Jana Publication & Research

Design and Simulation of IoT-Based Intelligent Home Automation Systems Using MATLAB Simulink and Python Inte...

27

BioTech

Institut Seni Indonesia Surakarta

Document Details

Submission ID

trn:oid:::1:3220681054

Submission Date

Apr 18, 2025, 1:39 PM GMT+7

Download Date

Apr 18, 2025, 4:04 PM GMT+7

File Name

IJAR-51114.docx

File Size

3.2 MB

14 Pages

3,506 Words

20,198 Characters

9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

16 Not Cited or Quoted 9%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

4% Internet sources
3% Publications
6% Submitted works (Student Papers)

Match Groups

- **16** Not Cited or Quoted 9%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

4%	Internet sources
3%	Publications
6%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	Jabatan Pendidikan Politeknik Dan Kolej Komuniti	2%
2	Student papers	Middle East College of Information Technology	2%
3	Student papers	Swinburne University of Technology	<1%
4	Student papers	University of Greenwich	<1%
5	Student papers	Berlin School of Business and Innovation	<1%
6	Internet	dokumen.pub	<1%
7	Internet	opus.lib.uts.edu.au	<1%
8	Publication	"Reuse in the Big Data Era", Springer Science and Business Media LLC, 2019	<1%
9	Student papers	Instituto PolitÃ©cnico de BraganÃ§a	<1%
10	Publication	Shrikaant Kulkarni, P. William. "Advances in AI for Cloud, Edge, and Mobile Comp...	<1%

11 Internet

libweb.kpfu.ru <1%

12 Internet

www.msit.in <1%

13 Publication

A. A. Zaidan, B. B. Zaidan, M. Y. Qahtan, O. S. Albahri et al. "A survey on communic... <1%

14 Publication

Arya Yudidharma, Nicholas Nathaniel, Tang Nyquel Gimli, Said Achmad, Aditya K... <1%

15 Publication

V. Santhi, Yamala N. V. Sai Sabareesh, Ponnada Prem Sudheer, Villuri Poorna Sai K... <1%

Design and Simulation of IoT-Based Intelligent Home Automation Systems Using MATLAB Simulink and Python Integration

Abstract

The idea of "smart homes" has been completely transformed by the Internet of Things' (IoT) rapidly expanding technological capabilities, which allow for seamless automation and remote device control. Because of Python's strong and versatile programming features, this thesis discusses the design and simulation of IoT frameworks and device communication in a smart home setting. The suggested system incorporates a number of simulated Internet of Things (IoT) devices, including security cameras, smart lights, and thermostats. These devices use the MQTT (Message Queuing Telemetry Transport) protocol to connect with one another through a centralized message broker. The simulation demonstrates how various smart home components interact by simulating real-time communication between devices and a central controller using Python and the Paho MQTT module. Every gadget is represented as a MQTT client that reacts to simulated environmental changes and publishes status updates on a regular basis. Dynamic monitoring and control are made possible by the central controller, which processes incoming messages and subscribes to the device topics. The study simulates realistic smart home situations including automatic lighting, temperature control, and motion detection while highlighting the architectural concepts underlying effective communication, scalability, and security in IoT networks. This study advances knowledge about Internet of Things frameworks and how they may be used to improve the comfort, security, and energy efficiency of smart homes. It also lays the groundwork for future efforts to integrate more IoT protocols, cloud services, and sophisticated machine learning methods for predictive automation.

Keywords: MQTT, IoT, light, wifi, automatic

1. Introduction

The Internet of Things (IoT) and the concept of a "smart home" have revolutionized how we use our living areas and interact with them. Smart camera entry point security to thermostat management and automation are just a few of the chores that homeowners can automate and remotely monitor by integrating IoT-enabled devices. The improvements in energy efficiency, security, and general quality of life that come with these technological developments go beyond convenience. An indication of the growing need for intelligent, networked devices that interact with ease is the growing popularity of "smart homes." IoT frameworks provide the infrastructure required for automation, data exchange, and device communication, making them the core of smart home systems. These frameworks enable communication between a variety of devices and central controllers, including cameras, thermostats, and smart lighting. But creating a secure, scalable, and effective IoT infrastructure is not without its difficulties. In addition to responding to user inputs, devices need to be able to manage a variety of network situations, ensure data security, and communicate across dependable communication protocols.In this thesis, we investigate how to use Python to simulate and create Internet of Things frameworks and device communication in a smart home setting. Python is used because it is easy to understand, has a large library, and speeds up the creation of Internet of Things solutions. The MQTT (Message Queuing Telemetry Transport) protocol, a lightweight messaging protocol ideal for Internet of Things applications because of its low bandwidth consumption, scalability, and real-time communication capabilities, is at the heart of this study. In this study, an ecosystem of smart homes with several devices interacting with a central controller—like security cameras, smart lights, and thermostats—is simulated. We showcase how these devices can perform automatic tasks, share data, and react to changes in the environment through the simulation of real-world events. Beyond that, the study explores the fundamentals of IoT communication, tackling issues like security, scalability, and interoperability. Using IoT frameworks and devices in a smart home setting entails virtualizing gadgets such as security cameras, smart lights, and thermostats and integrating them with a framework that can manage control and communication. Typically, protocols like MQTT, HTTP, or CoAP are used.

