

Secure smart home automation and monitoring system using internet of things

Mohamed Khudhair Al-Gburi, Laith Ali Abdul-Rahaim

Department of Electrical Engineering, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received Apr 10, 2022

Revised Jun 25, 2022

Accepted Jul 8, 2022

Keywords:

Arduino

Home automation

Internet of things

Security

Smart home

ABSTRACT

As a result of the rapid increase in the number of users in internet of things (IoT) technologies, IoT becomes one of the most important technologies that play an important and essential role in various areas of human life, it provides service over 24 hours. In this paper, the proposed system relies on the implementation of a set of sensors for the Internet of things, which accomplish tasks inside the home automation, for example, controlling the main door, boiler and lock, as well as the ability to control lighting and air, internal temperature sensors, it based on the Arduino, to collect multimedia data, and remote-controlled sensors. The proposed system provides an efficient way to control and monitor the various devices in the home for security and safety purposes, and through sensors that rely on wireless technologies. The results show the abnormal alarm notification for healthcare/security purposes with the distance as 27 cm, smoke carbon monoxide on indoor air quality as 10211 degree Co as 6256 degree, Liquefied petroleum gas as 5097 degree, the delayed 3.4 ms and network latency as 0.0012 seconds of alarm notification with long distance as 60 m and high packet delivery ratio as 98.7%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohamed Khudhair Al-Gburi

Department of Electrical Engineering, University of Babylon

51002, Babylon, Iraq

Email: mohamed.algburi@uobabylon.edu.iq

1. INTRODUCTION

The internet of things (IoT) allows devices of various types to be connected and monitored via the Internet over long distances. This concept has been noticed in recent years and has attracted the attention of researchers, as it is used in various fields, including smart homes, industrial environments, and commercial fields, where this system depends on wireless sensor networks that are linked to each other where it consists of a set of sensors and electronic actuators that are connected with to build multiple applications such as smart homes [1].

The smart home is one of the parts and components of the internet of things, which aims mainly to integrate home automation and allows the connection of different things and the possibility of monitoring and controlling them remotely, for example, allowing the ability to manage the light switches, turning them off and on, remotely using the phone, as well as through voice or thermostats. Which contribute to controlling the internal temperatures of the house and the use of power units, as well as in level systems to manage the water [2].

The smart home provides very many facilities in terms of security, energy management and low operating costs, as it reduces time, effort, money and energy. These systems are adaptable and the possibility of adjusting the various special needs. I ask you about the house. The infrastructure is flexible and subject to

change and from different standards, as it provides measurement of home conditions. Precise control of embedded devices [3]. One of the many advantages of home automation systems is the ease of management and control through smart devices, phone, computer, mobile devices, tablets or smart watches, where the brakes are controlled by remote control and the devices lock the automatic doors, increase comfort by regulating temperatures and the possibility of controlling and saving money [4].

Many home automation systems that are based on the Internet of things have been proposed by researchers. Wireless networks are relied upon using different technologies, each of which has its advantages and disadvantages, for example, Bluetooth was born and used in many automations that are low-cost, fast and easy to install, but the distance is limited in addition to that. Global system for mobile communication (GSM) or Z** is one of the widely used wireless technologies, as it has provided lounges that do not extend. I send a design in a way that is low in cost and low in energy consumption, but it is characterized by low data transmission speed, low tiring, and network stability is also low and the possibility of maintenance is very high, and this is what it is devices based on Wi-Fi technology are cheap, which are always available in and can be based on this application [5].

View common uses can invest in hardware by relying on home automation Crescent basic setup operating system in the home [6]. However, whoever uses Wi-Fi to create interconnected networks, it targets energy ten times more than devices that rely on Bluetooth completely and allows a limited number of devices up to thirty devices connected at one time compared to Ethernet. Wi-Fi is characterized by ease of access and the ability to expand without the need for wires low cost, as it is affected by obstacles or walls that cause weak signal, and other challenges related to Wi-Fi, including Internet security and privacy issues, are the impact of noise [7]. The most related works in term of IoT based Smart home automation and monitoring systems have been discussed and overviewed as follow:

Domb [8] a set of main issues have been proposed in the scenario of the smart home for automation and hope. The problem of security is dealt with the smart home via the Internet. Focus on providing on confidentiality, credibility and safety of data that are sensitive to and exchanged by smart home objects. It is very important to know and study human behavior. The results show that the proposed concept of the home Smart reduce expense overhead.

