A Survey on IoT in Smart Houses: A Review Paper

Carmel Nkeshimana [1,] Tumusiime Kwiringira[1], Amuki Joseph Kesi[1] and Sinde Ramadhani[2]

[1,2] The Nelson Mandela African Institution of Science and Technology, Arusha, Tanzania

Abstract.

Internet of Things technology is expected to become an essential necessity in the growth of smart homes as it provides home users with a very high level of convenience and efficiency to improve their lives. Over the last decade, we've seen improvements in low and high-power technologies, advances in wireless protocols, the practice of machine learning, the growth of cloud services, and other technological advances based on the Internet of Things, and these have heralded a new era of smart houses. This survey focuses on analyzing and reviewing top-notch papers from reputable journals and publishers that are aimed at proposing, designing, and implementing improved smart home systems that help solve known technical issues typical of smart homes. Focusing mainly on privacy, security issues, and the application of machine learning techniques/algorithms for predicting the usage behavior of these smart home occupants. We will also discuss the challenges of implementing IoT in smart home systems.

Keywords: Internet of Things, Home automation, Smart Home Systems

1 Introduction

The term "Internet of Things" or "IoT" refers to the billions of physical devices ("things") that are embedded with sensors, software, and other technologies and are connected to the internet to exchange data with other devices and systems. The "thing" in the term "Internet of Things" can be an automobile that has built-in sensors to alert a driver when the tire pressure is low, an animal with a bio-chip corresponder, a person with a heart monitor implant, or any other object that can be assigned an internet protocol (IP) address or a unique identifier and can to transfer data over a network. The phrase "Internet of Things" was first coined by Kevin Ashton the co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (M.I.T) in his presentation titled "The Internet of Things" in 1999 to describe a system where the internet is connected to the physical world via ubiquitous sensors. An IoT ecosystem comprises internet-enabled smart devices that use embedded systems and communication hardware such as sensors and processors to collect, manipulate and send data they receive from their environments. This data can be sent to the cloud or analyzed locally and these devices often communicate with other related devices and respond to information received from each other. They often do this without human intervention as they (humans) only stop at setting them up, giving them instructions, and accessing data. A smart house could be based on a platform or a smart home hub such as the amazon echo, google home, Apple’s home-kit, and Samsung SmartThings Hub to control smart devices and appliances which can include lighting, heating, air conditioning, media, security systems, camera systems, etc.

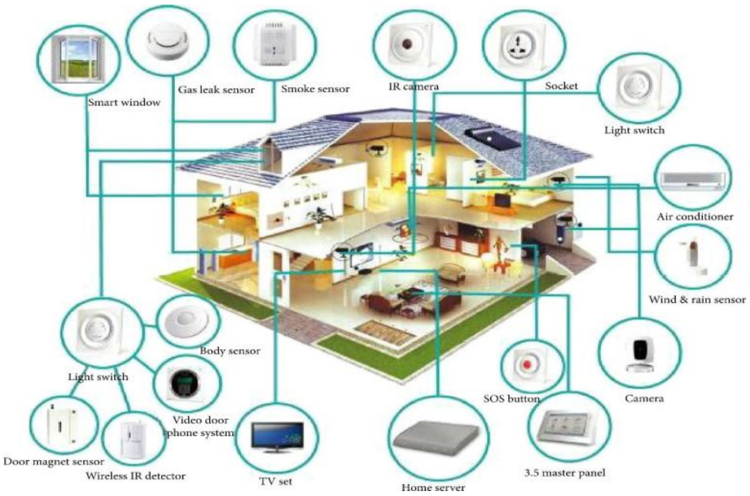

Fig 1. A typical IoT-based Smart-House - Image Source

2 Problem statement

The use of IoT technology to connect different things to the internet in smart houses brings new privacy and security concerns regarding the authenticity, integrity, and confidentiality of the data captured by different things, that are collected, and exchanged over the network. These problems make smart houses extremely susceptible to various types of security threats and attacks, making IoT-based smart houses insecure, therefore, it is essential to assess the potential security risks in order to improve the security status of smart houses and also improve the energy consumption of the various things connected to the Internet.

