RQF LEVEL 3

NITIS301

NETWORKING AND INTERNET TECHNOLOGIES

IoT System Installation

TRAINEE'S MANUAL

October, 2024

IoT SYSTEM INSTALLATION

KOICA Korea International Cooperation Agency

TQUM TVET Quality Management Project

2024

AUTHOR'S NOTE PAGE (COPYRIGHT)

- This work has been produced initially with the Rwanda TVET Board with the support from KOICA through TQUM Project
- This work has copyright, but permission is given to all the Administrative and Academic Staff of the RTB and TVET Schools to make copies by photocopying or other duplicating processes for use at their own workplaces.
- This permission does not extend to making of copies for use outside the immediate environment for which they are made, nor making copies for hire or resale to third parties.
- The views expressed in this version of the work do not necessarily represent the views of RTB. The competent body does not give warranty nor accept any liability
- RTB owns the copyright to the trainee and trainer's manuals. Training providers may reproduce these training manuals in part or in full for training purposes only. Acknowledgment of RTB copyright must be included on any reproductions. Any other use of the manuals must be referred to the RTB.

© Rwanda TVET Board
Copies available from:

- *HQs: Rwanda TVET Board-RTB*
- *Web: www.rtb.gov.rw*
- **KIGALI-RWANDA**

Original published version: October 2024

ACKNOWLEDGEMENTS

The publisher would like to thank the following for their assistance in the elaboration of this training manual:

Rwanda TVET Board (RTB) extends its appreciation to all parties who contributed to the development of the trainer's and trainee's manuals for the TVET Certificate III in Networking and Internet Technologies, specifically for the module **" NITIS301: IoT System Installation."**

We extend our gratitude to KOICA Rwanda for its contribution to the development of these training manuals and for its ongoing support of the TVET system in Rwanda
We extend our gratitude to the TQUM Project for its financial and technical support in the development of these training manuals.

We would also like to acknowledge the valuable contributions of all TVET trainers and industry practitioners in the development of this training manual.

The management of Rwanda TVET Board extends its appreciation to both its staff and the staff of the TQUM Project for their efforts in coordinating these activities.

This training manual was developed:

Under Rwanda TVET Board (RTB) guiding policies and directives

Under Financial and Technical support

COORDINATION TEAM

RWAMASIRABO Aimable

MARIA Bernadette M. Ramos

MUTIJIMA Asher Emmanuel

PRODUCTION TEAM

Authoring and Review

KWIZERA Ildephonse

MUKANYANDWI Leoncie

Validation

MANIRAGUHA Denys

HABAKURAMA Innocent

Conception, Adaptation and Editorial works

HATEGEKIMANA Olivier

GANZA Jean Francois Regis

HARELIMANA Wilson

NZABIRINDA Aimable

DUKUZIMANA Therese

NIYONKURU Sylivestre

NYINAWUMUNTU Gaudence

Formatting, Graphics, Illustrations, and infographics

YEONWOO Choe

SUA Lim

SAEM Lee

SOYEON Kim

WONYEONG Jeong

MANIRAKORA Alexis

Financial and Technical support

KOICA through TQUM Project

TABLE OF CONTENT

ACRONYMS

5G: 5th Generation

ACK: Acknowledgement

ARIB: Association of Radio Industries & Businesses

AWS: Amazon Web Services

BLE: Bluetooth Low Energy

CE: Coverage Enhancement

CI: Coding Indicator (for Bluetooth 5)

CI: Connection Interval (BLE)

CIOT: Cellular Internet of Things

CoAP: stands for Constrained Application Protocol

DHT: Digital Temperature and Humidity

EC-GSM-IoT: Extended Coverage GSM Internet of Things

EDGE: Enhanced Data Rates for GSM Evolution

EtherCAT: Ethernet for Controlled Automation Technology

FDD: Frequency Division Duplexing

FreeRTOS: Free Real-Time Operating System

FSK Frequency Shift Keying

GND: Ground

GPRS: General Packet Radio Service

GSM: Global System for Mobile Communications

HTTP: stands for Hypertext Transfer Protocol

HTTPS: stands for Hypertext Transfer Protocol Secure

IIOT: Industrial Internet of Things

IIoT: Infrastructure IoT

IoMT: Internet of Military Things

IoT: Internet of Things

IoT: Internet of Things

IP: Internet Protocol

ISM: Industrial, Science, and Medicine

ISP: Internet Service Provider

JTAG: Joint Test Action Group

LEDs: Light Emitting Diodes

LoRa: Long Range Radio

LPWAN: Low-power Wide Area Network

LTE: Long-Term Evolution

LTE-M: LTE for Machine-Type Communications

M2M: Machine to Machine

MCU: Microcontroller unit

MQTT: Message Queuing Telemetry Transport

MTC: Machine Type Communications

NB-IoT: Narrowband Internet of Things

NB-PLC: Narrow-Band PLC

NFC: Near-Field Communication

PAN: Personal Area Network

PCG: Project Coordination Group

PCP: priority Code Point

PDU: Protocol Date Unit

PLC: Power Line Communication

PPFN: Profinet Process Field Network

PRTG: Paessler Router Traffic Grapher

QoS: Quality of Service

RAN: Radio Access Networks

RFID: Radio Frequency Identification

RTB: Rwanda TVET Board

RTOS: Real-Time Operating System

RU: Resource Unit

RX: Receive

SDR: Software-defined radio

SNR: Signal-to-Noise Ratio

TbE: Tera Bit Ethernet

TCP/IP: Transmission Control Protocol/Internet Protocol

TQUM: Project: TVET Quality Management Project

TVET: Technical and Vocational Education and Training

TX: Transmit

VLAN: Virtual Local Area Network

Wi-Fi: Wireless Fidelity

INTRODUCTION

This trainee's manual includes all the knowledge and skills required in Networking and Internet Technologies, specifically for the module of **" IoT System Installation ".** Trainees enrolled in this module will engage in practical activities designed to develop and enhance their competencies. The development of this training manual followed the Competency-Based Training and Assessment (CBT/A) approach, offering ample practical opportunities that mirror real-life situations.

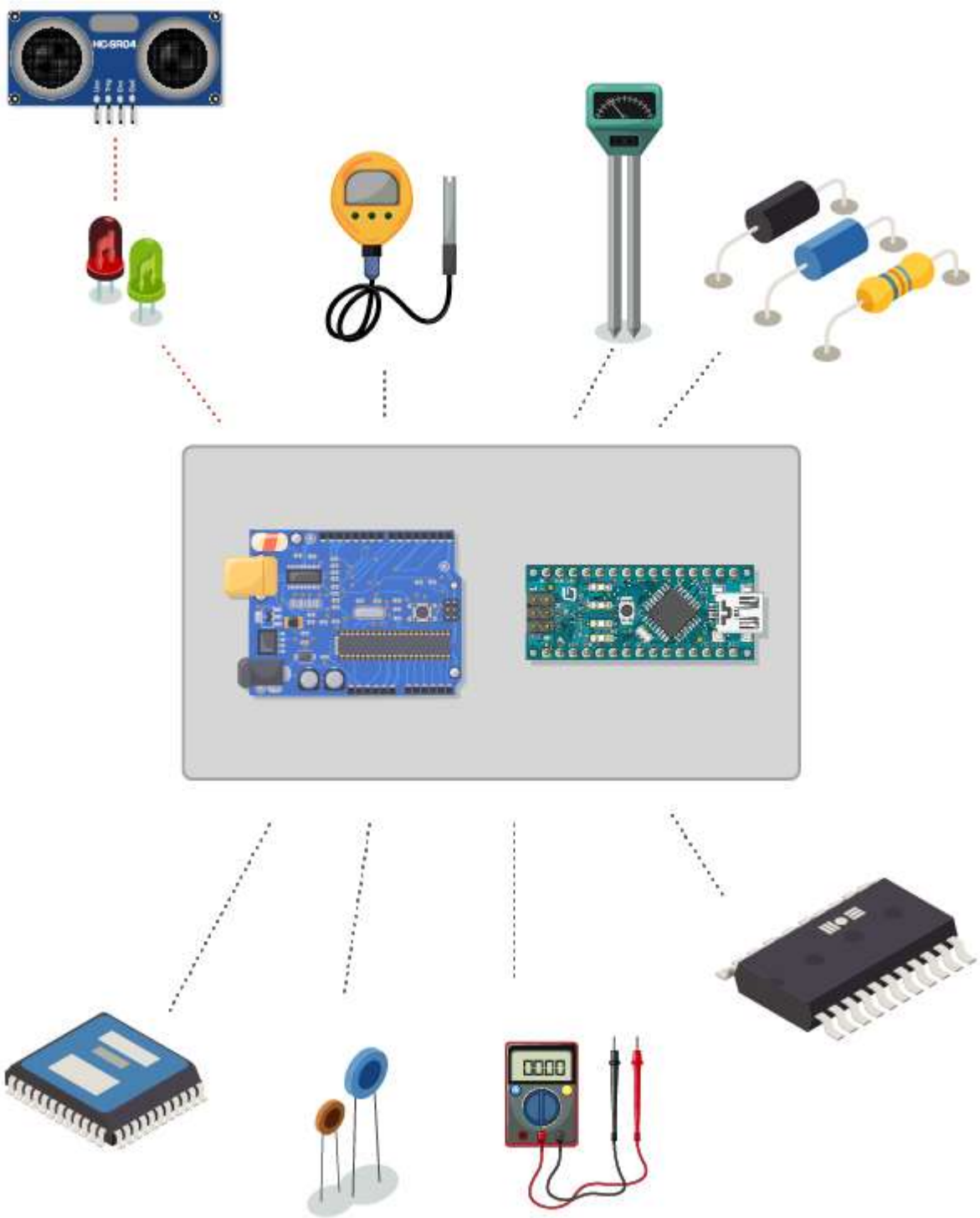
The trainee's manual is organized into Learning Outcomes, which is broken down into indicative content that includes both theoretical and practical activities. It provides detailed information on the key competencies required for each learning outcome, along with the objectives to be achieved.