Yar *et al.* [9] a method based on exploring the concept of the smart home and its related services, integrating the Internet of things and cloud computing, by integrating artificial intelligence (AI) in sensors, modern technology, chocolate, access to different sites and increasing storage space, the efficiency of data transmission, as it was based on a system based on three main components that contribute to explaining the results expected from a smart home.

Stolojescu *et al.* [10] they proposed an integrated cost-effective system based on the concept of the edge as an internet of things computer. The proposed system provides the possibility of remote control of home appliances. YouTube Security and safety stores data. Maintaining the privacy of this data. Data is processed from visual and standard sensors. Bandwidth is reduced. Storage cost. The proposed efficiency is 6% of the efficiency of the current solutions in terms of energy consumption, and it achieves a speed exceeding 5% in detecting motion.

Islam *et al.* [11] a system has been proposed that connects sensors and other data sources, and this system is called qToggle and works by relying on a flexible and powerful application programming interface based on application programming interface (API). With Arduino, the proposed system through the results, ease of use, second development, more reliance on various additions.

Taiwo and Ezugwu [12] the proposed system responses to the organization and analysis of home automation that is based on the Internet of things using IoT technology NodeMCU rely on a proven message queuing telemetry transport (MQTT) protocol, the proposed system, surveillance cameras, remote devices, using the phone application over the Internet.

Jo *et al.* [13] they design and development proposals for smart and cloud-based home automation systems? The proposed system from the home through a mobile phone with an Android system on a controller that overlays devices and environmental factors and supervises home security through movement and taking pictures. It was relied on a camera that takes pictures to avoid false alarms. Was it done? Relying on the concept of machine learning to distinguish between images of persons authorized to enter images of intruders The proposed algorithm classifies the features of the captured image and talks about what was normal intrusive before doing the work of warning the proposed system that these algorithms improve the functionality of the system.

ALiero *et al.* [14] they aim to achieve a perception of the behavior of the elderly, using sensors based on a comprehensive assessment of negative responses based on a set of Integrated Sensor Hub sensors (ISHS), where the proposed system depends on four factors: advanced use, advanced use, perceived privacy and perceived benefit. And the years living in an elderly care center in South Korea showed negative

reactions check usability promise as the proposal indicated the need for a friend for you Reduce negative reactions and response.

Alani *et al.* [15] the researchers analyzed the smart home energy management system to determine the current trends to improve performance in the future, and the results showed the lack of quality headphones in safety and privacy, interoperability, expansion and adaptation of the population, which exposes them to health risks. The proposed system also demonstrated the possibility of providing smart homes free of energy consumption and cyber security threats.

Ammi *et al.* [16] they relied on special frameworks NETPI and BLYNK that support based on the Internet of things, smart phone applications and websites that do it providing work for the system and extracting deep learning data results. The proposed system provides flexibility in dealing with many control units applicability in home devices based on remote control.

Schomakers *et al.* [17] a proposal for a system based on the blockchain, working smart home systems, where the proposed system was designed based on a group of missing security, which is based on four layers of cloud storage and a hyper-ledger fabric, and implemented a smart home, where the system aims to set the speaker of this house design and raise the security needs rely on a needy Internet. The results showed that the proposed system is characterized by transparency, interoperability and the confidentiality of the smart home. Alfakeeh *et al.* [18] the proposed system explores various privacy aspects related to trust, using the smart home from the user's point of view, with regard to determining the level of automation and the field of application. The general use of the smart home is proposed to adapt to the needs of the user.