3 Challenges of using IoT in Smart Houses statement

The Internet of things (IoT) in smart houses faces a lot of challenges and these include but are not limited to the following; **Reliability**; the distributed nature of IoT devices makes it difficult to ensure their dependability. Various conditions such as natural disasters, cloud service interruptions, power outages, and system failures can greatly impact the functionality of these IoT devices**. Privacy**; IoT devices that are connected to the internet are susceptible to external attacks and these collect and send private data over open networks that are not encrypted, making it easily accessible to hackers. **Internet availability**; can be a challenge for many IoT devices, especially if they are widely distributed in remote areas or if bandwidth is very limited. **Insufficient testing & Outdated products;** The IoT industry is currently flooded with a large number of manufacturers. Due to competition, they tend to rush to launch their products and software without sufficient testing. Most manufacturers do not provide timely updates, and their IoT devices are not normally updated, which can make them susceptible to data theft. As new weaknesses are identified to maintain security, IoT devices should be thoroughly tested and updated. **Lack of technical know-how**; IoT technologies have been around for some time and it's a fast-growing industry but unfortunately, most people do not know much about it. One of the biggest security threats associated with this technology is the lack of technical knowledge of users about its capabilities, which poses a threat to all users. **Energy consumption**; is also a big problem in the IoT industry as IoT devices need a lot of energy to collect, process, and communicate information. If the grid-separated things depend on battery power, a replacement can be a problem.

4 Problem statement

This section describes the previous works that different researchers have worked on to develop and implement improved smart home systems focusing mainly on how to reduce energy consumption, mitigate security flaws, and predict smart homes' usage patterns. The authors **JiHyeon Oh et al.** [1] examine the protocol developed by Xiang and Zheng and they emphasize its limitations as it is insecure, unable to perform mutual authentication, and is susceptible to attacks. Using the ROR model and BAN logic, they propose to develop a lightweight and secure authentication protocol for IoT-based smart homes to address vulnerabilities in the protocol developed by Xiang and Zheng. However, there are still problems with the proposed protocol as it has not been fully developed and has not been implemented in a real environment. **Isaac Machorro-Cano et al.** [2] use machine learning algorithms to learn the behavior and energy usage patterns and rank homes by energy usage. They are proposing a smart home energy management system for home IoT devices that is based on big data and machine learning called (HEMS-IoT) to monitor energy consumption patterns for home comfort, security, and energy savings. The proposed system only supports Android OS and does not give custom power-saving recommendations due to some limitations. **Marios Anagnostopoulos et al.** [3] present the traffic monitoring and capturing mechanism that is used to monitor smart-home activity holistically and it also enables the extraction of significant data from traffic captures of multiple IoT protocols. The proposed model was only limited to a single data set and subjected to a few scenarios. A cost- effective integrated system for smart homes based on IoT and Edge-Computing paradigm is proposed by Hikmat **Yar et al.** [4] propose a cheap IoT integrated system for smart homes that controls home appliances remotely ensuring security and safety using edge-computing paradigm to store sensitive data in a local cloud to preserve the customer's privacy. However, the system does not support built-in vision-enabled technologies for processing different kinds of multimedia data such as images and surveillance video. **Shahzadi Tayyaba et al.** [5] used fuzzy logic to simulate a smart home model for the safe and robust mobility of visually impaired people. The proposed system allows users to move with ease while avoiding obstacles. The proposed system is limited to simulation only and does not take into account the integration of additional functionalities such as vibration signals. **Ezequiel Simeoni et al.** [6] use KNX technology to implement a standard with home automation ontology and provides a Living Lab gateway that enables users to leverage any IoT device from their smart home. Their research suggests mitigating technology fragmentation and improving access to devise operations in heterogeneous device ecosystems. The Living Lab Gateway was not benchmarked with other similar technologies for performance comparison. A platform based on IoT and cloud technologies that enable users to use a mobile application to monitor and control their wireless devices in the home remotely is proposed by **Fabian Garcia-Vazquez et al.** [7] The system can collect and store e-switch data used for further processing and analysis, but there is no tool to convert home automation devices to smart devices. An element of AI is missing to allow devices to make their own decisions based on the residents' habits. **Ladislav Huraj et al.** [8] investigated SYN flood attacks & HTTP Get flood attacks by behavior when IoT devices and the entire smart homes were victims of DDoS attacks. They present experimental results for single-scenario attacks performed and demonstrate the response of real IoT device sensors against these attacks. Their work does not give a detailed study on the case of cloud communication between IoT sensors and personal assistant systems and no strong framework against DDoS attacks was proposed. **Soojung Chang et al.** [9] proposed a system that can provide important information to build effective services and identify appropriate target users using Regression analysis. But the study failed to present the correlation between demographic factors and this scope does not include services. The importance of simulation was shown by **Erdal Ozdogan et al.** [10] when they used Cisco packet tracer 8.0 to show how to use simulation tools effectively in the building of IoT supported home intelligent control systems but the analysis of network traffic and bandwidth consumption was not examined. **Nermeen A. Eltresy et al.** [11] designed an energy-efficient IoT platform system for reducing energy consumption using RF energy but their scheme has a high-power consumption and node failure. **Ziaur Rahman et al.** [12] proposed an IoT-based smart home environment system to protect against various failures but its methods are not consistently applied to the security of the entire vulnerability. **Bako Ali et al.** [13] tackled 15 security risks from within and outside of IoT-based smart houses and they proposed some countermeasures using the OCTAVE method, but a platform for realization and evaluation of security threats in IoT-based smart homes was not included. **Victor Takashi Hayashi et al.** [14] demonstrated a concept that helps with the financial transaction and smart-home recognition by voice commands using PUF, but their scheme doesn’t evaluate experimentally and doesn’t provide better results for the trusted IoT device with PUF. A design of a multi-purpose Android OS mobile application for remotely controlling a smart home was proposed by **Olutosin Taiwo et al.** [15] and they used a machine learning algorithm (CNN) but they failed to build a model to classify extended family members and their friends. **Adrian Micu et al.** [16] used TAM in their proposed smart home IoT system to minimize energy consumption and production using a small sample size. Zi-Wi protocol was demonstrated by **Iván Froiz-Míguez et al.** [17] when they demonstrated the usability of ZigBee and Wi-Fi for computing in home automation systems (HAS) but they found that Zi-Wi increases power consumption measurements. **Heetae Yang et al.** [18] demonstrate using PLS-SEM interconnectivity and reliability which are required in the implementation, development, and adoption of smart home systems but they didn’t take into consideration a significant variation between existing and potential smart home service users. **Ruili Zheng et al.** [19] designed a system using RSSI which combines sensor technology and smart home design however they select a lower threshold that affects the complex home environment. Using reinforcement learning (RL) **Metin Ozturk et al.** [20] were able to reduce power consumption while meeting the quality requirements of all relevant applications, resulting in reduced computing power and failure to meet overall context-aware performance goals.

