according to preferences.

The disadvantage of wireless systems is that they require strong Wi-Fi coverage and broadband services in their homes. Also, this may require investment in band extenders or wireless access points. Their small size makes wireless smart home systems generally more suitable for smaller homes or rental properties. However, solid wire systems are more reliable and are usually more difficult to penetrate. A tangible system can increase the value of the home. In addition, wired smart home systems are easily expandable, making them the default method for designing new buildings or conducting significant renovations. However, there is a flaw in that it is relatively expensive. Installing a luxurious smart system with hardware can cost homeowners tens of thousands of dollars. In addition, there should be space for network hardware equipment, including Ethernet cables. Ensure the home network is robust and secure for handling the IoT devices. Use strong passwords and encryption protocols (such as WPA2/WPA3), and update firmware regularly. A dedicated IoT network can be installed to separate IoT devices from critical systems for added security.

8.4 Mobile device uses in smart home

Mobile devices are essential in smart home systems and are central hubs for control, monitoring, and management. They enable various functions, including remote control, voice control, monitoring, and surveillance. Mobile apps allow users to remotely control devices, adjust their settings, and lock doors. Integration with virtual assistants such as Google Assistant, Amazon Alexa, and Apple Siri enables voice control. Users can monitor their homes using live feeds from security, doorbells, and baby monitors. Notifications and alerts inform users about motion detection and door/window openings. Mobile apps also facilitate automation and scheduling, allowing users to create custom settings and set schedules for specific actions.

Several popular mobile apps for smart-home control include SmartThings, Google Home, Apple Home Kit, Amazon Alexa, and Philips Hue. They offer different features such as device compatibility, automation routines, voice control, and lighting control. Mobile integration enables advanced features such as geofencing, which triggers actions based on the user's location, and enhanced security. AI and ML algorithms in mobile apps can proactively learn user preferences and adjust settings, improving energy management and automation. Mobile apps also track energy usage and allow remote adjustments to save energy.

Security considerations in smart home systems include implementing robust authentication methods, encrypting data transmissions, regularly updating devices and mobile apps, and using secure network configurations.

Future trends in mobile integration with smart homes include enhanced AI integration, personalized and intuitive automation experiences, and predictive maintenance. Augmented reality (AR) can assist with device setup and control, providing a visual and interactive method for managing the home environment. Blockchain technology can enhance security by providing decentralized and secure authentication methods.

8.5 Integration and automation

The integration and automation of smart home devices has substantially improved in recent years. Numerous studies have emphasized incorporating technologies such as IoT, Raspberry Pi, Arduino, and mobile applications to develop effective smart home systems. These systems provide functionalities such as remote access, security measures, light management, gas leak detection, intrusion detection, real-time meteorological updates, music players, and image browsers. Utilizing Wi-Fi, RF modems, and open-source platforms such as Blynk facilitates smooth communication between users and devices, thereby enhancing user interaction and control over household appliances. To connect IoT devices with a central smart home hub or platform, such as Amazon Alexa, Google Home, Apple HomeKit, Bluetooth, or a specific smart home controller such as Samsung SmartThings or Hubitat Elevation, it may be necessary at times to establish intermediary controllers or develop automation routines and settings for the purpose of streamlining operations and enhancing efficiency.

8.6 Testing and optimization

Testing and optimizing smart home devices is crucial for ensuring functionality, security, and efficiency. Optimize settings and configurations based on user feedback and performance observations. Testing and optimizing smart home devices involves several key steps and considerations.

- Functionality testing: Ensure that the device correctly performs its intended function. For example, a smart thermostat should accurately control the temperature according to user settings.
- Compatibility testing: Test the device's compatibility with other smart home products and platforms. The device should integrate and communicate seamlessly with other devices in the ecosystem.
- Security testing: Assess the device's security features to protect against unauthorized access and data breaches. These include encryption protocols, authentication mechanisms, and software vulnerabilities.
- Usability testing: Evaluate the device's user interface and the overall user experience. The device should be easy to use and should provide users with clear feedback.
- Performance testing: Test the performance metrics of the device, such as response time, power consumption, and reliability under different usage scenarios.
- Optimization: Based on the test results, areas for improvement and optimization of the device firmware or software could involve bug fixes, performance enhancements, or adding new features.
- Field testing: Conduct real-world testing in various environments to validate the device's performance and reliability.
- Feedback loop: Collect and incorporate user feedback into the optimization process to address user concerns and improve the overall product experience.

