# INTERNET OF THINGS (PART-2)

## Abstract

The paper contains information about different aspects of Internet of Things (IoT) mainly concentrating on Embedded systems, sensors, Privacy and Security, Virtual reality and Augmented reality and applications of it. The part-I discusses about embedded systems, sensors and their main applications and brief description of them. The part-II discusses about privacy and security which were part of previous chapter. This is part-III contains information about virtual reality and augmented reality and the latest products. At the end we also discuss about the different applications of IoT in everyday life and also challenges that exist in developing IoT.

**Keywords:** Internet of Things (IoT), sensors, Privacy and Security, Virtual reality and Augmented reality.

## Authors

**Mr. K. Srinivasa Rao**
Assistant Professor
Department of Computer Science
Bhavan’s Vivekananda College
Secunderabad, Telangana, India.

**Mr. Kasarapu Ashok**
Assistant Professor
Department of Computer Science
Bhavan’s Vivekananda College
Secunderabad, Telangana, India.

**Maanya Rajan**
Department of Computer Science
Bhavan’s Vivekananda College
Secunderabad, Telangana, India.

**T. Sethu Venkat**
Department of Computer Science
Bhavan’s Vivekananda College
Secunderabad, Telangana, India.

## I. IOT COMMUNICATION TECHNOLOGIES

The rapid evolution of technology has brought us to the doorstep of an interconnected world, where devices, sensors, and systems seamlessly communicate, share data, and collaborate to enhance our lives and industries. This phenomenon is known as the Internet of Things (IoT), and at its heart lies a diverse array of communication technologies that empower the exchange of information, enabling the realization of its transformative potential.

## II. INTRODUCTION

IoT (Internet of Things) communication technologies refer to the various methods and protocols that enable devices, often referred to as "things," to exchange data and information over the internet. These technologies play a crucial role in the functioning of IoT ecosystems, enabling seamless connectivity and data sharing among a wide range of devices, from smart appliances and wearable devices to industrial sensors and autonomous vehicles. Some prominent IoT communication technologies include Wi-Fi, Bluetooth, Zigbee, LoRaWAN, cellular networks (3G, 4G, 5G), and MQTT (Message Queuing Telemetry Transport). Each technology offers distinct advantages and trade-offs in terms of range, data rate, power consumption, and scalability, making them suitable for different IoT use cases and scenarios.
The Internet of Things, a paradigm that has gained immense momentum, envisions a world where everyday objects become intelligent entities, capable of sensing their environment, collecting data, and communicating with other devices or systems. The foundation of this

vision rests upon robust and efficient communication technologies that facilitate real-time interactions among these interconnected entities.

## III. WIRELESS COMMUNICATION TECHNOLOGIES

Among the various communication technologies that drive IoT, wireless technologies hold a significant place. Wi-Fi (IEEE 802.11), Bluetooth, Zigbee, and Z-Wave are prime examples of wireless solutions that power IoT ecosystems. Wi-Fi offers high-speed data transmission suitable for applications demanding high bandwidth, such as video surveillance or real-time monitoring. Bluetooth and Zigbee cater to shorter-range, lower-power applications like home automation, wearables, and industrial sensors. Z-Wave, optimized for home automation, boasts low power consumption and a mesh networking architecture that enhances communication reliability.

Certainly! Here are some commonly used wireless communication technologies in IoT:

1. **Wi-Fi:** Provides high-speed data transfer over short distances. Used in applications like smart homes, offices, and retail for devices needing high bandwidth.

2. **Bluetooth:** Enables short-range communication between devices, making it ideal for wearables, smart home gadgets, and personal area networks.

3. **Zigbee:** Low-power and low-data-rate technology often used in home automation, industrial control systems, and sensor networks.

4. **Z-Wave:** Similar to Zigbee, it's optimized for home automation with low-power consumption and is widely used in smart home devices.

5. **LoRaWAN:** Designed for long-range communication with low power consumption, suitable for applications like agriculture, environmental monitoring, and smart cities.

6. **NB-IoT** (Narrowband IoT)**:** A cellular technology for low-power, wide-area coverage, making it suitable for applications like asset tracking and utility metering.