8

2. Overview of the Primary Objective

14

The main goal of this thesis is to create and model an Internet of Things (IoT) framework for smart homes using Python. This framework will allow for efficient communication between various simulated devices, including security cameras, smart lights, and thermostats. The framework will address important issues including scalability, security, and data transmission while demonstrating real-time interaction, automation, and control using the MQTT protocol. The purpose of this simulation is to improve knowledge of IoT systems in smart homes and lay the groundwork for upcoming developments in IoT technology.

Aims:

Utilizing essential IoT protocols and libraries, the goal is to use Python to create IoT frameworks and set up effective device communication in smart home settings, guaranteeing scalability, security, and smooth IoT device integration.

3. Literature Review

13

Python has become a popular choice for the development of IoT-based smart home systems due to its ease of use, abundance of libraries, and robust community. Important IoT frameworks like MQTT, CoAP, and REST APIs facilitate device communication, allowing for the smooth integration of smart home devices like sensors, actuators, and controllers. Additionally, Python-based IoT frameworks improve data analytics, cloud integration, and edge computing, addressing issues like scalability, interoperability, and network constraints. All things considered, Python remains a useful tool for creating scalable, secure, and effective smart home IoT.

4. Python IoT Device Simulation

Here, we use MQTT to imitate a security camera, a thermostat, and a smart light.

I. Device: Smart Light

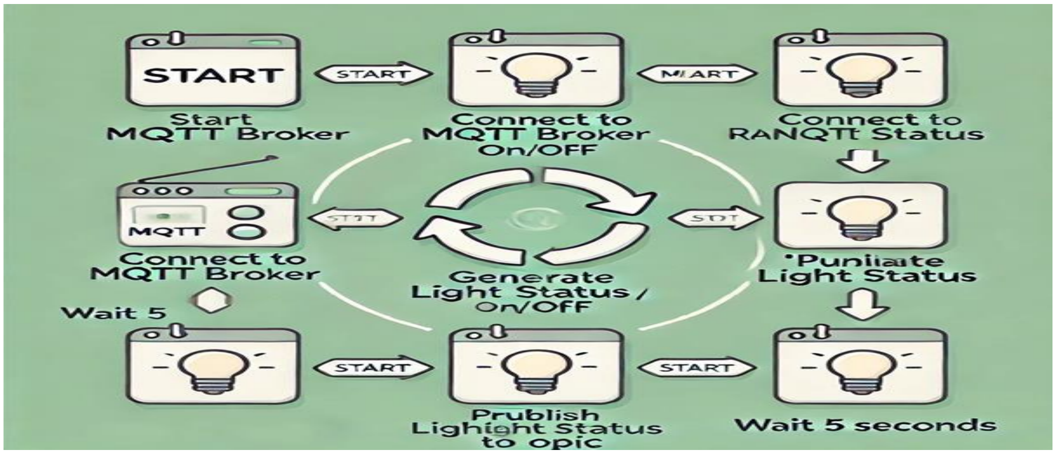


Fig 1 : Smart Light

```
while True:

    # Randomly turn the light on or off

    light_status = random.choice(["ON", "OFF"])

    client.publish(TOPIC, light_status)

    print(f"Light status: {light_status}")

    time.sleep(5)  # Update every 5 seconds

      simulate light()
```

9

II. The Smart Thermostat

12 15

A smart thermostat is a networked gadget that uses Internet of Things (IoT) technology to regulate the temperature in a house or building. Frequently using smartphone apps or voice assistants like Alexa or Google Assistant, it modifies the heating and cooling systems according to user preferences, schedule, or outside factors like the weather. By learning from user behavior, smart thermostats optimize energy use to lower energy consumption and increase comfort, which lowers costs and promotes environmental efficiency.

```
while True:

    # Randomly set a temperature between 18°C and 24°C

    temperature = round(random.uniform(18.0, 24.0), 1)

    client.publish(TOPIC, f"Temperature: {temperature}°C")

    print(f"Thermostat: {temperature}°C")
```

