Journal of Operational and Strategic Analytics
https://www.acadlore.com/journals/JOSA

Investigation of IoT-Integrated Smart Homes

Rita de Fátima Muniz[1*], Sheila Maria Muniz[2]

[1] Federal University of Ceara, Fortaleza, CE, Brazil
[2] Municipal Secretary of Education of Jijoca de Jericoacoara, Jijoca de Jeric., CE, Brazil

[*] Correspondence: Rita de Fátima Muniz (ritafatimamuniz@gmail.com)

Received: 01-30-2023 **Revised:** 03-10-2023 **Accepted:** 03-17-2023

Citation: R. F. Muniz, S. M. Muniz, "Investigation of IoT-integrated smart homes," *J. Oper. Strateg Anal.*, vol. 1, no. 1, pp. 42–45, 2023. https://doi.org/10.56578/josa010106.

Abstract: The growth of internet-connected services, known as the Internet of Things (IoT), has led to a proliferation of new applications. One such application is the smart home, where household appliances and devices can be remotely monitored and controlled. To achieve this, appropriate network architecture and standard protocols are used to connect various devices to the internet, resulting in an "IoT-based smart home." However, managing and regulating the entire system, as well as ensuring the security of servers and smart homes, present challenges. This paper presents an IoT architecture and discusses the issues and difficulties faced by IoT-enabled smart home systems while also proposing potential solutions. Smart homes simplify home automation tasks and offer greater convenience to users. The Industrial Wireless Sensor Network (WSN) has already demonstrated the potential of IoT, and the integration of IoT into smart homes is a logical next step. The article explores various aspects of IoT-based smart homes and highlights the need for proper management and security protocols. In conclusion, the study investigates the integration of IoT into smart homes, highlighting the challenges and solutions associated with the development of an IoT-based smart home system. The objective is to provide a framework for the development and management of IoT-based smart homes that will enhance the quality of life for users.

Keywords: Smart house; Internet of Things (IoT); Radio frequency identification

1 Introduction

The ability to interact with anyone, anywhere, at any time has been revolutionized by the internet. Technological advancements have made sensors, processors, transmitters, and receivers more affordable, enabling their integration into our daily lives [1]. IoT is an expansion of the range of internet services available [2]. IoT refers to a network of computers that connect physical objects or things in the real world using the existing internet infrastructure. These things can be anything, such as furniture, equipment, automobiles, etc., and the entire system is called IoT once devices link to the internet using a particular infrastructure and accepted protocols [3–5].

Things, whether physical or digital, play an active role in the IoT system and can communicate with other things (things-to-things communication) or with humans (things-to-human communication) [6]. The IoT is not just a futuristic fantasy; it already exists and has far-reaching effects on technological advancement. Devices and objects communicating via the internet can set up their configurations and operate autonomously [7]. As shown in Figure 1, the IoT architecture consists of interconnected devices and objects [8].

A smart home is a living space equipped with technology that enables automatic and remote control of all appliances and household gadgets [9]. Users of smart homes can easily monitor and manage all home electronics and appliances online. Home appliances connect using established protocols and correct network architecture. Figure 1 illustrates a fundamental IoT-based concept for smart homes, which can be divided into two sections: one section includes all household appliances, switch modules, and RF transmitters and receivers, while the second section has all interface devices, processors, data collectors, and GPRS modules that connect to the internet [10].

The paper focuses on four domestic appliances: a light, a fan, a television, and a gas outlet, but users can connect various other gadgets [11]. All home appliances are connected to switch modules, which can modify their state in response to a signal. Switch modules can be any type of module that changes its state, and when a switch module is linked to a device, the associated home devices' states also change accordingly [2, 4, 8, 12]. Relays are commonly used as switch modules, which magnetically join two circuits while electrically isolating them [13]. Switch modules

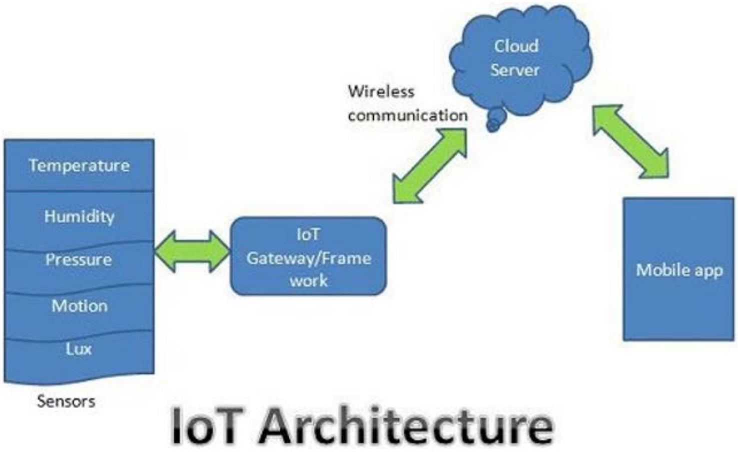

Figure 1. IoT architecture

Figure 2. Smart home basic idea

are connected to a smart central controller via an RF transceiver. Each switch module has one transceiver, or one transceiver can connect to all modules, with each module and device given a unique identity [12]. The smart central controller, which has one RF transceiver, acts as the intermediary between home appliances and the internet server [14, 15]. RF modules communicate with each other at a frequency of 433MHz, which was created specifically for RF communication [4].