Various studies have addressed different aspects of testing and optimizing smart home devices. One study proposed a swarm-based cyber-security penetration testing method for IoT networks to enhance their security [14].

8.7 User observations

In the context of smart homes, user observations involve examining the operation and use of such systems in real-world settings. Researchers and professionals can conduct user observations to gather data, understand user behavior, assess system performance, and identify challenges and opportunities for improvement. Some aspects typically observed in smart home field studies are as follows [15]:

- Observing how users interact with smart home devices and systems, including their usage patterns, preferences, and challenges encountered during operation.
- Evaluating the effectiveness of automated processes within a smart home, such as energy-saving features, security protocols, and home automation routines.
- Evaluating the usability of smart home interfaces, apps, and control mechanisms and the overall user experience when managing and interacting with connected devices.
- Monitoring environmental factors such as temperature, humidity, light levels, and air quality to understand their impact on smart home operations and user comfort.
- Measuring energy consumption patterns within a smart home to identify areas for energy optimization and efficiency improvements.
- Observing security measures in place and privacy concerns related to smart home devices, data collection, and remote access.
- Examining issues related to device maintenance, troubleshooting, software updates, and user support services.
- User observations often involve qualitative data collection methods such as interviews, surveys, participant observations, and ethnographic studies. The insights gained from these observations can inform the design, development, and deployment of smart home technologies to better meet user needs and enhance the overall system performance.

Singh conducted a study to understand user perceptions and attitudes toward smart home technologies [22]. They found that 55.1% of users were familiar with smart home technologies, and they used smartphones (94.4%), smart TVs (57.7%), and tablets (59.8%) across various locations in Asia (N = 100), Europe (N = 101), America (N = 27), Australia (N = 4), and Africa (N = 22).

8.8 Measurable objectives

In implementing the IoT system in a smart home, it is essential to set specific and measurable targets to ensure the project's success and track progress. As stated, the objectives of each component or device need to be defined. To ensure that these units operate within the acceptable targets, there must be limits and scales in terms of their appropriateness or acceptance.

1. To measure energy efficiency and consumption, read a monthly energy bill and compare it to energy bills from before the system was implemented.
2. To enhance security and door access, monitor and record the number of access attempts discovered by the security system before and after installation.
3. To ensure the safety and smooth functioning of automated and temporary devices, track the number of automated tasks performed by the IOT system, such as lighting, irrigation, and control of devices, and ensure that these results align with expectations.

So, for each device or system, there is a need for standards that define behavior or acceptable rates.

9 IMPLEMENTATION EVALUATION

The success of IoT implementation in a smart home involves evaluating technical performance, user satisfaction, cost efficiency, and the overall impact on quality of life. A structured process involves defining objectives and metrics, conducting pre-implementation benchmarking, monitoring implementation progress, collecting data, analyzing performance, assessing user satisfaction, and comparing against benchmarks. Continuous improvement is essential, including regular updates, user training, and feedback loops. Reporting and documentation are crucial, including sharing findings with stakeholders. Long-term monitoring ensures the system remains effective and efficient and adapts to new technologies. This structured approach ensures a thorough evaluation of the IoT implementation in a smart home, focusing on technical performance and user satisfaction. This leads to continuous improvement and optimization. These steps are shown in Figure 3.