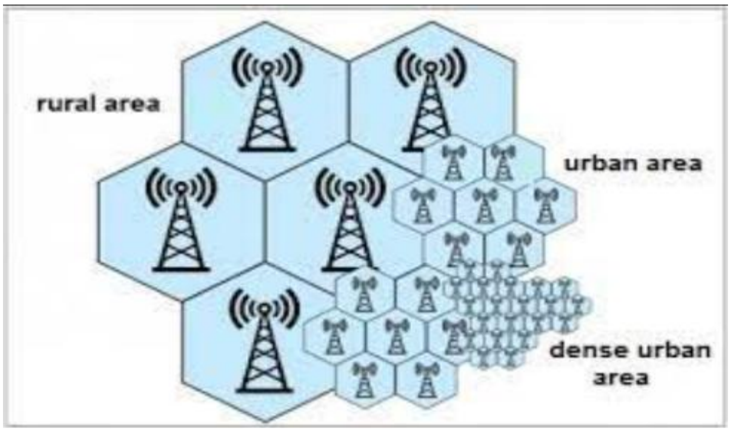
7. **LTE-M:** Another cellular technology, offering moderate data rates and power efficiency, used in applications like wearables, vehicle tracking, and industrial monitoring.

8. **5G:** The latest cellular technology with high data rates, low latency, and massive device connectivity. It's expected to support applications like smart cities, autonomous vehicles, and augmented reality.

These technologies cater to various IoT requirements, including range, data rate, power consumption, and scalability, allowing them to be deployed in diverse IoT applications.

## IV. CELLULAR COMMUNICATION TECHNOLOGIES

Cellular technologies, known for their extensive coverage and reliability, are also being harnessed for IoT. The progression from 2G to 5G has ushered in faster speeds, lower latency, and enhanced capacity, making cellular networks suitable for applications requiring wide coverage and mobility. Cellular IoT variants like Narrowband IoT (NB-IoT) and LTE-M offer low-power and cost-effective connectivity for applications such as smart cities, agriculture, and logistics.



Cellular communication technologies play a significant role in IoT by providing wide-area connectivity and enabling devices to communicate over cellular networks. Here are some key cellular technologies used in IoT:

1. **2G (GSM/GPRS):** Though older, 2G networks are still used in some IoT applications due to their widespread coverage. They are suitable for applications with low data requirements, like remote monitoring and tracking.

2. **3G (UMTS):** 3G networks offer higher data rates compared to 2G, making them useful for applications that need moderate data transfer, such as video surveillance and vehicle tracking.

3. **4G (LTE):** LTE networks provide even higher data rates and lower latency, making them suitable for applications like real-time video streaming, industrial automation, and smart cities

4. **5G:** The latest generation of cellular technology, 5G, promises extremely high data rates, ultra-low latency, and the ability to connect a massive number of devices. It's well-suited for applications like autonomous vehicles, remote surgery, and augmented reality.

5. **NB-IoT (Narrowband IoT):** This is a specialized cellular technology designed for IoT applications with low data requirements. It offers good coverage, deep indoor penetration, and low power consumption, making it ideal for applications like smart meters and agricultural sensors.

6. **LTE-M:** LTE-M (LTE for Machines) is optimized for IoT devices that require a balance between data rates and power consumption. It's commonly used in asset tracking, smart agriculture, and industrial IoT.

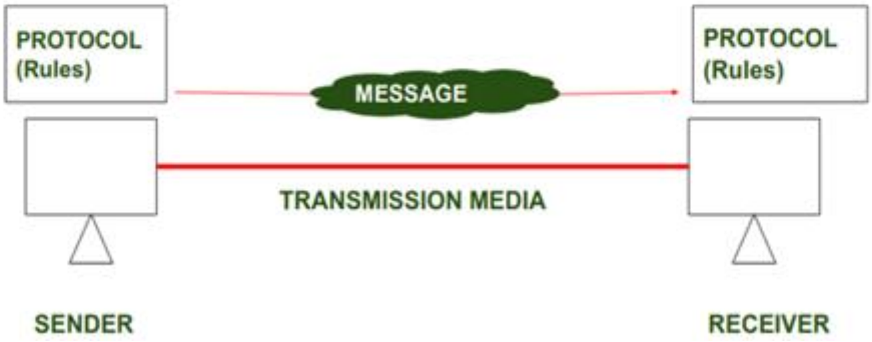
These cellular technologies provide reliable and secure connectivity over large areas, making them suitable for IoT deployments that need coverage beyond the reach of traditional short-range wireless technologies. The choice of cellular technology depends on factors such as the required data rates, coverage area, power efficiency, and overall IoT application needs.