2 Related Work

Descriptions of IoT-based Smart Homes' layered architecture can be found in reference [8]. The smart home system is structured into application, network, and sensor layers. The sensing layer gathers data from all household appliances and sends it to the network layer in the center [16]. Various applications at different levels are found in the topmost application layer, which uses the internet to transfer data. Data collecting and processing at the sensing layer were performed using the SAMSUNG S3C2440A microprocessor, an ARM-based microcontroller [8]. In reference [5], the authors designed a reconfigurable smart sensor interface device for industrial Wireless Sensor Networks (WSN) that applies CPLD. This device integrates data collection, processing, and wired and wireless transmission [17]. Although microcontrollers have advantages such as low cost and low power consumption, they conduct tasks via interrupts, making multisensory acquisition interfaces not parallel in gathering multisensory data. CPLDs are complex programmable logic devices and are used in industrial wireless sensor networks.

The wireless sensor and actuator network (WSAN) operates at 433MHz radio frequency with the help of the smart central controller. All types of appliances can be controlled directly by radio frequency modules developed by Mohapatra and Rath [2, 4]. RF identification was used in references [1, 2, 4], providing each household device with a unique identity. The RF's range can be adjusted in both directions. For smart homes, efficient and secure human-machine connections are challenging to manage.

Wireless sensor networks linked to the internet have security issues. Two primary problems are establishing the initial session key and controlling the center. An easy key establishment mechanism is provided for the smart home energy management system [13]. IP addresses are required for all internet-connected devices [3]. IPv4 protocol has a limited address space and is still in use. With the increase in users, people must switch to IPv6, which offers a vast address space. However, smart home systems cannot fully interoperate due to current market practices that effectively bind consumers to proprietary technologies. Consumers must purchase devices that conform to a specific manufacturer's system to be fully interoperable. The DomoNet system, created by Vittorio Miori et al., is an innovative ”ecosystem” software designed to overcome compatibility issues with pre-existing smart home systems.

3 Study Summarize

The Smart Home system is susceptible to various concerns, issues, and challenges. Managing applications in IoT environments can be challenging since they expand rapidly in number, and the question of how to govern and oversee these numerous applications arises. If these applications are not adequately managed, the entire system's security and comfort could be compromised [2]. On the server side, security is lower because no unique authentication technique is employed, which can result in an insecure system. An attacker could gain entry to the victim's home and destroy the entire smart home system. Another issue that could arise is connectivity [4].

•Standards: Standardization is crucial for ensuring interoperability, security, and reliability in IoT systems. However, deciding which standards to employ, which will provide a secure medium, and how to increase system reliability can be challenging.

•Identification: Every device needs a unique identifier to be recognized individually, while user information should be kept private. Maintaining privacy while maintaining connectivity is essential.

•Authentication: Authorization and authentication are necessary to protect a Smart Home system from an intruder. Only authorized users should be able to receive access from the server.

•Security: The system must be capable of responding appropriately to security risks, and it must be capable of reconfiguring itself after attacks.

•Application integration: Integration of applications is a significant hurdle to overcome in an IoT environment.

•Coordination: Coordination is necessary between globally connected items, people, programs, and processes.

•Data Storage: As IoT applications grow, a vast amount of data is being gathered. The problem of where to store this data can be resolved by using large databases and employing artificial intelligence algorithms to separate meaningful information from redundant data.

•Network Self-Organization: The topology of a network should be designed so that each linked device can self-organize, ensuring that the network has the ability to self-organize.

4 Conclusion

The Internet of Things has the potential to benefit numerous industries. It is already being utilized in industrial Wireless Sensor and Actuator Networks (WSANs) and Smart Home Systems. This paper provides an overview of IoT architecture and Smart Homes while also highlighting some of the challenges associated with these technologies. However, these issues can be mitigated with the use of new technologies and approaches. The essay explores potential problems and difficulties, as well as innovations that can enhance IoT applications. Currently, IoT relies on technologies such as CPLD controllers, Zigbee modules, and RF modules.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Mohapatra and A. K. Rath, “Fault-tolerant mechanism for wireless sensor network,” *IET Wirel. Sens. Syst.*, vol. 10, no. 1, pp. 23–30, Feb 2020. https://doi.org/10.1049/IET-WSS.2019.0106