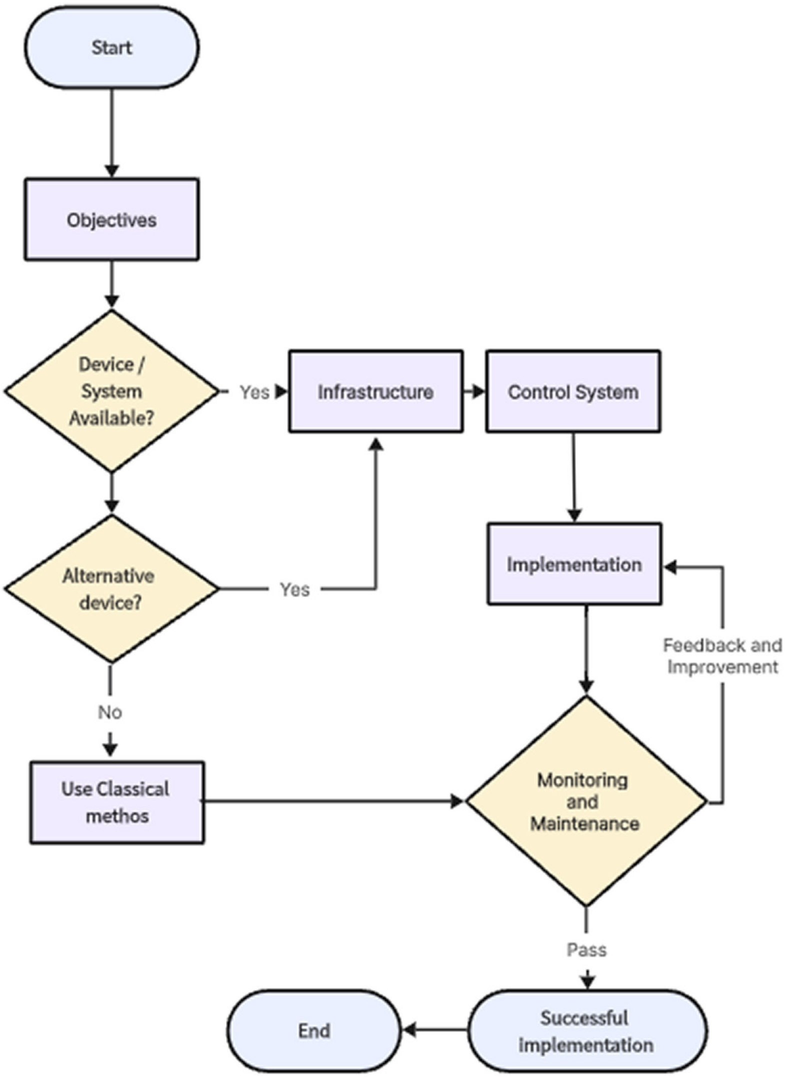

Fig. 3. A flowchart showing the step-by-step implementation process of IoT in a smart home

10 RISK MANAGEMENT

To mitigate the various risks associated with IoT in smart homes, a comprehensive plan incorporating encryption method, firmware updates, strong passwords, double authentication, maintenance schedules, and troubleshooting protocols is essential [13]. Implementing security measures such as the AES algorithm, RSA-based methods, and MQTT protocol can enhance data protection and secure data transfer within smart home IoT devices [16]. Additionally, utilizing Wi-Fi-enabled smart home automation systems driven by Wi-Fi connectivity can offer increased security through integrated sensors, cameras, and motion detectors, enhancing home safety and mitigating risks associated with intruders or hazards [17]. Furthermore, employing authentication mechanisms such as username and password verification, as proposed in the research, can prevent unauthorized access and usage of smart home appliances, ensuring data privacy and security [16]. By integrating these strategies, homeowners can safeguard their smart homes against security breaches, privacy concerns, and other potential risks, ensuring a safe and reliable IoT environment.

11 CONCLUSION

This paper discusses the need for a semantic vision or a drafted framework for the application and dissemination of IoT for smart homes. We provide a step-by-step description of IoT deployment's concepts, requirements, and procedures in a SHE. Smart homes are promising applications of ubiquitous computing that combine sensors, multimedia devices, communication protocols, and systems to provide context-aware services and remote home control. This study includes classifying IoT devices based on their hardware capabilities, the detection and prevention of IoT devices for work, and their applications in SHE. Furthermore, security concerns are addressed by assigning SLC to IoT devices, developing a communication plan, and integrating it with legacy systems. The proposed view aims to enhance users' quality of life by providing a secure and convenient IoT-based smart home system. The addition of the IoT aims to achieve several important goals, including making things easier to control, saving energy through automation, making things safer with smart monitoring systems, and providing people with better information about how they use their homes to make them more efficient. To achieve these objectives, many pieces of equipment, devices, and software fall into the following categories: thermal devices, lighting devices, security cameras, door locks, doorbells, and smart alarms. This study also investigates the complex relationship between smart devices and the data they gather and the importance of improving the functionality of these systems.