As a trainee, you will start by addressing questions related to the activities, which are designed to foster critical thinking and guide you towards practical applications in the labor market. The manual also provides essential information, including learning hours, required materials, and key tasks to complete throughout the learning process.

All activities included in this training manual are designed to facilitate both individual and group work. After completing the activities, you will conduct a formative assessment, referred to as the end learning outcome assessment. Ensure that you thoroughly review the key readings and the 'Points to Remember' section.

MODULE CODE AND TITLE: NITIS301 IoT SYSTEM INSTALLATION

Learning Outcome 1: Prepare IoT system installation.
Learning Outcome 2: Deploy IoT equipment.
Learning Outcome 3: Operate IoT system.
Learning Outcome 4: Test IoT system
Learning Outcome 5: Maintain IoT system


HC-SR04

Indicative Contents

1.1 Introduction to IOT

1.2 Identification of IoT Network Technologies

1.3 Description of IoT Architecture and Protocols

1.4 Calibration of Tools, Equipment and Materials

1.5 Interpretation of Manual/Datasheet

Key Competencies for Learning Outcome 1: Prepare IoT System Installation

Knowledge	Skills	Attitudes
• Description of IoT Components • Identification of IoT Network Technology and Their Challenges • Identification of IoT Tools, Materials, and Equipment • Description of IoT Architecture and Protocols • Description of Manual and Datasheet	• Calibrating of IoT Tools and Equipment • Interpreting of Manual and Datasheet • Selecting of IoT Network Technologies	• Having an Innovation • Having a Team Work • Having a Time Management • Having a Creativity • Having a Self Confidence

Duration: 20hrs

Learning outcome 1 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe correctly IoT component as used in IoT system installation
2. Interpret properly Installation manual based on IoT system installation
3. Identify correctly IoT tools, materials and equipment as used in IoT system installation
4. Identify properly IoT network technology and challenges based on IoT system installation
5. Calibrate accurately IoT Tool, devices, and equipment as per manufacturer's standards

Resources

Equipment	Tools	Materials
• Wireless Router • Gadgets • Appliances • Arduino board • Computer	• Calibration software • Simulators • Screw drivers' kit • Pliers set • Digital multimeter	• IoT Device • Internet • Arduino Starter Kit, • IoT Device Datasheet

Indicative content 1.1: Introduction To IOT

Duration: 4 hrs

Theoretical Activity 1.1.1: Description of IoT Fundamentals

Tasks:

1: You are requested to answer the following questions related to Description of IoT Fundamentals

i. What is the definition of IoT?
ii. Name a few key benefits and challenges of implementing IoT in various industries
iii. Provide examples of real-world applications where IoT technology is extensiv ely used
iv. What are some common devices or components that are essential for buildin g an IoT system?
v. Explain the role of IoT platforms in the development and management of IoT solutions.
vi. How has IoT technology evolved over the years, and what are some significa nt milestones in its development?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

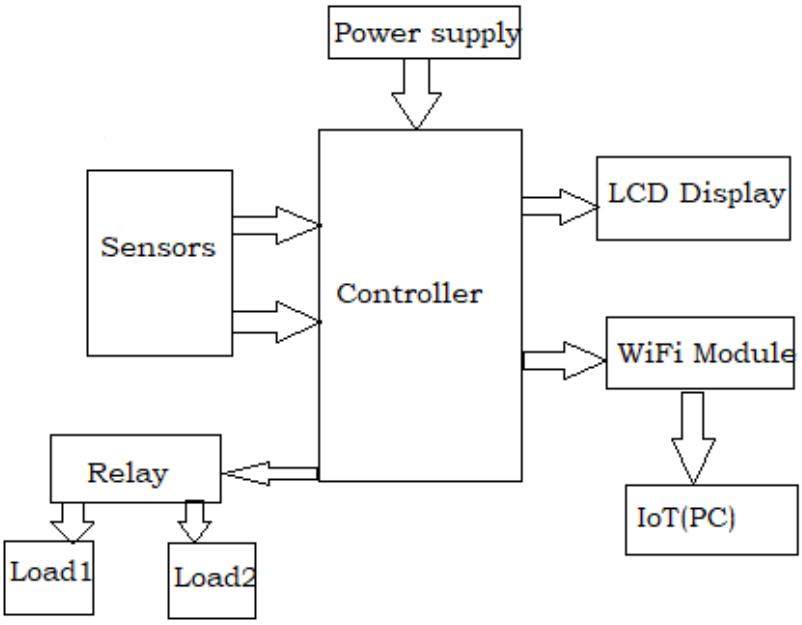
5: For more clarification, read the key readings 1.1.1

Key readings 1.1.1.: Description of IoT Fundamentals

- **Definition of IoT**
  - **The Internet of Things (IoT)**: is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided

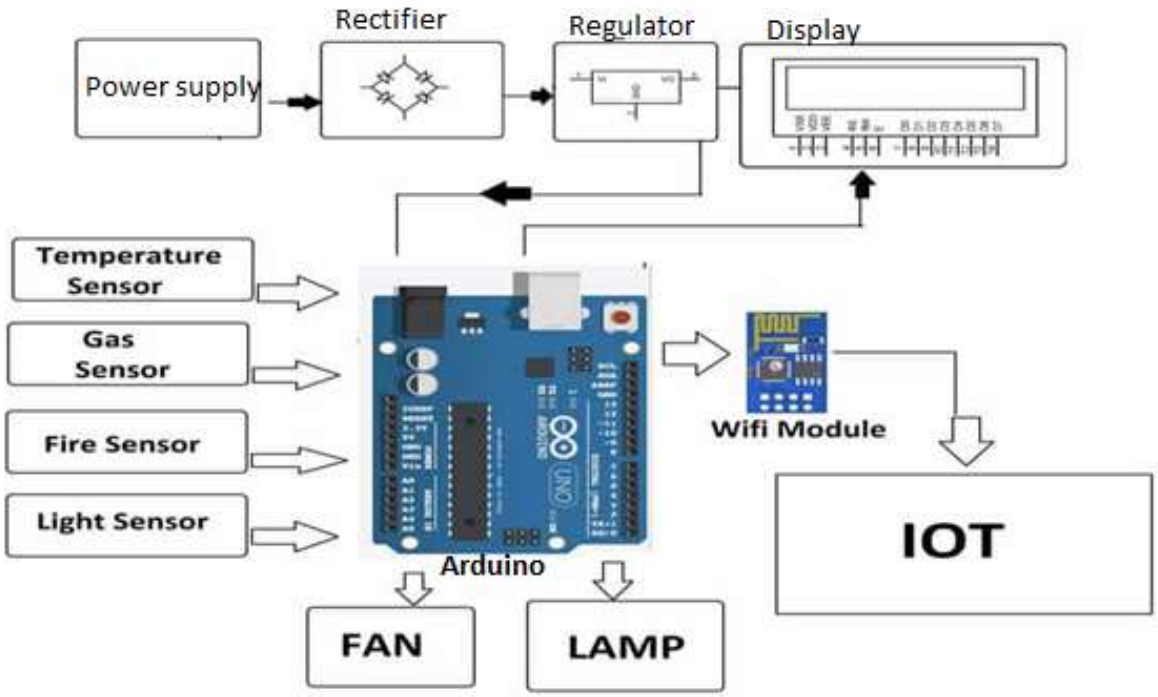
with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

- **Working principle of IoT**: The Internet of Things (IoT) is nothing but "A network of Internet-connected objects able to collect and exchange data". IoT works by connecting items and then having the ability to sense and communicate. This leads the devices to communicate or interact with other devices and with the human.



IoT works like this:

- Devices have hardware, like sensors, that collect data.
- The data collected by the sensors is then shared via the cloud and integrated with software.
- The software then analyzes and transmits the data to users via an app or website.



- **Challenges Facing the IoT Industry:** Concerns over security, interoperability, scalability, and standardization.