[2] H. Mohapatra and A. K. Rath, “Fault tolerance in wsn through pe-leach protocol,” *IET Wirel. Sens. Syst.*, vol. 9, no. 6, pp. 358–365, Dec 2019. https://doi.org/10.1049/IET-WSS.2018.5229/CITE/REFWORKS

[3] H. Mohapatra and A. K. Rath, “Detection and avoidance of water loss through municipality taps in india by using smart taps and ict,” *IET Wirel. Sens. Syst.*, vol. 9, no. 6, pp. 447–457, Dec 2019. https://doi.org/10.1049/IET-WSS.2019.0081

[4] H. Mohapatra and A. K. Rath, “Survey on fault tolerance-based clustering evolution in wsn,” *IET Networks*, vol. 9, no. 4, pp. 145–155, Jul 2020. https://doi.org/10.1049/IET-NET.2019.0155

[5] J. Y. Kim, H.-J. Lee, J.-Y. Son, and J.-H. Park, “Smart home web of objects-based iot management model and methods for home data mining,” in *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. Busan, Korea (South): IEEE, 2015, pp. 327–331. https://doi.org/10.1109/APNOMS.2015.7275448

[6] A. Kumar and A. C. F. Thomaz, “Prediction of fertilizer in horticulture through iot enabled technology,” *Big Data and Computing Visions*, vol. 3, no. 1, pp. 15–20, 2023. https://doi.org/10.22105/bdcv.2022.332448.1057

[7] V. Govindraj, M. Sathiyanarayanan, and B. Abubakar, “Customary homes to smart homes using internet of things (iot) and mobile application,” in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*. Bengaluru, India: IEEE, 2017, pp. 1059–1063. https://doi.org/10.1109/SmartTechCon.2017.8358532

[8] P. Mtshali and F. Khubisa, “A smart home appliance control system for physically disabled people,” in *2019 Conference on Information Communications Technology and Society (ICTAS)*. Durban, South Africa: IEEE, 2019, pp. 1–5. https://doi.org/10.1109/ICTAS.2019.8703637

[9] Y.-H. Lin, H.-S. Tang, T.-Y. Shen, and C.-H. Hsia, “A smart home energy management system utilizing neurocomputing-based time-series load modeling and forecasting facilitated by energy decomposition for smart home automation,” *IEEE Access*, vol. 10, pp. 116 747–116 765, 2022. https://doi.org/10.1109/ACCESS.2022.3219068

[10] J. Liu, M. Wang, and X. Wang, “Research on general model of intelligence level for smart home,” in *2022 7th International Conference on Computer and Communication Systems (ICCCS)*. Wuhan, China: IEEE, 2022, pp. 123–129. https://doi.org/10.1109/ICCCS55155.2022.9846791

[11] V. D. Vaidya and P. Vishwakarma, “A comparative analysis on smart home system to control, monitor and secure home, based on technologies like gsm, iot, bluetooth and pic microcontroller with zigbee modulation,” in *2018 International Conference on Smart City and Emerging Technology (ICSCET)*. Mumbai, India: IEEE, 2018, pp. 1–4. https://doi.org/10.1109/ICSCET.2018.8537381

[12] S. M. Muniz, “Deployment of agriculture 4.0 with the integration of iot,” *Computational Algorithms. Num Dimensions.*, vol. 1, no. 3, pp. 122–125, 2022. https://doi.org/10.22105/cand.2022.161803

[13] L. Liu, Y. Liu, L. Wang, A. Zomaya, and S. Hu, “Economical and balanced energy usage in the smart home infrastructure: A tutorial and new results,” *IEEE T. Emrg Top. Com.*, vol. 3, no. 4, pp. 556–570, 2015. https://doi.org/10.1109/TETC.2015.2484839

[14] V. Nozick, “Adoption of drone technology for the smart safety mechanism of women,” *Big Data and Computing Visions*, vol. 2, no. 3, pp. 128–132, 2022. https://doi.org/10.22105/bdcv.2022.333758.1073

[15] E. B. Priyanka, C. Maheswari, and S. Thangavel, “A smart-integrated iot module for intelligent transportation in oil industry,” *Int J. Numer Model.*, vol. 34, no. 3, p. e2731, 2021. https://doi.org/10.1002/jnm.2731

[16] H. Alqahtani, “Role of wireless sensor network in precision agriculture,” *Computational Algorithms. Num Dimensions.*, vol. 1, no. 2, pp. 84–88, 2022. https://doi.org/10.22105/cand.2022.158703

[17] A. Yousif and B. Almaz, “Amplifying the yield of the harvests through wireless sensor network in smart agriculture,” *Big Data and Computing Visions*, vol. 2, no. 4, pp. 138–142, 2022. https://doi.org/10.22105/bdcv.2022.334373.1077