Manojkumar *et al.* [19] design a new model controlling complementary automation based on a machine learning model. In this model the extent of changes in the environment of the smart home adoption of the squash tree room different levels of mating where the decision tree is designed based on the possible decisions that apply the customized requirements. The elderly regardless of assistance verified using scales of assistance and delay, it is necessary to control the bridges of meters, the implementation of a comparison of the form. Oh *et al.* [20] a special automation system called HIS is designed with low cost and remote control, relying on the IoT, monitoring and controlling home appliances through the web, how much Arduino uses, technologies, connecting to Wi-Fi, the proposed system reduces power consumption by 30% of the load.

In (Desnanjaya, et al.) [21] they proposed system based on a special protocol to distinguish smart device theft and identity theft Providing mutual authentication securely relying on the weight loss protocol is happy on the Internet of things. What is the proposed system provides in performance and reduce the computational cost and is suitable to work in the environment of a smart home based on the internet of things.

Podder *et al.* [22] a security monitoring system has been established, using Raspberry Pi, ruling the system, and connecting it to many consultants, detecting things that enter the room, using the camera, as well as using sensors, degrees of love, gas, detection, status, temperature and gas concentration in the room, and the Telegram application has been adopted. Sending notifications from these devices. The proposed system is efficient in providing security, monitoring the house from thieves and intruders, as well as sending alerts about the dangers of high temperatures and detecting gas in the room.

Kumar and Chouhan [23] the proposals for a special system is called Smart AgroTech, which is based on the internet of things in the context of urban agriculture, taking into account a set of variables, including the percentage of humidity, temperature, and soil moisture. It adds reliability to the system by determining the error rate between the actual data and the data collected from the sensors and provides various improvements compared to other traditional methods.

Bhatt *et al.* [24] they proposed a secure address and authentication system based on the smart card reliance on the standard IPv6 protocol reducing security threats in the internet of things. The proposed system provides uniquely elegant and authenticated smart devices and uses a secret session key that prevents the network from unauthorized access and analysis. Informal or formal security the use of a set of tools including record of rights (ROR) prove the proposed system from the results obtained from the internet of things smart home from points and the attacks that are presented to them.

Sequeiros *et al.* [25] a balanced deep learning environment has been used. Solutions to address these three limitations. Three limitations, including the multi-objective optimization problem, the fitness function, solve the price management problem in the energy consumption that is used in heating systems, where he used methods by systems. Heating ventilation and air conditioning (HVAC) in terms of energy loss, price management and capacity, interactive use of several experiments to verify the integrity of the section system, and the results showed that the proposed system is good, except for a comparison between other communication protocols.

Murad *et al.* [26] they relied on a research model that combines the technology of pleasure and happiness motives with the unified theory of acceptance and use of technology. Providing visas for well-being. Relying on a sample consisting of 260 responses to the survey. The results are that the motive behind

the hedonistic behavior associated with some smart home services as well as the existence of a positive relationship using smart home services is well-being.

Froiz *et al.* [27] the proposed design includes many subsystems, adding a group of types of sensors, such as the passive infrared sensor, passive infrared sensor (PIR), gas sensor, soil moisture sensor, water level sensor, and temperature sensor. The proposed system relies on Bluetooth technology. The Android application controls these devices and their properties from Smart home remote control using Arduino Nuno.

Our model completely merges the automation and monitoring system based on IoT system architecture to provide reliable IoT sensing state and how to monitoring smart home with specific devices and notify home administration in case of any abnormal state. The rest of our paper is organized as shown in: In section 2, the proposed system method has been explained. Section 3, describes the proposed system results and Discussion. In section 4, concluded the used method.

2. METHOD

The applications of the internet of things are increasing on a large scale to include simple household applications for daily tasks. Does the internet of things use in the homes for the purposes of monitoring energy, determining and maintaining a certain level of it, as well as monitoring the opening and closing of doors, the high levels of smoke in the atmosphere and identification, adding many other applications that you use from home. The proposed system consists of three components, the first component is the sensors, which are responsible for the environment and are not based on the internet of things, in addition to a main node connected to these sensors, which is busy collecting gathered data valid for the final processor part. It has been illustrated in Figure 1.