Table 1. Description & demerits of Related Works….

SN	Author Name	Method	Contribution	Objective	Demerits/Limitations
1	JiHyeon Oh et al. [1]	ROR, BAN, AVISPA	Developed a secure and lightweight authentication protocol for IoT-based smart homes to deal with the security flaws of the protocol developed by Xiang and Zheng.	To examine a protocol developed by Xiang and Zheng and point out its flaws such as its inability to provide secure, mutual authentication, and vulnerability to attacks.	The suggested protocol still contains flaws, as it was not fully developed and wasn't implemented in an actual environment.
2	Isaac Machorro-Cano et al. [2]	J48 ML algorithm & Weka API	It proposed a home energy management system for IoT devices in homes (HEMS-IoT) to monitor energy consumption patterns.	To develop a smart home management system for energy consumption based on big data and machine learning.	The system only supports android OS, it does not generate customized energy- saving recommendations
3	Morios Anagnostopoulos et al. [3]	NFDA	It enables the extraction of significant data from traffic captures of multiple IoT protocols.	To develop a model/mechanism that is capable of monitoring smart-home activities.	The proposed model was only limited to a single data set and subjected to a few scenarios.
4	Hikmat Yar et al. [4]	Edge computing paradigm	Energy usage, processing, and	To develop a cheap IoT integrated system	The system does not support