Benefits of IoT technology:

- ✔ Access Information in Real-Time
- ✔ Machine-to-Machine Communication
- ✔ Better Quality of Life
- ✔ Cost Reduction
- ✔ Remote Health Monitoring

IoT technology Applications:

- ✔ Smart Home and Office
- ✔ Wearable Devices
- ✔ Healthcare
- ✔ Autonomous Driving
- ✔ Agriculture and Smart farming
- ✔ Industrial IoT for manufacturing
- ✔ Disaster management
- ✔ Logistic and fleet management
- ✔ Smart Grids and energy management

IoT Devices/Components:

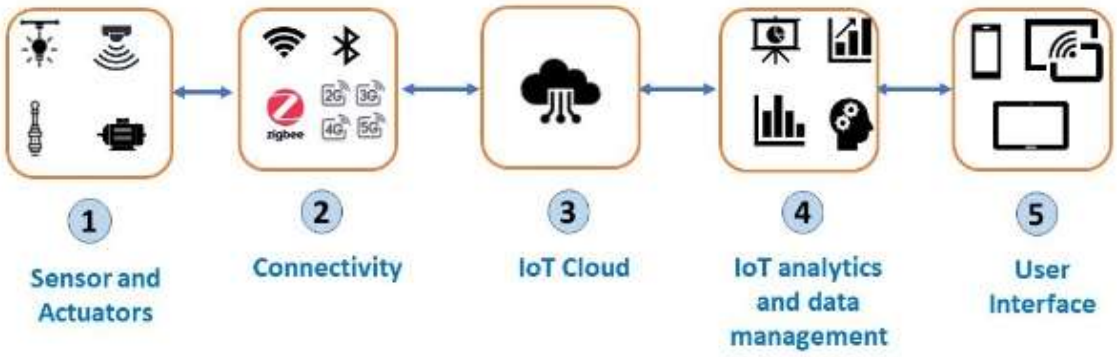
IoT systems are composed of various devices and components that work together to collect, process, and transmit data.

Devices

- **Sensors:** These are the primary data collection devices. They measure physical parameters such as temperature, humidity, pressure, light, motion, and more.
- **Actuators:** These devices perform actions based on the data received. They can control physical objects. Examples include: Motors, Valves, Lights and Heating/cooling systems
- **Microcontrollers and Microprocessors:** These are the brains of IoT devices. They process data from sensors, make decisions, and control actuators.
- **Gateway:** This device acts as a bridge between IoT devices and the internet. It collects data from multiple devices, aggregates it, and transmits it to the cloud or a local server.

Components

- **Connectivity Modules**: These components enable IoT devices to connect to the internet. They can use various technologies such as Wi-Fi, Bluetooth, cellular networks (e.g., 2G, 3G, 4G, 5G), or LoRaWAN.
- **Power Sources:** IoT devices can be powered by various sources, including batteries, solar panels, or mains power.
- **Operating Systems**: These software platforms provide a foundation for IoT devices. They handle tasks such as resource management, communication, and data processing.
- **Cloud Platforms**: These remote servers store and process data collected by IoT devices. They also provide tools for data analysis, visualization, and application development.
- **Applications:** These software interfaces allow users to interact with IoT devices and view data. They can be web-based, mobile, or desktop applications.



- **IoT platforms**

IoT connectivity platforms: IoT connectivity platforms refer to the underlying systems and technologies that enable devices and sensors to connect, communicate, and exchange data within the Internet of Things (IoT) ecosystem. These platforms provide the necessary infrastructure and protocols to establish and manage connectivity between IoT devices, networks, and applications.

Examples of IoT connectivity platforms:

- ✓ Amazon Web Services (AWS) IoT,
- ✓ Microsoft Azure IoT,
- ✓ Google Cloud IoT Core,
- ✓ IBM Watson IoT Platform,
- ✓ Siemens MindSphere, and
- ✓ Cisco IoT Cloud Connect

- **IoT device platforms:** IoT device platforms, also known as IoT platforms, refer to software frameworks or ecosystems that enable the development, deployment, and management of Internet of Things (IoT) devices. These platforms provide a set of tools, services, and functionalities to facilitate the creation and operation of IoT solutions.
- **Analytics platforms:** Analytics platforms refer to software systems or frameworks that facilitate the collection, processing, analysis, and visualization of data to derive meaningful insights and support data-driven decision-making. These platforms offer a range of tools, technologies, and functionalities to handle large volumes of data and extract valuable information from it.
- **IoT Cloud Platforms:** IoT Cloud Platforms, also known as Internet of Things

Cloud Platforms, are software-based platforms that enable the management, processing, and analysis of data generated by Internet of Things (IoT) devices. These platforms provide a set of services and tools that facilitate the development, deployment, and scaling of IoT applications and solutions.

- **Evolution of IoT Technology and Milestones:**

  Progressed from basic communication to complex device ecosystems.
  Major milestones include IPv6 adoption and the rise of edge computing.

Theoretical Activity 1.1.2: Identification of IoT components

Tasks:

1: In small groups, you are requested to answer the following questions related to the Identification of IoT Tools, Materials and equipment.

i. What are "Things" in the context of IoT, and can you give two examples?
ii. How does the "Internet" component support IoT devices?
iii. Name two wireless technologies used for IoT connectivity

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.1.2

Key readings 1.1.2.:

- **Things** "Things" in the context of IoT refer to the physical objects that are embedded with sensors, software, and other technologies to collect and exchange data with other devices and systems over the internet. These can be:
  - Sensors: These devices measure physical parameters like temperature, humidity, pressure, motion, light, and more.
  - Actuators: These devices perform actions based on data received, such as controlling motors, valves, or lights.
  - Microcontrollers and Microprocessors: These are the brains of IoT

devices, processing data and controlling other components.

- Gateways: These devices connect IoT devices to the internet, aggregating data and transmitting it to a cloud platform.

- **Internet:** The "Internet" component in IoT refers to the global network that facilitates the communication between IoT devices and systems. This involves:
  - **Network Infrastructure**: The underlying hardware and software that make up the internet, including routers, servers, and data centers.

    Examples: Local Area Networks (LAN), Wide Area Networks (WAN), cellular networks (3G, 4G, 5G).
  - **Cloud Services**: Platforms that provide data storage, processing, and analysis capabilities. Cloud services enable the handling of large volumes of data generated by IoT devices and support applications like data analytics, machine learning, and artificial intelligence.

    Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Watson IoT.
  - **Data Management**: Systems and processes for collecting, storing, processing, and analyzing data. This includes databases, data lakes, and big data technologies.
- **Connectivity:** "Connectivity" is crucial for IoT as it ensures that data can flow between devices and the internet. This encompasses various communication technologies and protocols, such as:
  - **Wireless Technologies**: Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, and cellular networks (2G, 3G, 4G, 5G) that enable wireless communication between devices.
  - **Wired Technologies**: Ethernet and other wired connections that provide stable and high-speed data transfer.
- **Protocols**: Communication protocols like MQTT, CoAP, HTTP/HTTPS, and WebSocket that define the rules for data exchange between IoT devices and systems.

In an IoT system, the components can be broadly categorized into three key elements: **"Things" (Devices and Sensors)**, **"Internet" (Network and Cloud Services)**, and **"Connectivity" (Communication Protocols and Technologies)**. Here's how each of these components is identified and defined:

- **Things (Devices and Sensors):** "Things" refer to the physical objects in an IoT

system that are embedded with sensors, actuators, software, and other technologies. These objects can collect data from the environment, interact with each other, and be controlled remotely.

Examples:

Sensors: Temperature sensors, humidity sensors, motion detectors, GPS trackers.

Actuators: Motors, valves, switches, relays.

Devices: Smart thermostats, wearable health monitors, smart appliances, industrial machines.

- **Internet (Network and Cloud Services):** The "Internet" component in an IoT system refers to the infrastructure that enables data to be transmitted from the "Things" to other systems, and vice versa. This includes both local networks (such as home or enterprise networks) and cloud services that store, process, and analyze the data.

  Examples:

  - **Network:** Local Area Networks (LAN), Wide Area Networks (WAN), cellular networks (3G, 4G, 5G).
  - **Cloud Services:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud, IBM Watson IoT.

- **Connectivity (Communication Protocols and Technologies):** "Connectivity" in IoT refers to the various communication protocols and technologies that link the "Things" to the Internet and each other. This component ensures that data can be reliably transmitted, often across different environments and distances.

  Examples:

  - **Wired Protocols:** Ethernet, Modbus, CAN bus.
  - **Wireless Protocols:** Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRaWAN, NB-IoT.
  - **Cellular Technologies:** 2G, 3G, 4G, 5G.
  - **Protocols:** MQTT, CoAP, HTTP, TCP/IP.

- **Protocols**: Communication protocols like MQTT, CoAP, HTTP/HTTPS, and WebSocket that define the rules for data exchange between IoT devices and systems.