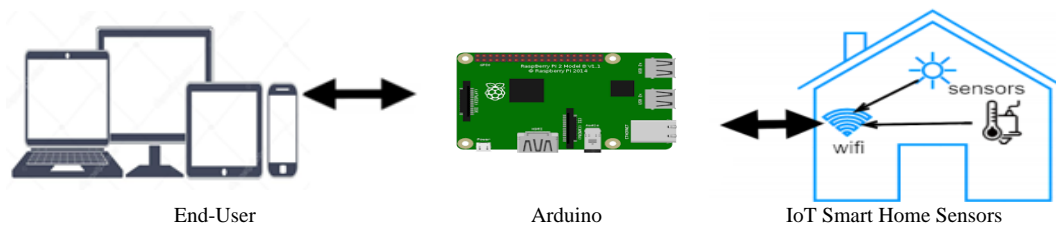


Figure 1. The proposed IoT home monitoring system illustrative diagram

The second part of the proposed system consists of the data processing process. After the data collection process, the sensors process and send it to the main node via wired and wireless communication. Translate this data and control it automatically or through the user interface through which this data is transmitted. It is through. Commonly more systems based on a special server to download the data after processing so that it can be accessed through its neck and through it and helps in the process of saving time and energy as shown in Figure 1 which shows the scheme of the proposed system.

Furthermore, Figure 2 showed the main blocks of the proposed system which it based on the IoT sensors as smart home automation elements and the network requirements components. The proposed IoT sensors are security locks, light control, and so on, which they are connected to the Arduino gateway through wifi, Bluetooth and ZigBee and the gathered data passed to the user interface through the internet, the end user used different application tools such as PC computers, mobile devices, and many others to access to the gathered data through web page link, API, and IoT App. The contribution of the proposed method is based on implementing the network topology showed below and enhanced network performance, with decrease end to end delay and network latency overall.

Besides, the Flowchart of the proposed method showed in Figure 3, as the main steps of the implementation system, from the point of beggeining gather data by IoT sensors to the steps of management data, analyis them and present the data in the graphical user interface. The main steps in Figure 3 are as shown in:

- Connect all devices with Arduino.
- Configuraing IoT sensors and setting.
- Cheacking code sussessfully and pass the request to the login page, or refuse the request.
- Network element configuration with API and widgets with starting home automation system and monitoring the sensing states.

- Checking the normal and abnormal state for each sensor reads and compared with the normal reading stored in the system if the upcoming read is within the normal rate it accepted otherwise the system inform the adminstartor about abnormal behaviour with alam notification with light and sound cases.
- Finally, the research result evaluations are passed from the IoT sensors to the specific service on computer web url with IP or address and to graphical user interface within the Mobile.

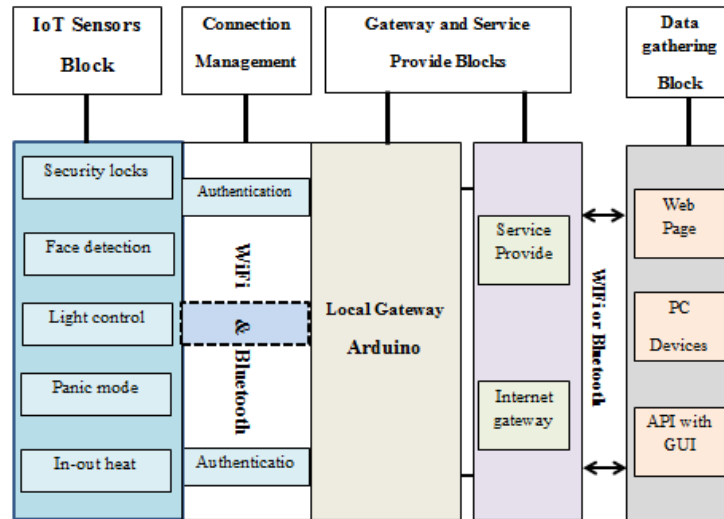


Figure 2. Block diagram of the proposed IoT based smart home automation and monitoring system