3

```
    time.sleep(10)  # Update every 10 seconds
```

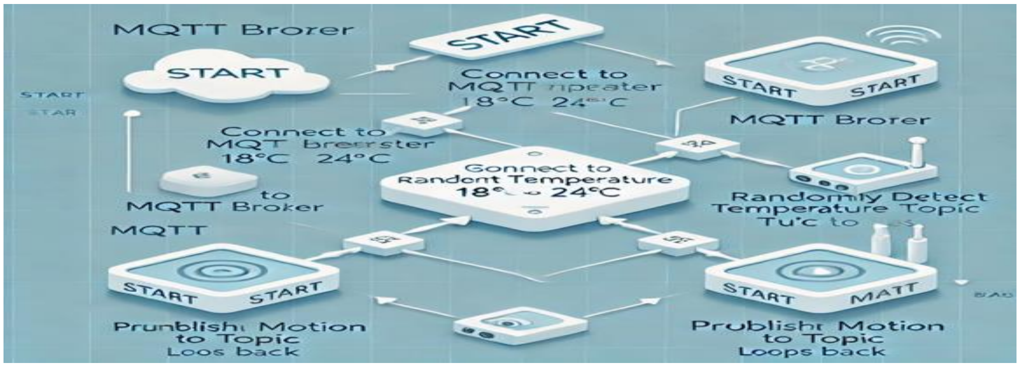


Fig 2: The Smart Thermostat

```
  while True:
    # Randomly detect motion or not
    motion_detected = random.choice([True, False])
    client.publish(TOPIC, f"Motion detected: {motion_detected}")
    print(f"Camera motion status: {motion_detected}")
    time.sleep(15) # Update every 15 seconds

simulate_camera()
```

III. Subscription-based Central Controller

A Subscription-based With access granted via a subscription model, a central device or system known as a "Central Controller" oversees and regulates a network's numerous IoT devices. Using a cloud-based platform or mobile app, this controller integrates various IoT devices (like lights, thermostats, and security systems) and enables users to monitor, automate, and control them. Advanced features, remote access, and cloud storage frequently require a subscription fee. Constant upgrades, scalability, and improved functionality are guaranteed by this approach, which usually provides customized services like sophisticated analytics, third-party system integration, and wider device compatibility.
All devices are subscribed to by the central controller, which also logs the messages.

```
def setup_controller():
  client = mqtt.Client("Smart_Home_Controller")
  client.on_message = on_message
  client.connect(BROKER)
  client.subscribe(TOPICS)
   client.loop_forever()
    setup_controller()
```

IV. Relay Control

Relay control is the process of regulating the electrical power flow in a circuit by means of an electromechanical relay. Relays are electrical switches that respond to outside impulses by opening or closing circuits. The relay's coil produces a magnetic field when a tiny control voltage is provided, which activates a set of contacts that either complete or break the circuit, permitting or prohibiting the passage of electricity.

3.1 Key An. Explanation

Modeling apparatuses:

1. The thermostat, light, and camera are all simulated devices that connect to the localhost MQTT broker.
2. The gadgets provide status reports on the subjects they are related to.
3. Updates are released on a regular basis (5 to 15 seconds) in order to replicate real-world activity.

3.1.1. Controller Central

1. Subscribes from the devices to various topics.
2. Replicating a smart home hub that keeps an eye on every gadget, it logs the messages it receives.

3.1.2. Diagram

This diagram shows an Internet of Things (IoT) smart home setup with a MQTT broker, a central controller, and smart lights, thermostats, and security cameras. The communication channel between the devices and the central hub is depicted in the diagram.

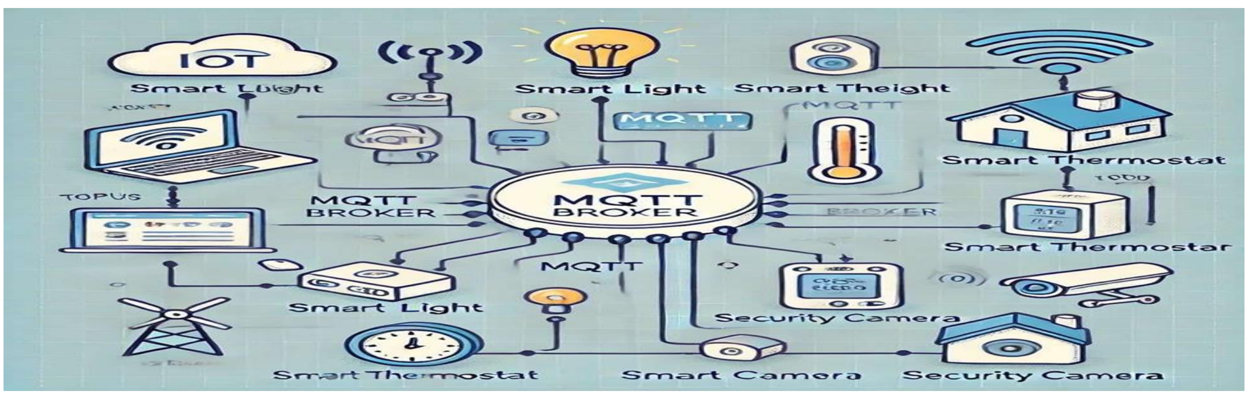


Fig 4: IoT-Diagram

3.1.3. Circuit

However, the following kinds of circuits and parts could be utilized in actual smart home system implementations:

Microcontrollers (such as the ESP8266, ESP32, and Arduino): These devices operate as the main control units for numerous IoT devices, such smart lighting, thermostats, or sensors.

3.2. ESP8266

Espressif Systems manufactures the ESP8266, a system-on-a-chip (SOC) Wi-Fi microprocessor for Internet of Things (IoT) applications. The ESP8266 is currently widely utilized in many Internet of Things devices due to its low cost, small size, and versatility with embedded devices.