Theoretical Activity 1.1.3: Identification of IoT Tools, Materials and equipment

Tasks:

1: In small groups, you are requested to answer the following questions related to the Identification of IoT Tools, Materials and equipment.

i. What are two examples of microcontrollers or microprocessors used in IoT devices?
ii. Name one software tool used for data analytics and visualization in IoT

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

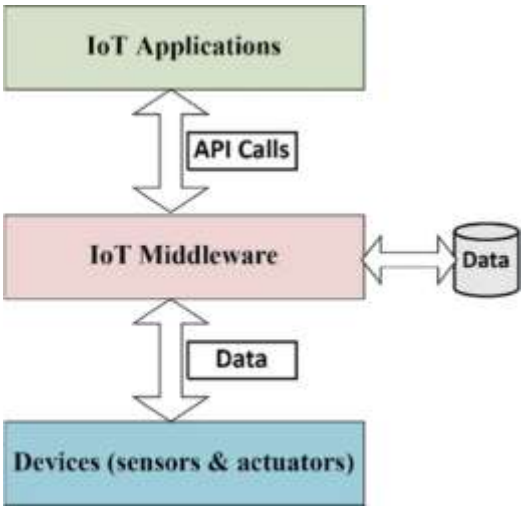
5: For more clarification, read the key readings 1.1.3

Key readings 1.1.3:

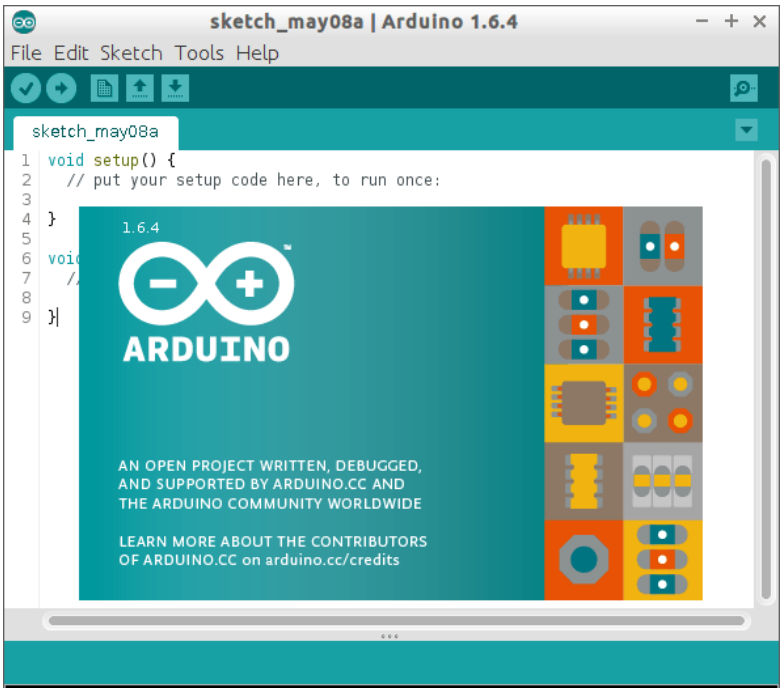
- **Software**
  - **Operating Systems**: Provide a platform for running applications and managing device resources. **Examples**: Windows IoT, Linux (Raspbian, Ubuntu), FreeRTOS

  - **Middleware and Frameworks**: Facilitate communication between hardware and software components, providing APIs and libraries for easier

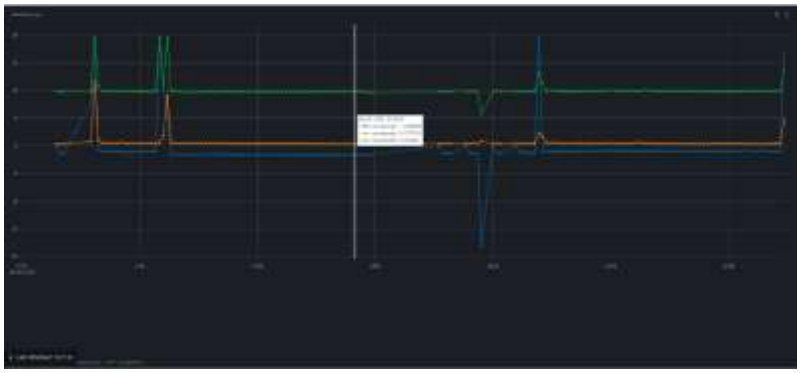
development. **Examples**: Google Cloud IoT Core, Amazon AWS IoT, Microsoft Azure IoT Hub



- **Development Tools and IDEs**: Provide environments for writing, debugging, and deploying code to IoT devices. **Examples**: Arduino IDE, Visual Studio Code, Eclipse



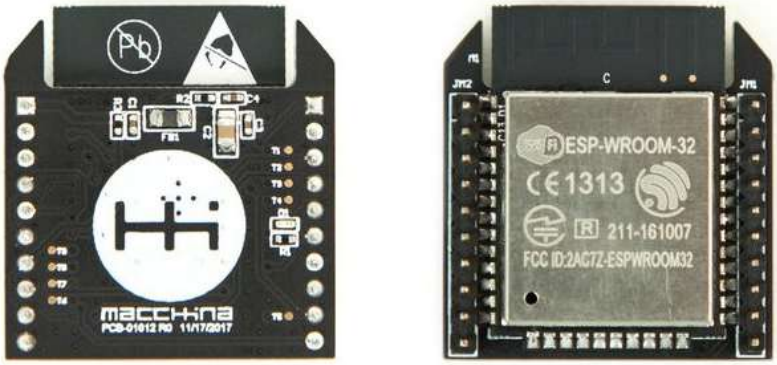
- **Data Analytics and Visualization Tools**: Analyze and visualize data collected from IoT devices. **Examples**: Tableau, Power BI, Grafana



- **Network Management Tools**: Monitor and manage network performance and device connectivity. **Examples**: Nagios, PRTG Network Monitor
- **Security Software**: Protect IoT devices and networks from cyber threats. **Examples**: Symantec IoT Security, Zingbox

- **Hardware**
  - **Microcontrollers and Microprocessors**: Act as the brain of IoT devices, processing data and controlling operations. **Examples**: Arduino, Raspberry Pi, ESP8266/ESP32

Espressif ESP8266 and ESP32



- **Sensors**: Collect data from the environment or the object being monitored. **Examples**: Temperature sensors, humidity sensors, motion detectors, light sensors
- **Actuators**: Perform actions based on commands received from the microcontroller or microprocessor. Examples: Motors, servos, relays, LEDs
- **Communication Modules**: Enable wireless communication between IoT devices and other systems Examples: Wi-Fi modules (ESP8266), Bluetooth modules (HC-05), Zigbee modules (XBee), Cellular modules (SIM800)
- **Power Supply Units**: Provide the necessary power for IoT devices to operate. **Examples**: Batteries, solar panels, power adapters
- **Prototyping Boards and Shields**: Facilitate the development and testing of IoT projects by allowing easy connection and integration of components. **Examples**: Breadboards, Arduino shields, Raspberry Pi HATs
- **Edge Devices**: Process data locally at the edge of the network, reducing latency and bandwidth usage**. Examples**: Edge gateways, edge servers

Theoretical Activity 1.1.4: Identification of IoT Technology Challenges

Tasks:

1: In small groups, you are requested to answer the following questions related to the identifying IoT Technology Challenges

i. What is one key challenge related to IoT security?
ii. Name one environmental impact challenge associated with IoT devices
iii. Compare IoT security from Data privacy

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.1.4

Key readings 1.1.4:

Identification of IoT Technology Challenges

- **IoT Security:** IoT devices often lack robust security features, making them vulnerable to cyberattacks. Weak authentication, inadequate encryption, and insufficient security updates can expose IoT devices to threats like hacking, data breaches, and malware.
- **Data Privacy:** The vast amount of data collected by IoT devices raises significant privacy concerns. Sensitive personal information can be collected, shared, and potentially misused without proper user consent and control, leading to privacy violations and misuse of data.
- **IoT Devices Safety:** Ensuring the safety and reliability of IoT devices in critical applications. Faulty devices or software bugs can lead to malfunctioning, causing potential harm, especially in healthcare, automotive, and industrial applications where safety is paramount.
- **Interoperability:** Lack of standardization and compatibility among different IoT devices and platforms. Diverse devices and communication protocols can result in integration challenges, leading to fragmented systems that hinder seamless communication and data exchange.
- **Environmental Impact:** The environmental footprint of IoT devices, including energy consumption and electronic waste. The production, operation, and disposal of IoT devices contribute to electronic waste and carbon emissions. Additionally, the energy required to power these devices and their supporting infrastructure can be significant.

Points to Remember

- **Benefits of Implementing IoT are** Enhances efficiency, data analysis, and decision-making, offers cost savings through predictive maintenance and optimization and Improves convenience and quality of life with smart devices.
- **IoT is in** Used in smart home automation**,** Industrial processes **and** Healthcare, and agriculture.