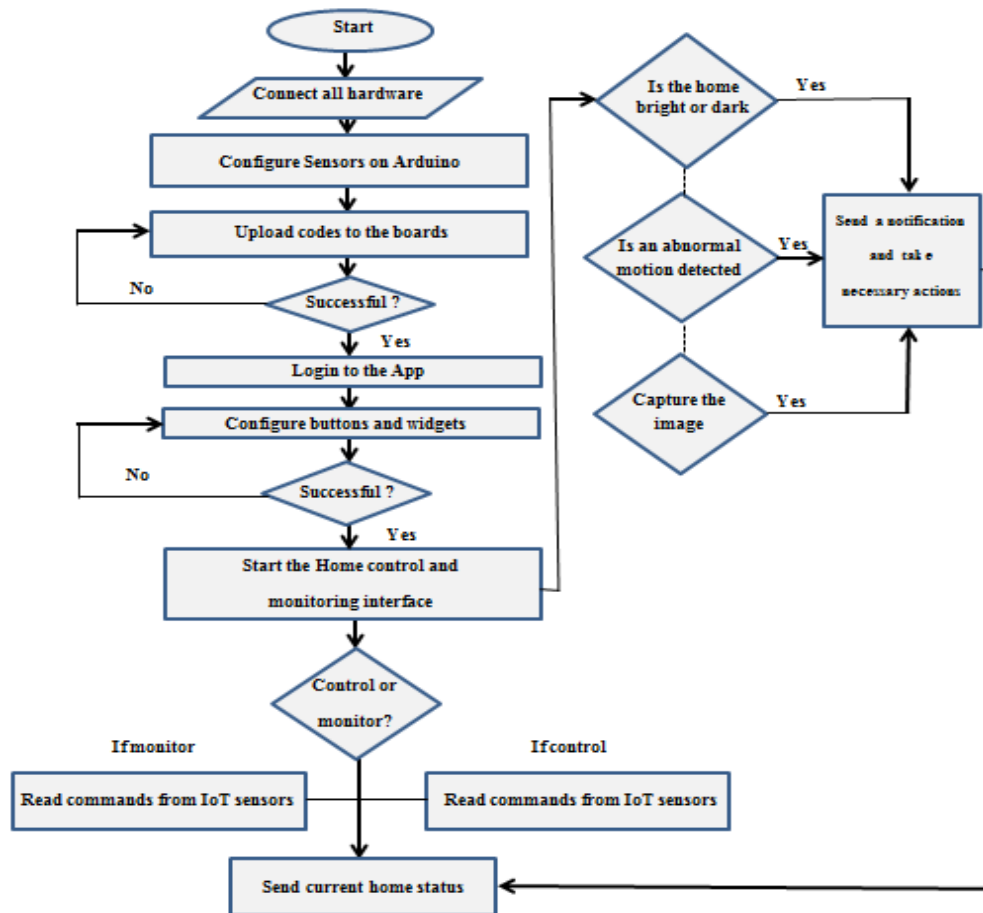


Figure 3. The proposed system flowchart

3. RESULTS AND DISCUSSION

In this section, it is explained the results of research and at the same time is given the comprehensive discussion of the proposed system case studies. The proposed system implemented with hardware side in Arduino and C# programming language. It is evaluated with network evaluation metrics as the delay, packet delivery ratio, add the results analyzed with Arduino to IoT sensor, Arduino to system administrator approaches

The mains steps of the system implementation as shown in:

- The Login page to verify the authorized user.
- The main system home page of normal state configured with remote connection public IP address
- The Abnormal sensor reads of CO about 13431 compared with normal state as less than 5000.
- Building results with the secure alarm notification system.