			response time were improved.	for smart homes that controls home appliances remotely.	built-in vision-enabled technologies to process different kinds of multimedia data such as images and video.
5	Shahzadi Tayyaba et al. [5]	Fuzzy logic	Proposed a smart house model for visually-impaired people's safe and reliable mobility, which aids in navigation and obstacle avoidance.	To create a model for smart houses that uses IoT devices to help visually-impaired people navigate more comfortably.	There was no consideration for extra vibrational signals, electronics, or IoT device integration because it was merely a simulation.
6	Ezequiel Simeoni et al. [6]	KNX Technology	It reduces technology fragmentation and improves device manipulation accessibility for heterogeneous devices.	To build and implement a secure and scalable smart home gateway to bridge technology fragmentation.	For performance comparison, the Living Lab Gateway was not benchmarked with other similar technologies
7	Fabian Garcia- Vazquez et al. [7]	Cloud technology	The system is capable of collecting and storing e- switch data used for further processing and analysis	To design and develop a mobile application to monitor and control wireless devices in a smart home.	The system is missing tools needed to turn home automation devices into smart gadgets. There isn't enough

					AI in the system to allow devices to make their own judgments.
8	Ladislav Huraj et al. [8]	SYN & HTTP (flood attacks)	It shows the response of IoT device sensors when they are subjected to distributed denial of service attacks	To investigate how IoT devices and the entire smart home will behave if they become victims of a distributed denial of service attacks	There was no robust mechanism for defending against DDoS attacks proposed.
9	Soojung Chang et al. [9]	Scheffe’s Regression analysis	All findings are useful to service providers and related enterprises such as IT, engineering, and architecture, to build effective services and identify appropriate target users.	To learn more about user views on the relationship between smart home service choice and adoption.	The association between demographic parameters was not taken into account and the scope did not include all of the services that make up the home market.
10	Erdal Ozdogan et al. [10]	REST API	Used sample situations to demonstrate the value of utilizing Cisco packet tracer 8.0 simulation software.	To discuss how to use simulation tools effectively in the development of IoT home control systems.	Network traffic and bandwidth consumption was not examined.

11	Nermeen A. Eltresy et al. [11]	RF energy	Proposed an IoT platform for smart homes that are powered by electromagnetic energy harvesting.	To develop an energy- efficient Internet of Things system to reduce the overall energy consumption	The proposed scenario has high power consumption and sensor node failure.
12	Ziaur Rahman Et Al. [12]	3-dimensional S-box (Substitution- box)	Uses a 3-dimensional key generation to increase the difficulty of key generation and reduce the probability of keys being broken.	To evaluate whether the suggested approach is secure against a range of faults, an IoT- based smart-home environment was created.	The proposed solution is not always appropriate for securing against various vulnerabilities.
13	Bako Ali et al. [13]	OCTAVE	Identifying 15 security dangers that originate from both within and outside of the smart home as well as potential solutions	To identify security dangers to residents and provide ways to mitigate the identified hazards.	The proposed solution lacks a framework for identifying and assessing security concerns in IoT-based smart homes.
14	Victor Takashi Hayashi et al. [14]	PUF	Developed a smart home authentication system that uses voice recognition commands.	To develop a device for hands-free scenarios, integrated with smart home behavior for continuous authentication.	This scenario doesn’t use obfuscation, key splitting, or secure multi-party computing procedures

15	Olutosin Taiwo et al. [15]	CNN (Convolution neural network)	Designed and developed a multi-purpose Android- mobile application for controlling and monitoring the smart home	To develop a mobile application for smart home automation with machine learning capabilities.	The model failed to classify extended family members and friends.
16	Adrian Micu et al.[16]	Technology Acceptance Model (TAM)	Energy consumption of IoT devices was reduced.	To develop a smart home IoT system that minimizes energy consumption.	The sample data used was limited
17	Ván Froiz-Míguez et al. [17]	Zi-Wi	Demonstrates the advantages of using Zi-Wi, a low-cost IoT fog computing home automation system (HAS).	To show that Zi-Wi can provide a low-cost and adaptable home automation system (HAS).	The use of Zi-Wi increases the amount of energy consumed.
18	Heetae Yang et al. [18]	PLS-SEM	It indicates that interconnection and reliability, as well as the right level of automation, are essential to deliver valuable insights regarding smart home service adaptation.	To examine the elements of smart homes services that present customers want, as well as experimentally assessing the relationship between important aspects and adaptation behavior.	Existing and potential smart home service users may have a considerable difference in the influence of antecedents on behavioral intention.