- **Common Devices/Components** Includes sensors, connectivity modules, and microcontrollers, IoT platforms manage data, analytics, and application development.
- **Role of IoT Platforms is to f**acilitate development, deployment, and management of IoT solutions and Manage device connectivity, data handling, and security features.
- **Evolution of IoT Technology and Milestones** progressed from basic communication to complex device ecosystems. Major milestones include IPv6 adoption and the rise of edge computing.
- **Challenges Facing the IoT Industry are** Concerns over security, Interoperability, Scalability and Standardization.
- **Things:** Physical objects with sensors, actuators, and embedded technologies.
- **Internet:** The global network infrastructure, cloud services, and data management systems.
- **Connectivity:** The communication technologies and protocols that enable data exchange.

Application of learning 1.1.

You are working as a technology consultant for a large agricultural company. The company is looking to implement IoT solutions to optimize their farming operations, reduce resource waste, and increase crop yield. As an IoT consultor advise them the components they have to use while designing and implementing an IoT-based agriculture system that monitors soil conditions, weather, and crop health, and automates irrigation and pest control

Indicative content 1.2: Identification of IoT Network Technology

Duration: 4 hrs

Theoretical Activity 1.2.1: Describe Low Range/Low Power

Tasks:

1: In small groups, you are requested to answer the following questions related to the Low Range/Low Power.

i. Which IoT technology is ideal for home automation and has mesh networking capabilities?
ii. What is the primary use of RFID technology in IoT applications?
iii. Which IoT technology is suitable for wearables and health monitors due to its energy efficiency and short to medium range?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.2.1

Key readings 1.2.1.: Describe Low Range/Low Power

- **Low Range/Low Power IoT Networks** are specialized wireless communication networks designed for Internet of Things (IoT) devices that require minimal power consumption and have a limited communication range. These networks are essential for enabling efficient and sustainable connectivity for a variety of IoT applications, particularly those involving battery-powered or energy-constrained devices.

- **Low Power Consumption:** Designed to operate on minimal power, allowing devices to run for extended periods on small batteries. This is crucial for applications where frequent battery replacement or recharging is impractical.
- **Short Range Communication:** Typically cover short distances, making them

suitable for localized applications such as home automation, wearable devices, and smart appliances. **Examples of Low Range/Low Power IoT Networks:**

- ✓ **Zigbee**: Low-power, low-data rate, and short-range wireless communication.

  Applications: Home automation, smart lighting, and industrial automation.

  Features: Mesh networking capabilities, low latency, and scalability.

- ✓ **Wi-Fi 6**: Next-generation Wi-Fi standard offering higher speeds, better performance in dense environments, and improved energy efficiency.

  Applications: Smart homes, smart cities, and IoT devices requiring higher data throughput.

  Features: Improved capacity, lower latency, and enhanced security.

- ✓ **Bluetooth/LE (Low Energy):** Low-power wireless communication with short to medium range.

  Applications: Wearables, health monitors, and proximity sensors.

  Features: Energy-efficient, easy to implement, and suitable for battery-powered devices.

- ✓ **NFC (Near Field Communication):** Short-range, high-frequency wireless communication.

  Applications: Contactless payments, access control, and data exchange between devices.

  Features: Simple tap-based interaction, low power consumption, and secure communication.

- ✓ **RFID (Radio Frequency Identification):** Uses electromagnetic fields to identify and track tags attached to objects.

  Applications: Inventory management, asset tracking, and supply chain logistics.

  Features: Passive and active tags, varying read ranges, and minimal power requirements for passive tags.

- ✓ **Ethernet:** Wired networking technology offering high data rates and reliable connections.

  Applications: Industrial automation, smart buildings, and high-performance IoT applications.

  Features: High-speed data transfer, low latency, and robust security.

Theoretical Activity 1.2.2: Describe Low Range/Low Power

Tasks:

1: In small groups, you are requested to answer the following questions related to the Low Range/Low Power.

i. What is the large range/Low power IoT networks?

ii. Differentiate large range from low range

iii. Enumerate Large range IoT network Technologies

iv. What does LPWAN stand for, and what is its primary benefit?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.2.2

Key readings 1.2.2.:

- **Large Range IoT Networks** are designed to provide long-distance communication for IoT devices. These networks are essential for connecting devices that are spread over wide areas, such as in smart cities, agriculture, and industrial IoT applications.
  - **Long Range Communication**: Capable of covering extensive areas, making them suitable for applications that require connectivity over large distances.
  - **Energy Efficiency**: Designed to balance long-range communication with energy efficiency, ensuring that devices can operate for extended periods on limited power sources.

Examples of Large Range IoT Networks

✓ **LPWAN (Low Power Wide Area Network)**: Low-power, wide-area network designed for long-range communication and extended battery life.

Applications: Smart cities, agriculture, environmental monitoring.

Examples: LoRa, SigFox, NB-IoT.

✓ **Cellular**: Utilizes existing cellular networks for IoT communication, providing

wide coverage and reliable connectivity.

Applications: Connected cars, smart grids, remote monitoring.

Examples: 4G, 5G, LTE.

- ✓ **LoRa (Long Range)**: A type of LPWAN technology known for long-range, low-power communication with strong penetration capabilities. It has Supports low data rates, long battery life, and secure communication.

  Applications: Smart agriculture, environmental monitoring, logistics.

- ✓ **SigFox:** A global LPWAN network offering low power, long-range, and low data rate communication. It has Ultra-narrowband technology, low cost, and widespread coverage.

  Applications: Asset tracking, remote sensor monitoring, smart cities.

- ✓ **WiFi HaLow**: A Wi-Fi standard designed for low-power, long-range IoT applications. It operates in sub-1 GHz frequencies, providing better range and wall penetration.

  Applications: Smart homes, industrial IoT, smart agriculture.

- ✓ **5G**: Next-generation cellular network offering ultra-fast speeds, low latency, and high device density support. It has Enhanced mobile broadband, massive IoT support, ultra-reliable low-latency communication.

  Applications: Autonomous vehicles, smart cities, industrial automation.

- ✓ **LTE (Long Term Evolution)**: High-speed wireless communication standard for mobile devices and data terminals. It has High data rates, low latency, wide coverage

  Applications: Connected vehicles, public safety, remote healthcare.

- ✓ **Satellite**: Uses satellite communication for IoT devices, providing global coverage, including remote and hard-to-reach areas. It has Wide area coverage, suitable for areas without terrestrial network infrastructure.

  Applications: Maritime, remote sensing, global asset tracking.

Points to Remember

- **Low Range/Low Power IoT Networks** are specialized wireless communication networks designed for Internet of Things (IoT) devices that require minimal power consumption and have a limited communication range. These networks are

essential for enabling efficient and sustainable connectivity for a variety of IoT applications, particularly those involving battery-powered or energy-constrained devices.

- **Large Range IoT Networks** are designed to provide long-distance communication for IoT devices. These networks are essential for connecting devices that are spread over wide areas, such as in smart cities, agriculture, and industrial IoT applications.

Application of learning 1.2.

Develop and deploy a smart agriculture system to monitor and manage crop conditions across a large farm. Explore and apply various IoT network technologies to optimize communication between sensors, controllers, and cloud-based systems. You are tasked with designing a comprehensive IoT-based crop monitoring system.

Indicative content 1.3: Description of IoT Architecture and Protocols

Duration: 4 hrs

Theoretical Activity 1.3.1: Description of Physical Model of IoT

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Physical Model of IoT.

i. What do IoT devices and sensors do?
ii. Name one wired and one wireless way to connect IoT devices.
iii. What is the function of a gateway in IoT?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.3.1

Key readings 1.3.1.: Description of Physical Model of IoT

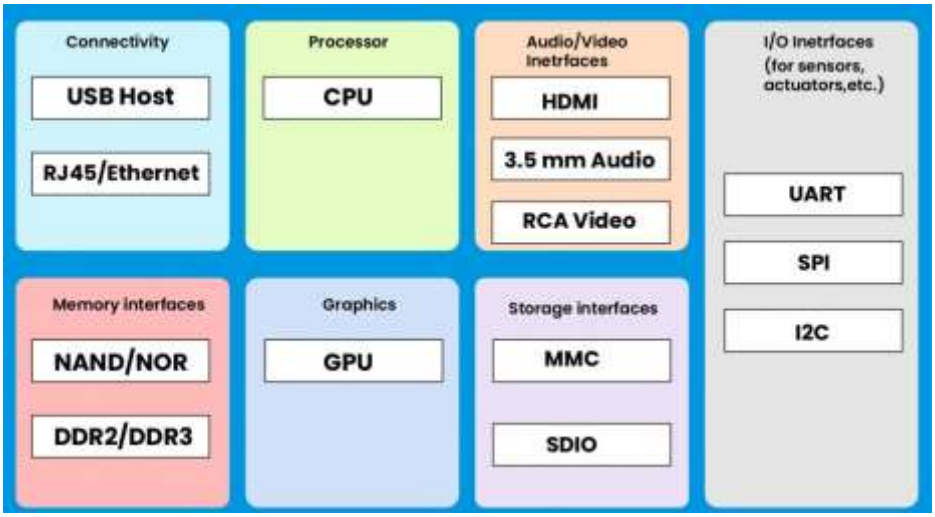
- The physical model of the Internet of Things (IoT) consists of various components that work together to enable connectivity, data exchange, and interaction between devices.