## V. LPWAN TECHNOLOGIES

Low-Power Wide-Area Network (LPWAN) technologies, designed to meet the demands of IoT devices with low data rates and extended battery life, are gaining traction. LoRa (Long Range) and Sigfox are notable LPWAN solutions that offer long-range communication and operate in unlicensed spectrum. These technologies find applications in asset tracking, environmental monitoring, and smart agriculture, where devices need to communicate over vast distances while conserving energy.

## VI. COMMUNICATION PROTOCOLS AND STANDARDS

Efficient communication is guided by protocols and standards that ensure compatibility and seamless integration. MQTT (Message Queuing Telemetry Transport) and Co-AP (Constrained Application Protocol) are popular lightweight protocols for IoT communication. MQTT's publish-subscribe model facilitates real-time data flow, while CoAP's resource-oriented architecture suits constrained devices and resource-constrained networks.



Certainly, there are several communication protocols and standards used in the IoT ecosystem to ensure devices can effectively exchange data and information. Here are some important ones:

1. **MQTT (Message Queuing Telemetry Transport):** MQTT is a lightweight messaging protocol ideal for IoT due to its low overhead. It's commonly used for remote device monitoring and control.

2. **Co-AP (Constrained Application Protocol):** Co-AP is designed for resource-constrained devices and supports request/response interactions between IoT devices and servers.

3. **HTTP (Hypertext Transfer Protocol):** While not exclusive to IoT, HTTP is widely used for communication between web-based applications and IoT devices. It's suitable for devices with higher processing power and data requirements.

4. **AMQP (Advanced Message Queuing Protocol):** AMQP is a messaging protocol for connecting devices and applications using message-based communication patterns.

5. **DDS (Data Distribution Service):** DDS is a standard for real-time, data-centric communication. It's used in applications where low-latency, high-throughput data exchange is crucial.

6. **Bluetooth Low Energy (BLE):** BLE is a protocol used for short-range communication between devices, often found in wearable devices, home automation, and healthcare applications.

7. **Zigbee:** Zigbee has its own set of communication protocols for creating personal area networks with low-power devices, often used in home automation and industrial applications.

8. **Z-Wave:** Z-Wave utilizes its own wireless communication protocol for home automation, focusing on low power consumption and ease of use.

9. **Modbus:** Modbus is a popular protocol used in industrial automation for connecting devices to a supervisory control and data acquisition (SCADA) system.

10. **OPC UA (Open Platform Communications Unified Architecture):** OPC UA is used for secure and reliable data exchange in industrial automation and manufacturing environments.

11. **Thread:** Thread is a low-power, wireless communication protocol that's often used in smart home devices for mesh networking.

12. **LWM2M (Lightweight M2M): L**WM2M is a protocol for managing IoT devices and applications, offering features like remote device management and firmware updates.

These protocols and standards cater to different IoT scenarios, including different levels of power consumption, data rates, and requirements for real-time communication. The choice of protocol depends on factors such as the application's needs, device capabilities, and overall system architecture.

## VII. SECURITY AND PRIVACY CONSIDERATIONS

The proliferation of IoT devices introduces concerns over security and privacy. Protecting data integrity, confidentiality, and authentication are paramount. Encryption, secure bootstrapping, and identity management mechanisms are essential components of securing IoT communication. As IoT ecosystems grow, it becomes imperative to implement comprehensive security practices to mitigate potential risks.

Security and privacy are critical considerations in the design, deployment, and management of IoT systems. Here are some key aspects to keep in mind:

1. **Device Security:** Ensure that IoT devices have strong security measures, including unique credentials, secure boot, and firmware updates to patch vulnerabilities.