In addition, the proposed system discussed based on the two main case studied to recognized the normal and abnormal sensor reads where the normal state was as less than 5000 value and the distance less than 15 cm, and the abnormal state as more than 5000 and distance more than 15 cm as well as the proposed system provides the authorization to identify the legitimate and illegitimate users through cloud login page as remote access connection. The used system decrease time and delay of captured data from IoT sensors and the data logged to the central Arduino are recorded and displayed over time through a data-viewing dashboard in the specific tool, and flexibility of the data displayed for the user on a app that was designed for this purpose. Besides, it decreases computation power (RAM, CPU usages and execution time). Alongside, the proposed method is expected to detect intruders by identifying the people who are authorized or not authorized to enter the system, through verification tools in IoT sensors, and pre-protection by avoiding disasters when gas leakage or fire breaks out in time. The normal of distance is less 15 cm and it depends on the radio frequency identification (RFID) if it isn't correct and distance more than 15 cm as explained in Table 1.

Table 1. The results of the proposed system

Sensor Reading	Distance	Smoke	Co	LPG
Normal	16	22	20	46
Abnormal	20	13402	7301	5102
	27	10211	6256	5097

There are differernt evaluation metrics used in the proposed system as shown in:

- Network latency is the time it takes for data or a request to go from the source to the destination. Latency in networks is measured in milliseconds [28].
- Packet delivery ratio (PDR): This network performance metric is defined as the ratio between the number of data packets successfully delivered to the destination and the number of packets transmitted by the source [29].
- The delay time is the time used to transmit packet from the sender IoT to the receiver Arduino and it explains the delay time of data traffic in simulation environment for entire packets [29].

Furthermore, the proposed system is based on real data transmission for data exchanges between Arduino and IoT sensors, it showed better latency time as it provides 0.0012 seconds for alarm notification exchanged data from the Arduino to the system administration as the minimum average latency. Alongside, the Arduino node can greatly reduce the delay since it is located near IoT devices and it controlled on all data generated by sensors, Table 2 showed the latency of the proposed environment. In addition. data traffic delay and packet delivery ratio are listed in Table 3, for some range in meter between Arduino and system administrator. Figure 4 shows the chart for some range to calculate the traffic delay and packet delivery ratio for the main network elements as Arduino and IoT sensors for secure smart home automation.

Table 2. Network latency

Sensor reading	Distance in cm	Connection type	Avg. latency (s)
Arduino to IoT sensor	100	Wire	0.0018 Seconds
Arduino to System Administrator	500	Wireless	0.0012 Seconds

Table 3. The main results for traffic delay and packet delivery ratio (PDR)

Range in meter	Avg. delay	Packet delivery ratio
< 10	2 ms	100%
10 - 40	2.8 ms	99%
40 - 60	3.4 ms	98.7%