3.2.1. ESP32

The ESP32 is a semiconductor that gives embedded devices, or Internet of Things devices, Wi-Fi and (in certain models) Bluetooth connectivity. Although ESP32 is only the chip, the manufacturer also frequently refers to the development boards and modules that contain this chip as "ESP32."

3.2.2. Arduino

Robots, home automation, sensing, and data collection are just a few applications for Arduino circuits. We'll be learning how to construct a basic circuit using an LED (light-emitting diode) and a button in this intractable.

I. Weaknesses

Several vulnerabilities can occur while using Python to create IoT frameworks and device interactions in smart home setups. The following is a condensed list of possible flaws:

Vulnerabilities in Security:

1. Insufficient encryption is used when sending data.
2. Inadequate methods of device authentication.
3. Possibility of illegal entry and device control.

Compatibility Concerns:

1. Communication between devices made by different manufacturers may be hampered by the absence of standard protocols.
2. Merging older technology with newer ones is difficult.

Challenges with Scalability:

1. As the number of devices rises, performance can suffer.
2. When there is a high device density, network congestion may happen.

Issues with Dependability:

1. Reliance on dependable internet access.
2. In the absence of reliable failover methods, devices may malfunction or fall down.

Challenges related to User Experience:

1. User interface complexity may discourage efficient use.
2. Inconsistent management and monitoring features.

Energy Use:

1. Devices that run on batteries could have problems with power management.
2. Constant connectivity may result in increased energy use.

Upkeep & Updates:

1. Distributing updates to field-based equipment might be challenging.

2. Possibility of interruptions when performing maintenance.

II. Data Table:

Element	Synopsis	Methods	Factors
Device Level,	Data transfer and messaging between devices	MQTT, Web Sockets, Zigbee, LoRa	Power consumption and device compatibility
Layer of Communication	Data transfer and messaging between devices	MQTT, Web Sockets, Zigbee, LoRa	Bandwidth, latency, reliability
Layer of the Gateway	Connects nearby gadgets to the web	HTTP, REST, WebSockets	Security (firewalls, VPNs), data aggregation
Layer of Data Processing	Storing and analyzing data	SQL, NoSQL, InfluxDB	Policies for data retention and scalability
Level of Application	User interfaces for mobile and online apps	Django, React Native, and Flask	Response time and user experience

III. Math Equation

Let's apply some of the previously covered mathematical ideas to a real-world case. To demonstrate how to determine data transfer rate, energy usage, and storage needs, we'll set up a scenario.

Situation
Assume the following specifications for a smart home environment are met:

Data Size: A data packet of size $D = 256$ D = 256 bits is sent by each smart device.
Transmission Time: A single packet takes $T = 0.1$ T = 0.1 seconds to transmit.
Power Consumption: An apparatus uses 2 P = 2 Watts of power to run and transmits data for 60 t = 60 seconds every hour.
A total of $N = 1440$ N = 1440 data points (one every minute for 24 hours) are generated by the device's minutely data transmissions during the course of a day.

Calculations

1. Data Transmission Rate (R)
   Applying the equation:

   $$R=\frac{D}{T}$$

   $$R=\frac{256 \text{ bitS}}{\mathbf{0.1} \text{ se}} = 2560 \text{ bits per second}$$

2. Energy Usage (E) Applying the following formula:

   E= P×t = $E \times t$, where $t = 60$ t = 60 seconds:

   60 seconds × 2 Watts = 120 Joules
   E = 2 W × 60 s = 120 joules
   Given that this is carried out once every hour, the total energy used in a day (24 hours) would be:

120 joules per hour multiplied by 24 hours equals 2880 joules.
E total = 120 hours/hour × 24 hours = 2880 hours

3. Needs for Data Storage (S)
Applying the equation:

$$S = N \times D$$

Since one byte equals eight bits, start by converting *D*
D from bits to bytes:

$$D = \frac{256 \text{ bitS}}{8} = 32 \text{ bytes}$$

Next, figure out the overall storage:

S = 1440 data points × 32 bytes = 46080 bytes ≈ 45 KB

IV. Matlab Simulink

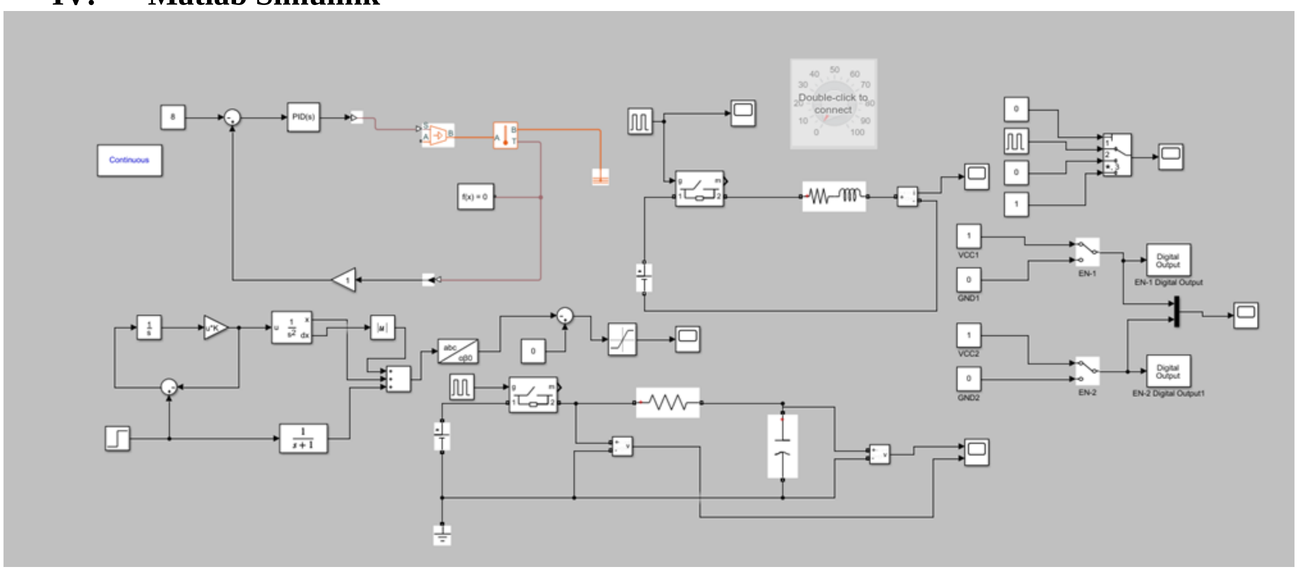


Fig 5 : Overall Model

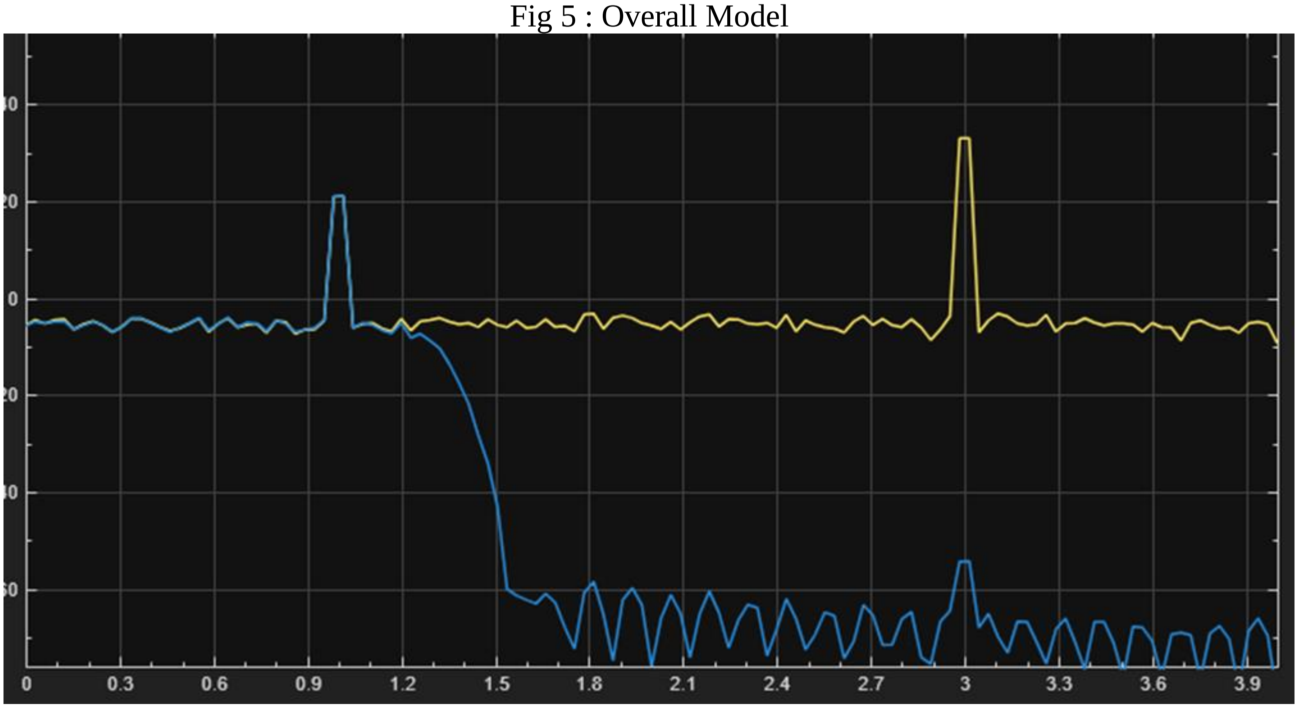


Fig 6 : Temperature Sensor1

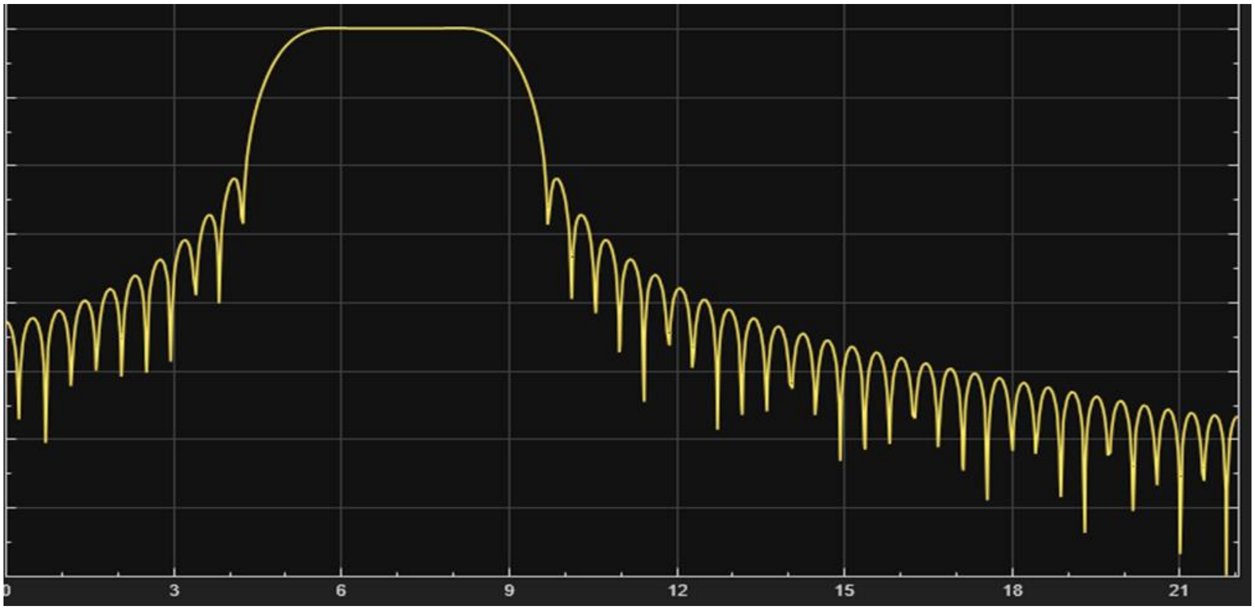


Fig 7: Temperature Sensor2

```
Thermostat: 21.3°C
Thermostat: 19.8°C
Thermostat: 23.5°C
Thermostat: 20.0°C
...
```

Fig 8: Switch Control1

```
Published: {'temperature': 24, 'humidity': 60}
Relay OFF
Published: {'temperature': 26, 'humidity': 58}
Relay ON
Published: {'temperature': 24, 'humidity': 62}
Relay OFF
...
```