- **IoT Devices/Sensors:** These are the physical objects equipped with sensors, actuators, and communication interfaces. **Their function** is to Collect data from the environment (e.g., temperature, humidity, motion) and send it to the network.

- **Connectivity:** Refers to the communication methods used to connect IoT devices to the internet or other networks. **Wired types**: Ethernet, Powerline communication and **Wireless type:** Wi-Fi, Bluetooth, Zigbee, LPWAN (LoRa, SigFox), Cellular (4G, 5G).

- **Gateway:** A device that acts as an intermediary between IoT devices and the cloud or data center. Aggregates data from multiple devices, manages communication, and may perform local processing or analytics.

- **Cloud/Edge Computing:** Centralized or decentralized processing environments where data is analyzed, stored, and managed.
  - ✓ **Cloud Computing**: Provides scalable resources for data storage and processing, allowing for complex analytics and machine learning.
  - ✓ **Edge Computing**: Processes data closer to where it is generated, reducing latency and bandwidth usage for real-time applications.
- **Data Management and Analytics:** Software and tools used to analyze the data collected from IoT devices. Transform raw data into actionable insights through data visualization, machine learning, and reporting.
- **User Interface:** Platforms through which users interact with IoT systems. Allows users to monitor, control, and manage IoT devices, often through mobile apps, dashboards, or web interfaces.
- **Security and Privacy Mechanisms:** Tools and protocols to ensure the integrity, confidentiality, and availability of IoT systems. Protects against unauthorized access, data breaches, and ensures secure communication between devices.



Theoretical Activity 1.3.2: Description of Logical Model of IoT

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of logical Model of IoT.

i. What does the communication layer do in the logical model of IoT?
ii. How does edge computing help IoT devices?

iii. What is the purpose of the analytics layer?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

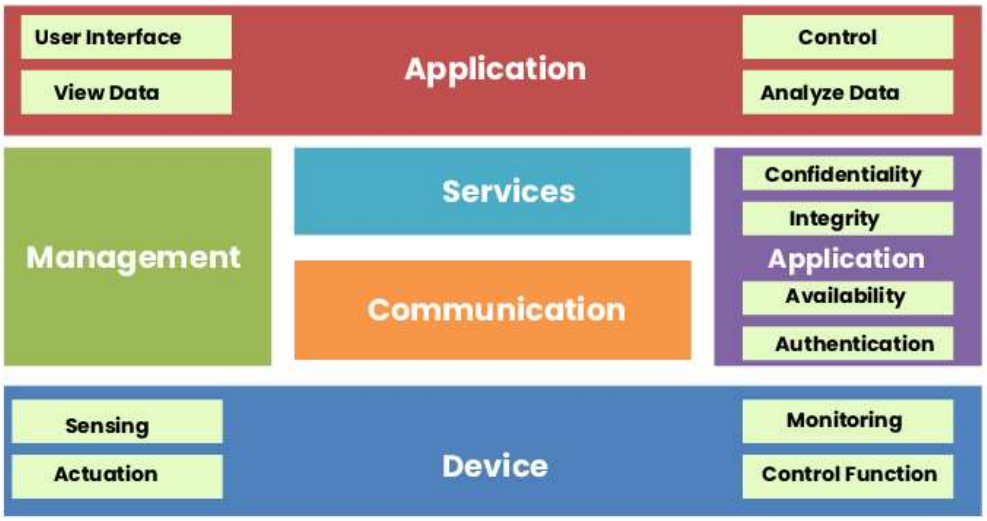
4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.3.2

Key readings 1.3.2:

- The logical model of the Internet of Things (IoT) defines the structure and relationships between different components and processes involved in IoT systems. It focuses on the functionality and data flow rather than the physical implementation. Here's an overview of the key elements:
  - **Device Layer:** Comprises the IoT devices and sensors that collect data. Sensing and actuating capabilities, gathering information from the environment (e.g., temperature, humidity, motion).
  - **Communication Layer:** Facilitates data transmission between devices and the cloud or other systems. This includes various communication protocols such as MQTT, CoAP, HTTP, and different network types (e.g., Wi-Fi, cellular, LPWAN).
  - **Edge Computing Layer:** Processes data closer to the source (IoT devices) to reduce latency and bandwidth usage. Performs local data processing, filtering, and decision-making before sending relevant data to the cloud.
  - **Data Accumulation Layer:** Collects and aggregates data from multiple devices. Manages data storage and ensures data integrity, preparing data for analysis.
  - **Analytics Layer:** Analyses the accumulated data to extract insights and generate meaningful information. Utilizes machine learning, statistical analysis, and data mining to identify patterns, trends, and anomalies.
  - **Application Layer:** Interfaces through which users interact with the IoT system. Provides dashboards, alerts, and control mechanisms to monitor and manage IoT devices.
  - **Security Layer:** Ensures the security and privacy of data and devices. Implements authentication, encryption, and access control measures

throughout the IoT ecosystem.



Theoretical Activity 1.3.3: Description of IoT protocols

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of IoT protocols

i. What is MQTT, and why is it commonly used in IoT applications?
ii. How does CoAP differ from HTTP in terms of its application in IoT?
iii. Name one key feature of LoRaWAN and explain its importance for IoT devices.

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

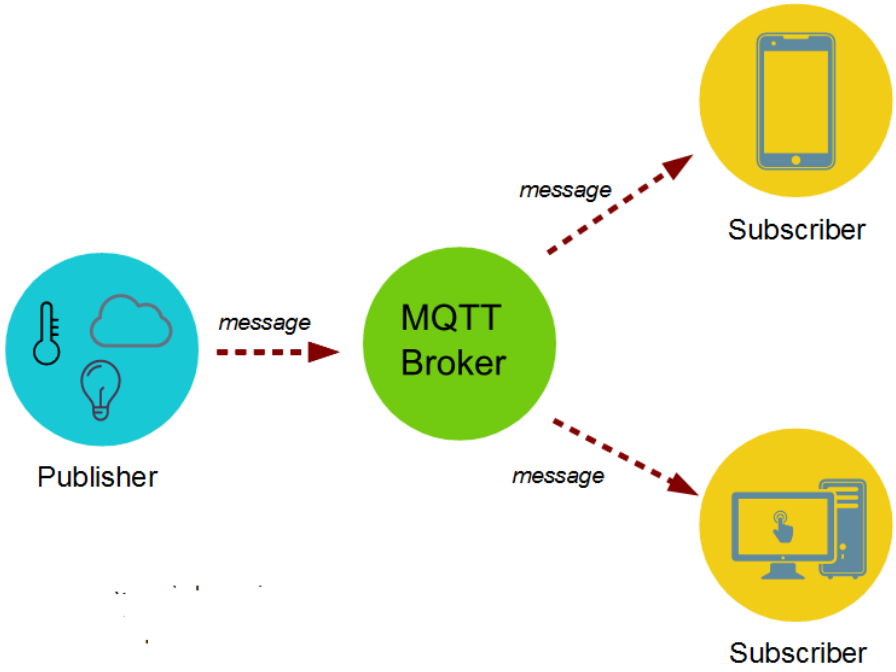
5: For more clarification, read the key readings 1.3.3

Key readings 1.3.3:

IoT protocols are essential for enabling communication between IoT devices, applications, and systems. They define how data is transmitted, formatted, and processed across different networks

- **MQTT**: Message Queue Telemetry Transport Protocol (MQTT) A publish/subscribe messaging protocol ideal for small sensors. It features low bandwidth usage and

reliable message delivery with QoS support.



MQTT (Message Queue Telemetry Transport) is a messaging protocol developed with the aid of Andy Stanford-Clark of IBM and Arlen Nipper of Arcom in 1999 and is designed for M2M communication. It's normally used for faraway tracking in IoT.

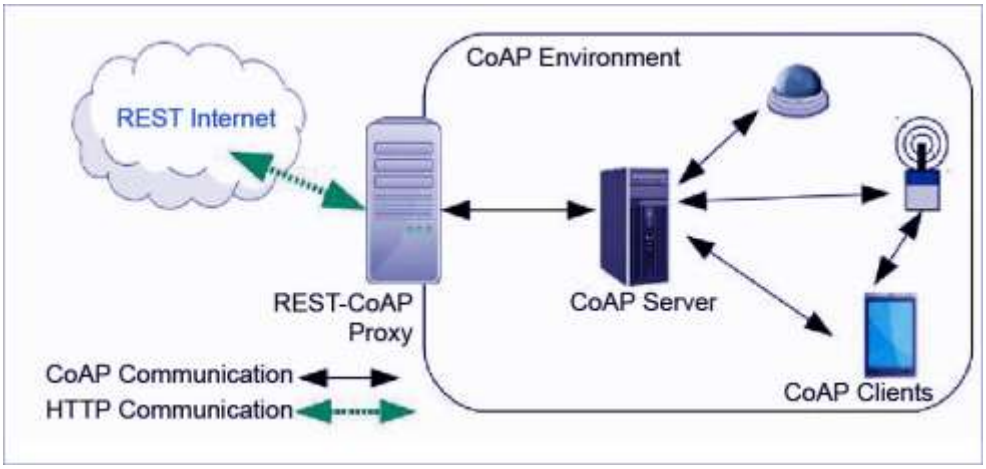
Its primary challenge is to gather statistics from many gadgets and delivery of its infrastructure. MQTT connects gadgets and networks with packages and middleware.