2. **Data Encryption:** Use encryption protocols to secure data both during transmission (TLS/SSL) and storage to prevent unauthorized access.

3. **Authentication and Authorization:** Implement strong authentication mechanisms to verify the identity of devices and users. Use role-based authorization to control access to data and functionalities.

4. **Network Security:** Secure communication channels between devices and backend systems using secure protocols. Implement firewalls, intrusion detection systems, and network segmentation to prevent unauthorized access.

5. **Privacy by Design:** Incorporate privacy protections into the design phase, minimizing the collection of sensitive data and allowing users to control their data.

6. **Data Minimization:** Collect only the data that is necessary for the intended purpose and avoid storing sensitive information unnecessarily.

7. **User Consent:** Obtain informed consent from users before collecting and using their data. Provide clear information about data usage and sharing practices.

8. **Secure APIs:** Implement secure APIs for data exchange between devices and applications, ensuring proper authentication and authorization checks.

9. **Regular Updates:** Keep devices and software up to date with security patches to address known vulnerabilities.

10. **Physical Security:** Protect physical access to devices to prevent tampering or unauthorized modifications.

11. **Monitoring and Logging:** Implement monitoring and logging to detect unusual activities and potential security breaches. Regularly review logs to identify any anomalies.

12. **Vendor Security:** Choose reputable vendors that prioritize security and provide regular updates and support for their products.

13. **Regulatory Compliance:** Be aware of relevant privacy and security regulations in your region, such as GDPR, CCPA, or industry-specific standards.

14. **Data Lifecycle Management:** Define how data is collected, processed, stored, and eventually deleted at the end of its lifecycle.

15. **Security Testing:** Conduct regular security assessments, penetration testing, and vulnerability scans to identify and address potential weaknesses.

16. **Incident Response Plan:** Have a well-defined plan in place to respond to security incidents, including communication, containment, and recovery measures.

17. **User Education:** Educate users about the importance of strong passwords, regular updates, and safe IoT usage practices.

Given the interconnected nature of IoT systems and the potential impact of security breaches, a comprehensive approach to security and privacy is essential to ensure the trustworthiness and longevity of IoT deployments.

## VIII. CASE STUDIES AND FUTURE TRENDS

Real-world applications of IoT communication technologies are found across industries. From smart agriculture optimizing resource usage to healthcare devices remotely monitoring patients, the impact is profound. As IoT evolves, trends such as edge computing and hybrid connectivity are emerging. Edge computing reduces latency by processing data closer to the source, while hybrid connectivity combines multiple technologies to ensure seamless communication across varying conditions.

Certainly, here are a couple of case studies and some potential future trends in the IoT landscape:

### 1. Case Studies

- **Smart Agriculture:** Precision Farming: IoT sensors, drones, and satellite data are being used to monitor soil conditions, weather patterns, and crop health in real time. This data helps farmers optimize irrigation, fertilization, and pest control, resulting in increased yields and resource efficiency.
- **Connected Healthcare:** Remote Patient Monitoring: IoT devices such as wearable health trackers and medical sensors enable remote monitoring of patients' vital signs and health conditions. Healthcare providers can receive real-time data, allowing for timely interventions and reducing hospital readmissions.

### 2. Future Trends

- **Edge Computing:** With the growth of IoT, processing data at the edge (closer to the data source) will become more prevalent. This reduces latency and improves efficiency by analyzing data locally before sending it to the cloud.
- **5G Integration:** The deployment of 5G networks will enable higher data speeds, lower latency, and increased device density. This will facilitate the growth of applications like autonomous vehicles, augmented reality, and real-time industrial automation.
- **AI and Machine Learning Integration:** IoT devices will increasingly incorporate AI and machine learning capabilities for real-time data analysis, predictive maintenance, and decision-making.