Fig 9 : Switch Control2

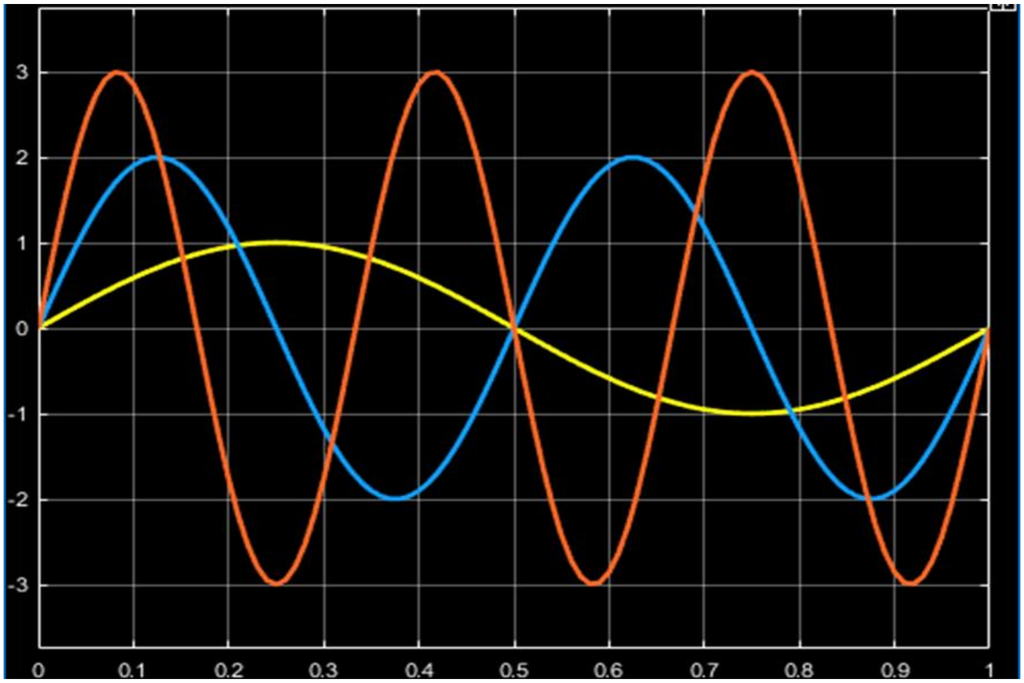


Fig 10: Output Display

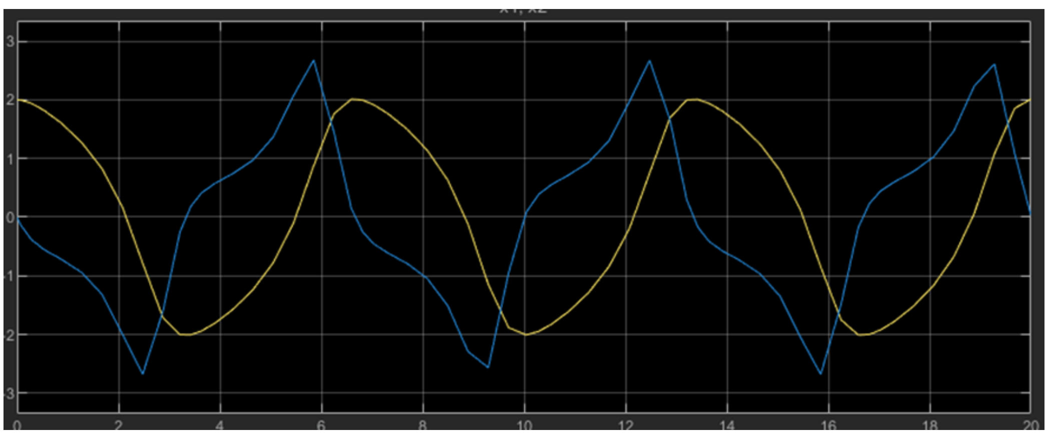
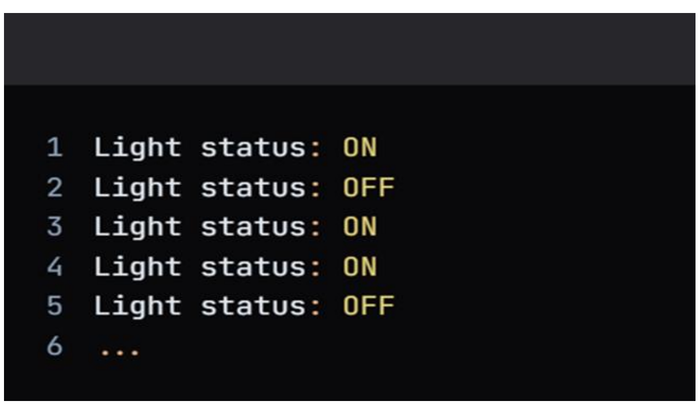


Fig 11 : Smart Light output



```
Light status: ON
Light status: OFF
Light status: ON
Light status: ON
Light status: OFF
...
```

Fig 12: Relay Controller

4. Summary

A central controller and multiple Internet of Things devices allow you to replicate a basic smart house. Real-time updates and commands are made possible via the MQTT broker, which simplifies communication between all devices. This system can be expanded by including additional devices or more sophisticated interactions, such as receiving commands to turn gadgets on or off. This provides you with a code-driven, fully complete smart home IoT framework simulation.

5. Future Suggestion

10 IoT frameworks and device connectivity in smart home environments have a lot of room to grow and innovate in the future. As technology develops further, we may anticipate that advances in machine learning and artificial intelligence will make it possible for systems to learn user preferences and optimize energy use on their own. This will lead to more intelligent automation and predictive analytics. Furthermore, resolving the growing concerns around data protection and privacy will depend on the development of stronger security mechanisms. The responsiveness of 11 smart devices can be improved by increasing the use of edge computing, which can lower latency and boost real-time processing capabilities. Furthermore, promoting cooperation between manufacturers and other relevant parties to develop global standards will guarantee improved interoperability and streamline user experiences in a variety of ecosystems. Future smart homes will become even more integrated, effective, and user-friendly by adopting these innovations, making daily life a seamless experience.

6. Conclusion

Python-based IoT frameworks and device communication for smart home environments lay the groundwork for connected and effective living environments. Standardized protocols guarantee interoperability across many systems, and a modular architecture facilitates scaling and the simple integration of new devices. Along with efficient data administration that permits perceptive analysis and automation, strong security measures are necessary to safeguard user data and foster confidence. Encouraging user-centric design improves usability by creating intuitive interfaces, while emphasizing energy efficiency encourages sustainable gadget operation. When combined, these components support creative smart home solutions that greatly enhance users' convenience and quality of life.

References

[1] Serna, M. Á., Sreenan, C. J., & Fedor, S. (2015, April). A visual programming framework for wireless sensor networks in smart home applications. In 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) (pp. 1-6). IEEE.

[2] Khoa, T. A., Nhu, L. M. B., Son, H. H., Trong, N. M., Phuc, C. H., Phuong, N. T. H., ... & Duc, D. N. M. (2020). Designing efficient smart home management with IoT smart lighting: a case study. Wireless communications and mobile computing, 2020(1), 8896637.

[3] Hoque, M. A., & Davidson, C. (2019). Design and implementation of an IoT-based smart home security system. International Journal of Networked and Distributed Computing, 7(2), 85-92.

[4] Jabbar, W. A., Kian, T. K., Ramli, R. M., Zubir, S. N., Zamrizaman, N. S., Balfaqih, M., ... & Alharbi, S. (2019). Design and fabrication of smart home with internet of things enabled automation system. IEEE access, 7, 144059-144074.

[5] Kalin, J. H. (2017). Simulating IoT Frameworks and Devices in the Smart Home (Doctoral dissertation, Virginia Tech).