12 FUTURE WORK

The future of smart homes is expected to be characterized by advancements in technology, including the integration of AI and ML, voice and gesture control advancements, interoperability and standardization, enhanced security and privacy measures, energy efficiency and sustainability, AR and virtual reality experiences, health and wellness integration, smart city integration, 3D printing and customization, data analytics and insights, and robotics and automation.

AI algorithms learn user behavior patterns to anticipate needs and automate tasks more intelligently, such as adjusting lighting and temperature based on user preferences without manual input. Contextual awareness can also be achieved through AI-powered systems, which gain context awareness and respond in a more nuanced way to environmental factors and user interactions.

Voice and gesture control will become more conversational and capable of understanding complex commands and context. Open standards reduce fragmentation and improve the compatibility between devices and ecosystems. Blockchain technology will be implemented for secure authentication, data integrity, and decentralized control of smart home systems. In contrast, privacy-focused designs will have built-in privacy features and transparent data handling practices.

Energy efficiency and sustainability can be enhanced through smart grid integration, environmental sensors, AR, virtual reality experiences, health monitoring devices, medical assistance integration, urban connectivity, 3D printing and customization, data analytics and insights, home robotics, and automation.

Smart homes will continue to evolve into sophisticated ecosystems that integrate seamlessly into our daily lives, providing comfort, efficiency, and personalized services. Future work will analyze a broader range of smart home devices to encompass various scenarios during system evaluation, as SHE can be obtained from various devices and apps.

Direct interviews with intelligent homeowners can provide valuable insight into the future of smart homes, particularly their long-term experiences with IoT devices. Recurrent observations indicate that users already have smart home devices and multiple and interconnected interfaces, as well as views and behaviors regarding the privacy and security provided by the smart home. Further research and analysis of the user experience is essential for improving the overall functionality and security of smart home devices.

13 REFERENCES

[1] H. A. Abdulghani, A. Collen, and N. A. Nijdam, "Guidance framework for developing IoT-enabled systems' cybersecurity," *Sensors*, vol. 23, no. 8, p. 4174, 2023. https://doi.org/10.3390/s23084174

[2] R. Vishal and J. Mahak, "Advancements in computer networking: A comprehensive overview of emerging technologies, protocols, and trends," *International Journal of Innovative Research in Technology and Science*, vol. 12, no. 2, pp. 416–420, 2024. https://ijirts.org/index.php/ijirts/article/view/64

[3] R. De and Sheila Maria Muniz, "Investigation of IoT-integrated smart homes," *Journal of Operational and Strategic Analytics*, vol. 1, no. 1, pp. 42–45, 2023. https://doi.org/10.56578/josa010106

[4] Tsvetelina Mladenova and Vladimir Cankov, "Smart home based on IoT – Architecture and practices," in *2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Istanbul, Turkiye, 2023, pp. 1–5. https://doi.org/10.1109/HORA58378.2023.10156739

[5] Weilu Lv, N. Wang, X. Xie, and Z. Hong, "A classification-based blockchain architecture for smart home with hierarchical PoW mechanism," *Buildings*, vol. 12, no. 9, p. 1321, 2022. https://doi.org/10.3390/buildings12091321

[6] W. J. Pitts *et al.*, "Understanding research methods, limitations, and applications of drug data collected by the National Forensic Laboratory Information System (NFLIS-Drug)," *Journal of Forensic Sciences*, vol. 68, no. 4, pp. 1335–1342, 2023. https://doi.org/10.1111/1556-4029.15269

[7] Y. Zhu and S. Wang, "Flying path optimization of rechargeable UAV for data collection in wireless sensor networks," *IEEE Sensors Letters*, vol. 7, no. 2, pp. 1–4, 2023. https://doi.org/10.1109/LSENS.2023.3237634

[8] J. L. Salazar-González, J. M. Luna-Romera, M. Carranza-García, J. A. Álvarez-García, and L. M. Soria-Morillo, "Enhancing smart home appliance recognition with wavelet and scalogram analysis using data augmentation," *Integrated Computer-Aided Engineering*, vol. 31, no. 3, pp. 307–326, 2024. https://doi.org/10.3233/ICA-230726