All the devices hook up with facts concentrator servers like IBM's new message sight appliance. MQTT protocols paintings on top of TCP to offer easy and dependable streams of information.

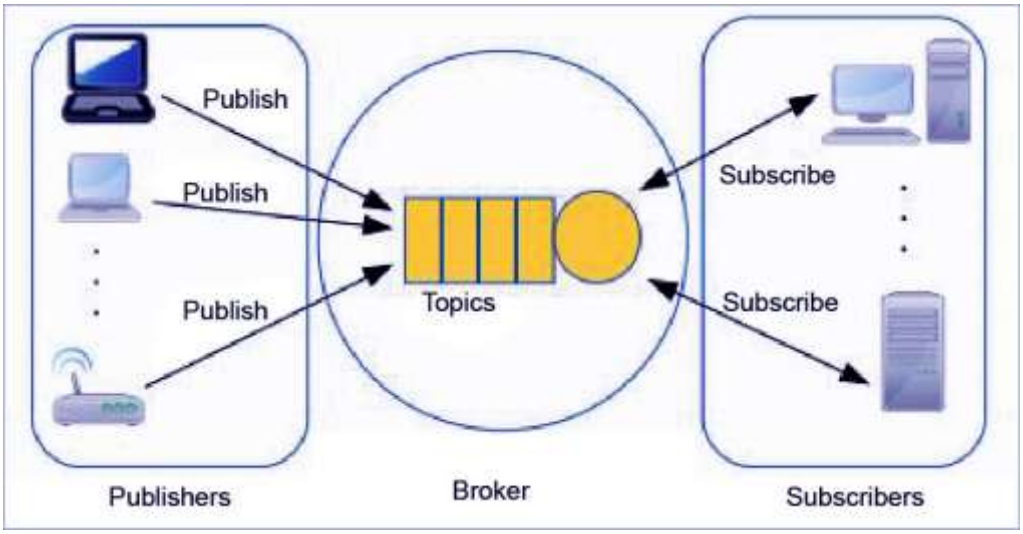
These IoT protocols include 3 foremost additives: subscriber, publisher, and dealer. The writer generates the information and transmits the facts to subscribers through the dealer. The dealer guarantees safety by means of move-checking the authorization of publishers and subscribers.

- **CoAP**: Constrained Application Protocol (CoAP) is an internet utility protocol for constrained gadgets. It is designed to enable simple, constrained devices to join IoT through constrained networks having low bandwidth availability.

  This protocol is primarily used for machine-to-machine (M2M) communication and is particularly designed for IoT systems that are based on HTTP protocols.



CoAP makes use of the UDP protocol for lightweight implementation. It also uses restful architecture, which is just like the HTTP protocol. It makes use of dtls for the cozy switch of statistics within the slipping layer.



- **HTTP/HTTPS**:

HTTP is the abbreviation of HyperText Transfer Protocol. It is the protocol which is applicable in TCP/IP Protocol which includes a group of foundation protocol for internet.

When you type a Web URL into Web browser, a HTTP code will be sent to Web server in order to request and guide to find exactly the website requested. This website will be pulled afterward and presented in Web browser. In another word, HTTP is the protocol helping the file transfer from a Web server to a Web browser that a customer could view a web presented in Web browser.

Characteristics of HTTP

- HTTP is IP based communication protocol that is used to deliver data from server to client or vice-versa.
- Any type of content can be exchanged as long as the server and client are

compatible with it.

- It is a request and response protocol based on client and server requirements.

HTTPS is the abbreviation of HyperText Transfer Protocol Secure. It is the combination of HTTP protocol and secure protocol SSL or TLS which allows the information exchange on Internet happening in a secure way. HTTPS protocol is usually used in sensitive deals that need high security.

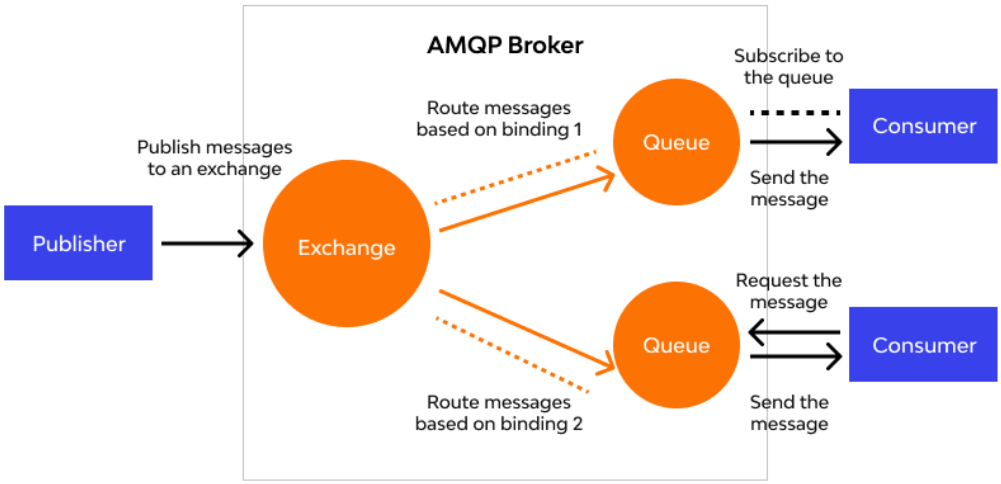
Characteristics of HTTPS

- HTTPS encrypts all message substance, including the HTTP headers and the request/response data. The verification perspective of HTTPS requires a trusted third party to sign server-side digital certificates.
- HTTPS is presently utilized more frequently by web clients than the first non-secure HTTP, fundamentally to ensure page genuineness on all sorts of websites, secure accounts and to keep client communications.

- **AMQP**: Advanced Message Queuing Protocol (AMQP)

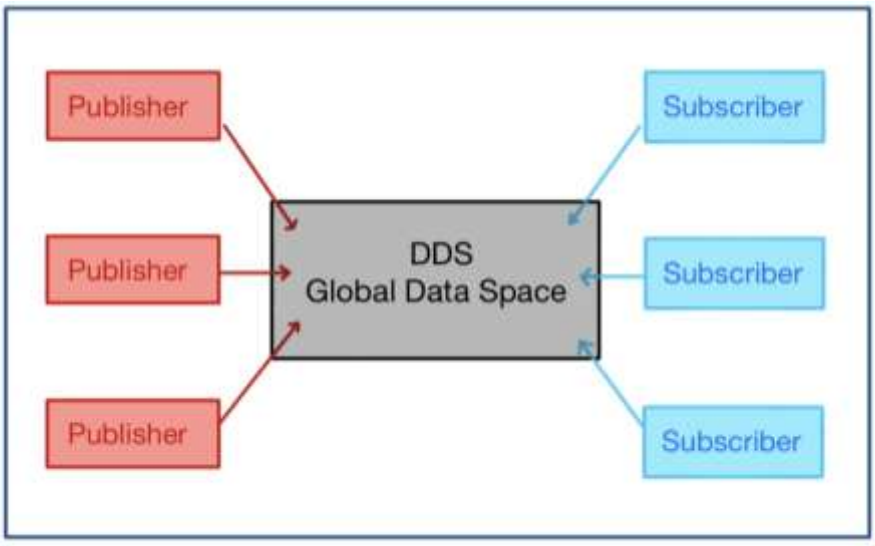
A message-oriented middleware protocol that supports reliable business messaging and communication in IoT. It supports reliable verbal exchange through message transport warranty primitives like at-most-once, at least once and exactly as soon as shipping.

The AMQP – IoT protocols consist of hard and fast components that route and save messages within a broker carrier, with a set of policies for wiring the components together. The AMQP protocol enables patron programs to talk to the dealer and engage with the AMQP model.