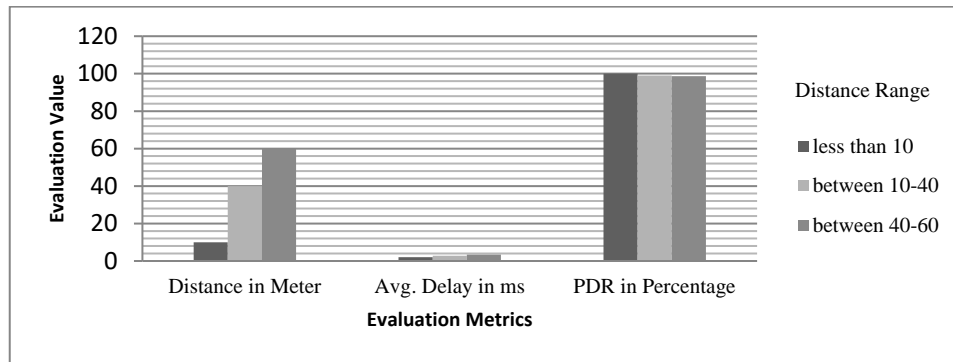


Figure 4. The used evaluation of range distance, traffic delay and PDR

4. CONCLUSION

The issue of providing security in smart home systems is one of the most important issues that have attracted the attention of researchers, as a result of the diversity of attacks, the increase in the amount of data generated by sensors in these applications, and therefore it has become necessary to develop a system that has the ability to deal with the amount of large data, its sensitivity and the type of data and the origin of alerts to the network administrator about the conduct of the sensor inside this network. The proposed system has proven through experience its ability to analyze the legitimate user from the malicious user, depending on the login interface, where this interface distinguishes the authorized person from the unauthorized one and after logging in remotely through a special link equipped with the remote connection service via cloud public IP (<http://176.223.140.119:1003/>), where it allows access to sensors, that was installed in a smart home environment. Which they used for IoT measurements such as the distance, gas, nature of the liquid and smoking. The normal reading can be distinguished from the abnormal readings of these sensors, where the proposed system sends an audio alert message when the values exceed the nature as well as and it recognized the possibility of unauthorized access to use the card identification (ID) with RFID, as the proposed system prevents bypassing the identity to theft or unauthorized opened the door. The results show that the sensor normal reading for distance 16 cm, smoke as 22, CO as 20 LPG as 46, while the Abnormal as 20, 13402, 7301, and 5102 for the first abnormal state and 27, 10211, 6256, 5097 respectively. Network delay and data traffic latency was enhanced in the proposed system for compared data in wireless IoT sensors.




REFERENCES

- [1] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, p. 101728, Mar. 2020, doi: 10.1016/j.scs.2019.101728.
- [2] F. Del Rio, and K. E. Makuch, "Critically reviewing smart home technology applications and business models in Europe," *Energy policy*, vol. 144, p. 111631, 2020, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0301421520303669?via%3Dihub>.
- [3] W. Li, T. Yigitcanlar, I. Erol, and A. Liu, "Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework," *Energy Research & Social Science*, vol. 80, p. 102211, Oct. 2021, doi: 10.1016/j.erss.2021.102211.
- [4] K. Sovacool. B and F. Del Rio, "Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies," *Renewable and sustainable energy reviews*, vol. 120, p. 109663, 2020, [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1364032119308688?via%3Dihub>.
- [5] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.
- [6] A. M. C. Drăgulinescu, A. F. Manea, O. Fratu, and A. Drăgulinescu, "LoRa-based medical IoT system architecture and testbed," *Wireless Personal Communications*, Mar. 2020, doi: 10.1007/s11277-020-07235-z.
- [7] T. Chaurasia and P. K. Jain, "Enhanced smart home automation system based on internet of things," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Dec. 2019, pp. 709–713, doi: 10.1109/I-SMAC47947.2019.9032685.
- [8] M. Domb, "Smart home systems based on internet of things," in *IoT and Smart Home Automation [Working Title]*, *IntechOpen*, 2019, pp. 444–448.
- [9] 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, p. 4932, Jul. 2021, doi: 10.3390/s21144932.
- [10] C. Stolojescu-Crisan, C. Crisan, and B. P. Butunoi, "An iot-based smart home automation system," *Sensors*, vol. 21, no. 11, p. 3784, May 2021, doi: 10.3390/s21113784.
- [11] S. F. Islam, M. I. Hasan, M. Akter, and M. S. Uddin, "Implementation and analysis of an IoT-based home automation framework," *Journal of Computer and Communications*, vol. 09, no. 03, pp. 143–157, 2021, doi: 10.4236/jcc.2021.93011.
- [12] O. Taiwo and A. E. Ezugwu, "Internet of things-based intelligent smart home control system," *Security and Communication Networks*, vol. 2021, pp. 1–17, Sep. 2021, doi: 10.1155/2021/9928254.