[9] A. S. Romanov, "Smart home technology: Automation system and industry development opportunities," *Upravlenie Kachestvom (Quality management)*, no. 4, pp. 44–47, 2023. https://doi.org/10.33920/pro-01-2304-08

[10] H. Shen, “Digital transformation of the smart home industry,” in *Lecture Notes in Electrical Engineering*, 2023, pp. 357–362. https://doi.org/10.1007/978-981-99-2092-1_45

[11] M. Ati and A. Khalid, “Smart homes in The Age of IoT,” in *IEEE International Conference on Computing (ICOCO)*, Kota Kinabalu, Malaysia, 2022, pp. 174–178. https://doi.org/10.1109/ICOCO56118.2022.10031788

[12] R. Altland, “Getting started with smart home tech: HomeKit, Amazon Alexa, SmartThings and more,” *9to5Toys*, 2017. [Online] Available at: https://9to5toys.com/2017/06/26/smart-home-getting-started/ [Accessed Aug. 23, 2024].

[13] A. Belal, “Search for smart devices,” Makhzan, 2021. [Online] Available at: https://www.m5zn.com/research-about-smart-devices/ [Accessed August 1, 2024].

[14] H. Allioui and Y. Mourdi, “Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey,” *Sensors*, vol. 23, no. 19, p. 8015, 2023. https://doi.org/10.3390/s23198015

[15] M. Hewitt and H. Cunningham, “Taxonomic classification of IoT smart home voice control,” arXiv, 2022. https://doi.org/10.48550/arxiv.2210.15656

[16] B. Farooq, “Privacy and security issues in smart homes in an IoT environment,” *Auerbach Publications eBooks*, pp. 285–303, 2024. https://doi.org/10.1201/9781003474838-16

[17] J. Rajasekhar, T. Thanusha, G. Naga Jyothi, K. Tejaswi, and Laith Abualigah, “IoT based security and privacy implementation in smart home,” *Applied and Computational Engineering*, vol. 44, pp. 202–207, 2024. https://doi.org/10.54254/2755-2721/44/20230067

[18] A. K. Jha, Akashh, and D. Imam, “Smart home automation system using IOT,” *International Journal of Scientific Research in Engineering and Management*, vol. 8, no. 5, pp. 1–5, 2024. https://doi.org/10.55041/IJSREM34993

[19] M. Q. Al-Obaidi and Nabil Derbel, “Design of IoT based remote renewable energy laboratory,” *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 12, pp. 75–87, 2023. https://doi.org/10.3991/ijet.v18i12.38659

[20] K. M. Ali Alheeti, I. Alsukayti, and M. Alreshoodi, “Intelligent botnet detection approach in modern applications,” *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 16, pp. 113–126, 2021. https://doi.org/10.3991/ijim.v15i16.24199

[21] S. Preetha and S. V. Sheela, “Multimodal biometric-based secured access mechanism for wireless sensor networks,” *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 9, pp. 86–99, 2022. https://doi.org/10.3991/ijoe.v18i09.30425

[22] D. Singh, I. Psychoula, J. Kropf, S. Hanke, and A. Holzinger, “Users’ perceptions and attitudes towards smart home technologies,” in *Smart Homes and Health Telematics, Designing a Better Future: Urban Assisted Living, ICOST 2018*, in Lecture Notes in Computer Science, M. Mokhtari, B. Abdulrazak, and H. Aloulou, Eds., Springer, Cham, vol. 10898, 2018, pp. 203–214. https://doi.org/10.1007/978-3-319-94523-1_18

14 AUTHOR

Dr. Galal Eldin Abbas Eltayeb is an Assistant Professor of information technology at the Department of Management Information Systems (MIS), College of Business and Economics (CBE), Qassim University (KSA). He graduated with a bachelor’s degree in computer science and statistics from Zagazig University, a master’s degree in computer science from Khartoum University, and a Ph.D. in information technology from Al-Neelain University. His research interests include data analysis, AI data applications, and e-learning. Since 1993, he has held numerous administrative and academic positions in higher education institutions (E-mail: g.eltayeb@qu.edu.sa; ORCID: 0000-0003-3778-2061).