19	Ruili Zheng [19]	RSSI	Design of a sensor- enabled smart home system.	To study a smart home automation system based on wireless sensor network positioning.	It chooses the lowest threshold that has an impact on the home's complex surroundings.
20	Metin Ozturk et al. [20]	Reinforcement Learning (RL)	It reduces computing power while meeting the quality requirements of all related applications.	To create a framework that maximizes the IoT network's connectivity and processing speed.	There are predictable scenarios that could result in lower computing costs or energy usage.

5 Recommendations of the proposed projects in the EA context

Based on the review conducted on the various papers published by different researchers, it has been observed that they recommend the implementation of security and privacy features as a key requirement in future systems because most of the IoT systems discussed in the papers above did not fully address the issue of security and privacy clearly, there is still a gap. We, therefore, propose the following ways to solve IoT vulnerabilities if these systems were to be implemented in the East African region, and these include; **Avoid universal plug and play devices/features**. The majority of the IoT devices have these plug-and-play features that allow them to communicate with each other without configuration. Although this provides convenience to the smart homeowners, these devices use local area networks for connectivity, and these networks are extremely vulnerable to external attacks and are easily accessible by anyone connected to the internet. **IoT devices need to be updated regularly**; as mentioned in Section 3 above about the lack of updates as one of the IoT security issues, smart homeowners need to set up or implement automatic updates to see official updates by device manufacturers. This will install the required security patches on the IoT devices and this will prevent hackers from breaking into them as well as increase the security level of the smart house. **Authenticate access using frequently changed passwords;** We're often encouraged to add some level of security while accessing these IoT devices by using not-easy-to remember passwords on internet accounts and for this, we recommend each IoT device should have a unique password that is complex and tough to crack and these should be changed occasionally. **Cloud Technology has challenges, have alternatives;** when dealing with IoT, the best or most preferred option for data storage is the cloud, but we've found out that this technology is highly susceptible to external attacks. Most of these devices have their own cloud storage space. For this reason, users of these systems are advised to always thoroughly review the data protection measures that come with their cloud accounts and store or back up files and data locally whenever possible. **Use multiple networks**; The approach of creating additional restricted networks can also be used for home IoT devices to prevent unauthorized access to personal data.

However, in the East African region, for IoT-based smart houses to be implemented, several issues need to be addressed to make this a success, and these include; **Internet availability** most countries in the East African region still face internet connectivity challenges. **Electricity fluctuations**; for IoT-based systems to perform effectively, they need 24/7 round-the-clock availability of electrical power which is not available in the East-African region. This could be solved by using onboard batteries or even using solar power. **Cost of the system**; before implementing such systems, their cost should be considered because the majority of the people living within the East African region are poor with little or no knowledge at all of how these systems operate.

6 Conclusion

Smart homeowners are now able to remotely monitor and control their smart houses and their surroundings regardless of where they're in the world all because of IoT technologies. In the past few years, prominent companies like Google, Amazon, Apple, Samsung, Xiaomi, LG, etc have brought to the market several IoT smart home devices that have already been implemented, tested, and applied for automated control and monitoring of homes. However, we've noticed that a lot of challenges as stipulated in section 3 still exist and in section 4 we see that several researchers have proposed and presented different approaches to mitigate these challenges. Having analyzed all the different proposed works from the above-mentioned researchers, we also realized that technologies such as machine learning/deep learning were not fully utilized in building predictive smart house automation systems. We, therefore, propose a machine learning IoT based home automation system that is capable of remote monitoring and controlling all electrical appliances, monitoring all home environmental conditions, detecting and reporting intruder movements in the home, and the data collected can then be stored on the cloud, which can be accessed and used for predicting home user patterns using machine learning algorithms.

References

1. J. Oh, S. Yu, J. Lee, S. Son, M. Kim, and Y. Park, "A secure and lightweight authentication protocol for iot- based smart homes," Sensors, vol. 21, no. 4, pp. 1–24, Feb. 2021, doi: 10.3390/s21041488.
2. I. Machorro-Cano, G. Alor-Hernández, M. A. Paredes-Valverde, L. Rodríguez-Mazahua, J. L. Sánchez- Cervantes, and J. O. Olmedo-Aguirre, "HEMS-IoT: A big data and machine learning-based smart home system for energy saving," Energies (Basel), vol. 13, no. 5, Mar. 2020, doi: 10.3390/en13051097.
3. M. Anagnostopoulos, G. Spathoulas, B. Viaño, and J. Augusto-Gonzalez, "Tracing your smart-home devices conversations: A real world iot traffic data-set," Sensors (Switzerland), vol. 20, no. 22, pp. 1–28, Nov. 2020, doi: 10.3390/s20226600.