- [13] T. H. Jo, J. H. Ma, and S. H. Cha, "Elderly perception on the internet of things-based integrated smart-home system," *Sensors*, vol. 21, no. 4, p. 1284, Feb. 2021, doi: 10.3390/s21041284.
- [14] M. S. Aliero, K. N. Qureshi, M. F. Pasha, and G. Jeon, "Smart home energy management systems in internet of things networks for green cities demands and services," *Environmental Technology & Innovation*, vol. 22, p. 101443, May 2021, doi: 10.1016/j.eti.2021.101443.
- [15] S. Alani, S. N. Mahmood, S. Z. Attaallah, H. S. Mhmood, Z. A. Khudhur, and A. A. Dhannoon, "IoT based implemented comparison analysis of two well-known network platforms for smart home automation," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 1, p. 442, Feb. 2021, doi: 10.11591/ijece.v11i1.pp442-450.
- [16] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Information Processing and Management*, vol. 58, no. 3, 2021, doi: 10.1016/j.ipm.2020.102482.
- [17] E.-M. Schomakers, H. Biermann, and M. Ziefle, "Users' Preferences for smart home automation – investigating aspects of privacy and trust," *Telematics and Informatics*, vol. 64, p. 101689, Nov. 2021, doi: 10.1016/j.tele.2021.101689.
- [18] A. S. Alfakeeh, M. A. Alqarni, K. H. Alyoubi, and S. H. Chauhdary, "A complementary automation control for Internet of Things-based smart home assistance for elder adults," *Personal and Ubiquitous Computing*, May 2021, doi: 10.1007/s00779-021-01575-8.
- [19] P. Manojkumar *et al.*, "A novel home automation distributed server management system using internet of things," *International Journal of Ambient Energy*, pp. 1–6, Jul. 2021, doi: 10.1080/01430750.2021.1953590.
- [20] 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, p. 1488, Feb. 2021, doi: 10.3390/s21041488.
- [21] I. G. M. N. Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 3, pp. 1295–1302, Jun. 2021, doi: 10.11591/ijeecs.v22.i3.pp1295-1302.
- [22] A. K. Podder *et al.*, "IoT based smart agrotech system for verification of Urban farming parameters," *Microprocessors and Microsystems*, vol. 82, p. 104025, Apr. 2021, doi: 10.1016/j.micpro.2021.104025.
- [23] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Networking and Applications*, vol. 14, no. 1, pp. 420–438, Jan. 2021, doi: 10.1007/s12083-020-00973-8.
- [24] D. Bhatt, D. Danalakshmi, A. Hariharasudan, M. Lis, and M. Grabowska, "Forecasting of energy demands for smart home applications," *Energies*, vol. 14, no. 4, p. 1045, Feb. 2021, doi: 10.3390/en14041045.
- [25] H. Sequeiros, T. Oliveira, and M. A. Thomas, "The impact of IoT smart home services on psychological well-being," *Information Systems Frontiers*, Mar. 2021, doi: 10.1007/s10796-021-10118-8.
- [26] M. Murad, O. Bayat, and H. M. Marhoon, "Design and implementation of a smart home system with two levels of security based on IoT technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, p. 546, Jan. 2021, doi: 10.11591/ijeecs.v21.i1.pp546-557.
- [27] I. F. Míguez, T. F. Caramés, P. F. 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*, vol. 18, no. 8, p. 2660, Aug. 2018, doi: 10.3390/s18082660.
- [28] M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs)," *Proceedings - IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Networks, MSN 2013*, pp. 324–329, 2013, doi: 10.1109/MSN.2013.74.
- [29] X. Xiang *et al.*, "Delay and energy-efficient data collection scheme-based matrix filling theory for dynamic traffic IoT," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 168, Dec. 2019, doi: 10.1186/s13638-019-1490-5.

BIOGRAPHIES OF AUTHORS



Mohamed Khudhair Al-Gburi    was born in Baghdad-Iraq. He received a B.Sc. degree in Electronic and Communication Engineering from the University of Technology in 2007 and an MSc degree in communications engineering from the international University of KAI for technology and research in 2017, Russia. He is working as a lecturer at the information network department/College of Information Technology at the University of Babylon. He is currently working on his Ph.D. degree in the communication field in the Department of Electrical/College of Engineering at the University of Babylon. His research interests include signal processing, cloud computing, IoT, information security, Massive MIMO. He can be contacted at email: mohamed.algburi@uobabylon.edu.iq.



Laith Ali Abdul-Rahaim    currently works at the Department of Electrical Engineering, University of Babylon. He received a Ph.D. degree in electrical engineering from the University of Technology in Iraq. He researches in digital communication systems design, information science, communication security, and reliability. Now he has a prof. degree in wireless communication. His current project is interested in smart system design, and wireless communications. He can be contacted at email: drlaithanzy@uobabylon.edu.iq.