[6] Froiz-Míguez, I., Fernández-Caramés, T. M., Fraga-Lamas, P., & Castedo, L. (2018). Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes. Sensors, 18(8), 2660.

[7] Iqbal, A., Ullah, F., Anwar, H., Kwak, K. S., Imran, M., Jamal, W., & ur Rahman, A. (2018). Interoperable Internet-of-Things platform for smart home system using Web-of-Objects and cloud. Sustainable Cities and Society, 38, 636-646.

[8] Pillai, M. M. (2023). A user level security framework for IoT in the smart home (Doctoral dissertation, North-West University (South Africa).).

[9] Bashir, M. R., & Gill, A. Q. (2016, December). Towards an IoT big data analytics framework: smart buildings systems. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1325-1332). IEEE.

[10] Anvekar, R. G., & Banakar, R. M. (2017, April). IoT application development: Home security system. In 2017 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR) (pp. 68-72). IEEE.

[11] Nobakht, M., Sivaraman, V., & Boreli, R. (2016, August). A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow. In 2016 11th International conference on availability, reliability and security (ARES) (pp. 147-156). IEEE.

[12] Costa, L., Barros, J. P., & Tavares, M. (2019). Vulnerabilities in IoT devices for smart home environment. In Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019. (Vol. 1, pp. 615-622). SciTePress.

[13] Duong, L. (2023). The techniques of IoT and it's applications for smart homes: internet of things techniques and standards for building smart homes.

[14] Torad, M. A., Bouallegue, B., & Ahmed, A. M. (2022). A voice controlled smart home automation system using artificial intelligent and internet of things. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(4), 808-816.

[15] Bianchi, V., Bassoli, M., Lombardo, G., Fornacciari, P., Mordonini, M., & De Munari, I. (2019). IoT wearable sensor and deep learning: An integrated approach for personalized human

activity recognition in a smart home environment. IEEE Internet of Things Journal, 6(5), 8553-8562.

[16] OConnor, T. J., Mohamed, R., Miettinen, M., Enck, W., Reaves, B., & Sadeghi, A. R. (2019, May). HomeSnitch: Behavior transparency and control for smart home IoT devices. In Proceedings of the 12th conference on security and privacy in wireless and mobile networks (pp. 128-138).

[17] Nasir, M., Muhammad, K., Ullah, A., Ahmad, J., Baik, S. W., & Sajjad, M. (2022). Enabling automation and edge intelligence over resource constraint IoT devices for smart home. Neurocomputing, 491, 494-506.

[18] Singh, M., & Dhablia, A. (2023). Smart Home Automation using IoT: Prototyping and Integration of Home Devices. Research Journal of Computer Systems and Engineering, 4(2), 130-143.

[19] Cornetta, G., & Touhafi, A. (2021). Design and evaluation of a new machine learning framework for IoT and embedded devices. Electronics, 10(5), 600.

[20] Marin, M. C., Cerutti, M., Batista, S., & Brambilla, M. (2024, January). A Multi-Protocol IoT Platform for Enhanced Interoperability and Standardization in Smart Home. In 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC) (pp. 1-6). IEEE.

[21] Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). IoT big data analytics for smart homes with fog and cloud computing. Future Generation Computer Systems, 91, 563-573.

[22] Uddin, M. Z. (2024). Machine Learning and Python for Human Behavior, Emotion, and Health Status Analysis. CRC Press.

[23] Gladence, L. M., Anu, V. M., Rathna, R., & Brumancia, E. (2020). Recommender system for home automation using IoT and artificial intelligence. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[24] Al-Shaboti, M., Welch, I., Chen, A., & Mahmood, M. A. (2018, May). Towards secure smart home IoT: Manufacturer and user network access control framework. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 892-899). IEEE.

[25] Mohanta, B., & Mohanta, H. C. (2020). Internet of things enables smart home security issue address using blockchain. Sodha Sarita Journal, 7(28), 147-153.

[26] Bui, H. D., & Chong, N. Y. (2018, September). An integrated approach to human-robot-smart environment interaction interface for ambient assisted living. In 2018 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO) (pp. 32-37). IEEE.

[27] Gunge, V. S., & Yalagi, P. S. (2016). Smart home automation: a literature review. International Journal of Computer Applications, 975(8887-8891).

[28] Nazir, S., Poorun, Y., & Kaleem, M. (2021, October). Person detection with deep learning and IOT for Smart Home Security on Amazon Cloud. In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-6). IEEE.

[29] Vadan, A. M., & Miclea, L. C. (2023). Software testing techniques for improving the quality of smart-home iot systems. Electronics, 12(6), 1337.

[30] Vadan, A. M., & Miclea, L. C. (2023). Software testing techniques for improving the quality of smart-home iot systems. Electronics, 12(6), 1337.

[31] Kalin, J. H. (2017). Simulating IoT Frameworks and Devices in the Smart Home (Doctoral dissertation, Virginia Tech).

[32] Thoung, T. H., & Myo, Z. M. M. Home Control and Monitoring System using MATLAB Graphical User Interface.