- **Blockchain for IoT Security:** Blockchain technology is being explored to enhance the security of IoT networks by providing transparent and tamper-proof data records and authentication mechanisms.
- **IoT in Smart Cities:** Smart city initiatives will leverage IoT technologies to enhance urban planning, traffic management, waste management, energy efficiency, and public safety.
- **Industrial IoT (IIoT) Growth:** In industrial sectors, IIoT will continue to drive efficiencies through predictive maintenance, supply chain optimization, and improved asset utilization.
- **Environmental Monitoring:** IoT will play a significant role in environmental monitoring, helping track air quality, water quality, and overall environmental conditions.
- **Wearables and Health Tech:** Wearable devices and health-focused IoT applications will become even more sophisticated, contributing to personalized healthcare and wellness monitoring.
- **Energy Management:** IoT will enable better energy management by optimizing energy consumption in buildings, factories, and transportation systems.
- **Standardization and Interoperability:** As the IoT ecosystem continues to expand, there will be a push for more standardized protocols and increased interoperability among different IoT devices and platforms.

These trends reflect the ongoing evolution of IoT technologies and their increasing integration into various aspects of our lives. They hold the potential to transform industries, improve efficiencies, and create new opportunities for innovation.

## 3. Simple Programs

**LED Control Program**

```
from machine import Pin
import network
import socket

led = Pin(2, Pin.OUT)
sta_if = network.WLAN(network.STA_IF)
sta_if.active(True)
sta_if.connect("YourWiFiSSID", "YourWiFiPassword")

def web_page():
    html = """
    <html>
        <head><title>LED Control</title></head>
        <body>
            <h2>LED Control</h2>
            <form action="/" method="post">
                <button name="LED" value="ON" type="submit">Turn ON</button>
                <button name="LED" value="OFF" type="submit">Turn OFF</button>
            </form>
        </body>
    </html>
    """
    return html

def main():
    addr = socket.getaddrinfo('0.0.0.0', 80)[0][-1]
    s = socket.socket()
    s.bind(addr)
    s.listen(1)
    print('Listening on', addr)

    while True:
        cl, addr = s.accept()
        print('Client connected from', addr)
        request = cl.recv (1024)
        request = str(request)

        if 'LED=ON' in request:
            led.value(1)
        elif 'LED=OFF' in request:
            led.value(0)

        response = web_page()
        cl.send(response)
        cl.close()

if __name__ == '__main__':
    main()
```

- **Expected Output:** when you access the ip address of your microcontroller in a web browser, you should see a webpage with buttons to turn the LED on and off. Clicking these buttons will control the LED accordingly.

### 4. Temperature Sensor Program

```
  import machine
import dht
import urequests
import time

d = dht.DHT11(machine.Pin(2))

def get_temperature_and_humidity():
    d.measure()
    temperature = d.temperature()
    humidity = d.humidity()
    return temperature, humidity
```

```
def send_data_to_thingspeak(api_key, temperature, humidity):
    url = "https://api.thingspeak.com/update"
    params = {
        "api_key": api_key,
        "field1": temperature,
        "field2": humidity
    }
    response = urequests.get(url, params=params)
    print("Data sent to ThingSpeak")
    response.close()

def main():
    api_key = "YOUR_THINGSPEAK_API_KEY"
    while True:
        temperature, humidity = get_temperature_and_humidity()
        print("Temperature:", temperature, "°C")
        print("Humidity:", humidity, "%")
        send_data_to_thingspeak(api_key, temperature, humidity)
        time.sleep(30)  # Send data every 30 seconds
if __name__ == '__main__':
    main()
```

- **Expected Output**

    - The program will read temperature and humidity data from the DHT11 sensor and print it to the console.
    - It will then send the data to Thing Speak using the provided API key.
    - You should see temperature and humidity data appearing on your Thing Speak channel graphs.

## IX. CHALLENGES IN INTERNET OF THINGS (IOT)

1. **Absence of encryption:** Despite being a fabulous strategy of anticipating programmers from getting to information, encryption is additionally one of the foremost critical IoT security concerns. These drives are acclimated to the preparing and capacity control advertised by a customary computer. The conclusion result is an increment in assaults where programmers may rapidly alter the security algorithms.