4. H. Yar, A. S. Imran, Z. A. Khan, M. Sajjad, and Z. Kastrati, “Towards smart home automation using iot- enabled edge-computing paradigm,” Sensors, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144932.
5. S. Tayyaba, M. W. Ashraf, T. Alquthami, Z. Ahmad, and S. Manzoor, “Fuzzy-based approach using iot devices for smart home to assist blind people for navigation,” Sensors (Switzerland), vol. 20, no. 13, pp. 1– 13, Jul. 2020, doi: 10.3390/s20133674.
6. E. Simeoni et al., “A secure and scalable smart home gateway to bridge technology fragmentation,” Sensors, vol. 21, no. 11, Jun. 2021, doi: 10.3390/s21113587.
7. F. García-Vázquez, H. A. Guerrero-Osuna, G. Ornelas-Vargas, R. Carrasco-Navarro, L. F. Luque-Vega, and E. Lopez-Neri, “Design and implementation of the e-switch for a smart home,” Sensors, vol. 21, no. 11, Jun. 2021, doi: 10.3390/s21113811.
8. L. Huraj, M. Šimon, and T. Horák, “Resistance of IoT sensors against DDOS attack in smart home environment,” Sensors (Switzerland), vol. 20, no. 18, pp. 1–23, Sep. 2020, doi: 10.3390/s20185298.
9. S. Chang and K. Nam, “Smart home adoption: The impact of user characteristics and differences in perception of benefits,” Buildings, vol. 11, no. 9, Sep. 2021, doi: 10.3390/buildings11090393.
10. E. ÖZDOĞAN and R. DAŞ, “IoT based a Smart Home Automation System Design: Simulation Case,” Balkan Journal of Electrical and Computer Engineering, Aug. 2021, doi: 10.17694/bajece.918826.
11. N. A. Eltresy et al., “Smart home IoT system by using RF energy harvesting,” Journal of Sensors, vol. 2020. Hindawi Limited, 2020. doi: 10.1155/2020/8828479.
12. Z. Rahman, X. Yi, M. Billah, M. Sumi, and A. Anwar, “Enhancing AES Using Chaos and Logistic Map- Based Key Generation Technique for Securing IoT-Based Smart Home,” Electronics (Basel), vol. 11, no. 7, p. 1083, Mar. 2022, doi: 10.3390/electronics11071083.
13. B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” Sensors (Switzerland), vol. 18, no. 3, Mar. 2018, doi: 10.3390/s18030817.
14. V. T. Hayashi and W. V. Ruggiero, “Hands-Free Authentication for Virtual Assistants with Trusted IoT Device and Machine Learning,” Sensors, vol. 22, no. 4, Feb. 2022, doi: 10.3390/s22041325.
15. O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, “Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model,” Wireless Communications and Mobile Computing, vol. 2022, 2022, doi: 10.1155/2022/9307961.
16. A. Micu, A. E. Micu, M. Geru, A. Capatina, and M. C. Muntean, “The challenge for energy saving in smart homes: Exploring the interest for iot devices acquisition in romania,” Energies (Basel), vol. 14, no. 22, Nov. 2021, doi: 10.3390/en14227589.
17. I. Froiz-Míguez, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, “Design, implementation and practical evaluation of an iot home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes,” Sensors (Switzerland), vol. 18, no. 8, Aug. 2018, doi: 10.3390/s18082660.
18. H. Yang, W. Lee, and H. Lee, “IoT Smart Home Adoption: The Importance of Proper Level Automation,”Journal of Sensors, vol. 2018, 2018, doi: 10.1155/2018/6464036.
19. R. Zheng, “Indoor Smart Design Algorithm Based on Smart Home Sensor,” Journal of Sensors, vol. 2022, pp. 1–10, Apr. 2022, doi: 10.1155/2022/2251046.
20. M. Ozturk, M. Jaber, and M. A. Imran, “Energy-Aware Smart Connectivity for IoT Networks: Enabling Smart Ports,” Wireless Communications and Mobile Computing, vol. 2018, 2018, doi: 10.1155/2018/5379326.