2. **Inadequate testing and overhauling:** As the number of Internet of things (IoT) gadgets rises, IoT producers are energetic to create and disperse their mechanisms as rapidly as conceivable without giving security any thought. The majority of these IoT items and mechanisms don’t get sufficient testing or upgrades, making them defenseless to programmers and other security risks.

3. **The threat of utilizing default passwords and brute forcing:** Nearly all IoT gadgets are defenseless to secret word hacking and brute drive assaults due to feeble qualifications and login data. Any firm that clears out the production line default passwords on its

gadgets uncovered not as it were its possess resources but too the touchy data of its clients to the plausibility of a brute constrain assault.

4. **IoT Malware and Ransomware:** Increases in the number of gadgets. While retaining access to a user's important data and information, ransomware exploits encryption to effectively lock off users from a variety of devices and platforms. **Example** –A programmer can seize a computer camera and take pictures. By utilizing malware accesses focuses, the programmers can request liberate to open the gadget and return the data.
5. **Targeting cryptocurrencies with IoT botnets:** IoT botnet employees have the capacity to alter information security, which postures critical concerns for an open cryptocurrency showcase. Programmers with noxious eagerly posture a danger to the precise esteem and generation of cryptocurrency codes. To extend security, blockchain businesses are working.

6. **Poor gadget security:** Destitute gadget security is the non-attendance of reasonable shields against cyber-attacks, hacking, information burglary, and unauthorized get to electronic gadgets counting computers, smartphones, and IoT devices.

7. **Need of standardization:** Need of standardization alludes to the nonattendance of agreed-upon determinations or conventions in a specific field or industry. This may result in various systems, things, or shapes being conflicting with each other, driving to perplexity, inefficiency, and decreased interoperability.

8. **Powerlessness to orchestrate ambushes:** Defenselessness to organize ambushes implies to the defenselessness of an arrange, system or contraption to being compromised or manhandled by cyber criminals. This may happen due to inadequacies inside the orchestrate establishment, unpatched computer program, dejected watchword organization, or an require of reasonable security measures.

9. **Unsecured file broadcast:** Unsecured file broadcast refers to the exchange of information over a network or the internet exterior sufficient care. This may take off the file open to blocking, tampering, or burglary by scornful entertainers. Unsecured file broadcast can happen when file is sent over an decoded arrange association or when temperamental commitments are used.

10. **Privacy concerns:** Protection concerns concern issues had association with the amassing, store, use, and sharing of private actualities. This may contain concerns almost the one has approach to private news, irrefutable truth being used, and either it is being protected from ill-conceived approach or abuse. Within the numerical age, isolation concerns have improve progressively fundamental as person realities is being calm and supplied on an uncommon scale.

## X. CONCLUSION

In conclusion, IOT communication technologies are the unsung heroes that power the interconnected world we inhabit today. Wireless, cellular, and LPWAN technologies, supported by efficient protocols, have ushered in an era of unprecedented connectivity. While we celebrate the successes achieved, it is essential to acknowledge the ongoing journey towards securing these connections and staying abreast of the evolving landscape. As we stand on the cusp of further advancements, the IoT communication technologies continue to shape our present and hold the key to an even more connected and intelligent future.

In this process, IoT will face many challenges in the future as requirements and our technology will become more complex every year. The demand for a smarter and more efficient connected world must overcome all challenges to thrive in the age of advanced technology.

## REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.
[2] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26 521–26 544, 2017.
[3] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of internet of things (iot) and data analytics in agriculture: Benefits and challenges," IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3758–3773, Oct 2018.
[4] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," IEEE Access, vol. 6, pp. 78 238–78 259, 2018.
[5] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of internet of things: A case study of the smart plug system," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1899– 1909, Dec 2017.
[6] Gupta, A. K., & Johari, R. (2019). IOT based Electrical Device Surveillance and Control System. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). doi:10.1109/iot-siu.2019.8777342.
[7] Fox, J., Donnellan, A., & Doumen, L. (2019). The deployment of an IoT network infrastructure, as a localised regional service. 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2019.8767188.
[8] MQTT.org, "MQTT." [Online]. Available: http://mqtt.org/.
[9] Challenges in Internet of things .https://www.geeksforgeeks.org/challenges-in-internet-of-things-iot/.