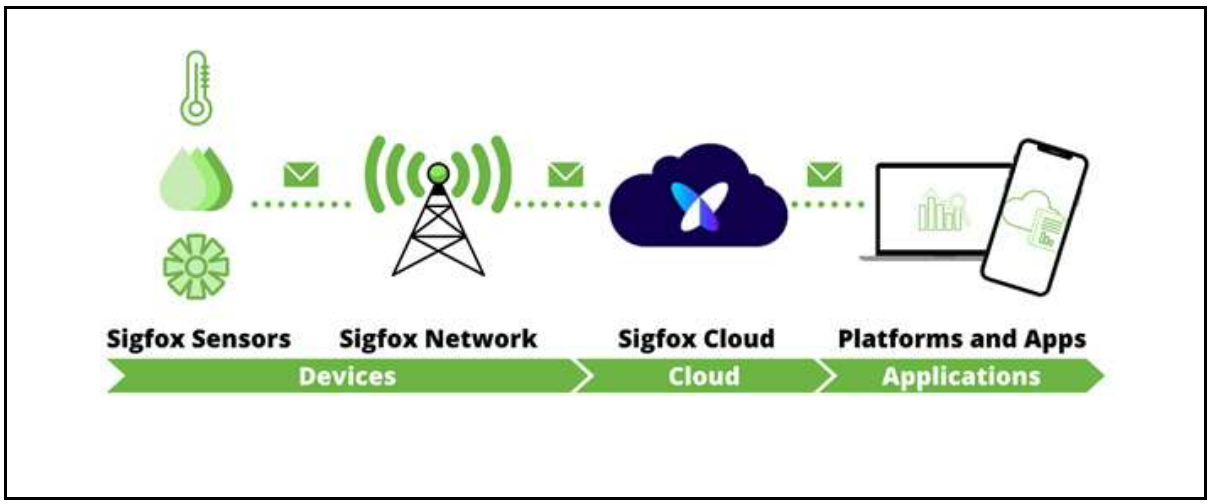


- **DDS**: A middleware protocol for real-time data exchange in industrial applications, utilizing a publish/subscribe model. Data Distribution Service (or DDS) is a fully distributed Global Data Space, which makes it fully distributed to avoid introducing a single point of failure or bottleneck.

DDS ARCHITECTURE



- **SigFox**: An LPWAN protocol for low-bandwidth IoT devices, ideal for applications like asset tracking and environmental monitoring, featuring ultra-narrowband technology.



Points to Remember

- The physical model of the Internet of Things (IoT) consists of various components that work together to enable connectivity, data exchange, and interaction between devices.
- The logical model of the Internet of Things (IoT) defines the structure and relationships between different components and processes involved in IoT systems. It focuses on the functionality and data flow rather than the physical implementation.
- IoT protocols are essential for enabling communication between IoT devices, applications, and systems. They define how data is transmitted, formatted, and processed across different networks

Indicative content 1.4: Calibration of Tools, Equipment and Materials

Duration: 4 hrs

Theoretical Activity 1.4.1 Description of calibration

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of calibration.

i. What is the purpose of calibration in maintaining measurement instruments?
ii. Why is calibration important for quality control?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 1.4.1

Key readings 1.4.1.: Description of calibration

- **Definition**
  Calibration is the process of adjusting and verifying the accuracy of measurement instruments by comparing their outputs against a known standard or reference. This ensures that the instruments provide precise and accurate measurements within specified limits**.**
- **Purpose:** The primary purpose of calibration is to maintain the accuracy and reliability of measurement instruments. This process helps to:
  - ✓ Ensure Accuracy: Verify that instruments provide correct measurements.
  - ✓ Maintain Consistency: Ensure consistent measurements over time.
  - ✓ Compliance: Meet regulatory and industry standards.
  - ✓ Quality Control: Enhance the quality and reliability of products and processes.
  - ✓ Minimize Errors: Reduce measurement errors and uncertainty**.**
- **Calibration techniques for IoT networks**

Manual Calibration:

- ✓ Direct comparison: Sensors are compared against a known standard or reference device.
- ✓ Calibration curves: A calibration curve is created by measuring the sensor's output at various known input values.
- ✓ Suitable for simple sensors and infrequent calibration.

Automatic Calibration:

- ✓ Self-calibration: Sensors use internal algorithms to adjust their output based on environmental conditions or internal measurements.
- ✓ External calibration: Sensors receive calibration data from a central server or external device.
- ✓ Suitable for large-scale deployments and frequent calibration.

Statistical Calibration:

- ✓ Regression analysis: Statistical models are used to fit calibration curves based on historical data.
- ✓ Bayesian methods: Probabilistic models are used to incorporate uncertainty and prior knowledge into the calibration process.
- ✓ Suitable for sensors with noisy or uncertain data.

Machine Learning Calibration:

- ✓ Neural networks: Deep learning models can learn complex relationships between sensor inputs and outputs.
- ✓ Support vector machines: SVM can be used for classification or regression tasks in calibration.
- ✓ Suitable for complex sensor systems and non-linear relationships.

Cloud-Based Calibration:

- ✓ Centralized calibration: Calibration data and algorithms are stored in the cloud, allowing for efficient management and updates.
- ✓ Distributed calibration: Calibration data is collected from multiple sensors and processed in the cloud.
- ✓ Suitable for large-scale IoT deployments and remote sensor management

Practical Activity 1.4.2: Calibration of tools, equipment and materials

Task:

1: Read the given task

An HVAC (heating, ventilation, and air conditioning) system in a residential community is monitored and controlled by means of a temperature sensor that is part of the smart home systems. To guarantee that these sensors produce accurate temperature readings and maintain the best possible levels of comfort and energy efficiency in the homes, regular calibration is necessary. You are asked to calibrate the temperature sensor in your capacity as an IoT technician installer who is in charge of maintaining these smart home devices.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present your work to the trainer and whole class

5: Read the key reading 1.4.2 and ask clarification where necessary perform the task provided in application of learning 1.4.

Key readings 1.4.2

- **Calibration Process:**

Step 1: Set the Temperature Bath:

- ✓ Adjust the water bath to a series of known reference temperatures (e.g., 0°C, 25°C, and 50°C).
- ✓ Allow the water bath to stabilize at each temperature point.

Step 2: Place Sensors in Bath:

- ✓ Immerse both the temperature sensor from Home #5 and the reference thermometer in the water bath.
- ✓ Ensure they are at the same depth and in close proximity to each other to minimize temperature variations.

Step 3: Record Readings:

- ✓ After allowing sufficient time for stabilization, record the readings from both the temperature sensor and the reference thermometer at each set point.

- ✓ Repeat this process for all the reference temperatures.

Step 4: Compare and Adjust:

- ✓ Compare the readings from the temperature sensor with the reference thermometer.
- ✓ Adjust the temperature sensor if discrepancies are found, following the manufacturer's instructions or using the calibration software.
- ✓ Document any adjustments made.

- **Documentation**:
  - ✓ Log Data: Record all calibration data, including the date, sensor details, reference values, and sensor readings at each temperature set point.
  - ✓ Calibration Certificate: Generate a calibration certificate that includes the date, details of the temperature sensor, standards used, and calibration results. Attach this certificate to the sensor's documentation.
- **Post-Calibration Check:**
  - ✓ Final Verification: Perform a final check at room temperature to ensure the temperature sensor remains accurate after calibration.
  - ✓ Marking: Seal or mark the temperature sensor to indicate it has been calibrated and is ready for reinstallation.
- **Reinstallation and Testing:**
  - ✓ Reinstall: Place the calibrated temperature sensor back into its original position in the HVAC system of Home #5.
  - ✓ System Test: Run a test of the HVAC system to ensure the temperature sensor accurately controls the system.
  - ✓ Report: Provide a calibration report to the homeowner, explaining the process and assuring them of the sensor's accuracy.
- **Periodic Recalibration:**
  - ✓ Schedule: Establish a recalibration schedule for the temperature sensor, typically every 6-12 months, depending on usage and environmental conditions.
  - ✓ Monitoring: Regularly monitor the sensor's performance during maintenance checks and recalibrate as needed to maintain accuracy.

Points to Remember

- **Definition:** Calibration is the process of adjusting and verifying the accuracy of measurement instruments by comparing their outputs against a known standard or reference. This ensures that the instruments provide precise and accurate measurements within specified limits**.**
- **Purpose:** The primary purpose of calibration is to maintain the accuracy and reliability of measurement instruments.

Application of learning 1.4.

Gasabo Plaza is commercial building which their owner want install HVAC for temperature and Humidity conditions. As IoT technician you are asked to interpret the datasheet effectively to ensure that the selected device will meet your IoT project requirements and integrate smoothly into your system**.**

Indicative content 1.5: Interpretation of Manual/Datasheet

Duration: 4 hrs

Practical Activity 1.5.1: Interpretation of Manual/Datasheet

Task:

1: Read the given task

You are working on an IoT project to monitor room temperature using a DHT22 temperature and humidity sensor. Before integrating the sensor into your system, you need to interpret its datasheet to ensure proper usage and functionality

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, perform the given tasks

4: Present your work to the trainer and whole class

5: Read key reading 1.5.1and ask clarification where necessary Perform the task provided in application of learning 1.5.

Key readings 1.5.1: Interpretation of Manual/Datasheet

- **Read the Overview:** You find that the DHT22 is designed for measuring temperature and humidity accurately, making it suitable for your monitoring project.
- **Check Electrical Specifications:** The datasheet specifies an operating voltage of 3.3V to 6V. You confirm that your power supply provides 5V, which is compatible.
- **Review Performance Characteristics:** The measurement range for temperature is -40°C to +80°C, and the accuracy is ±0.5°C. This meets your requirements for monitoring indoor temperatures.
- **Examine Communication Protocols:** The DHT22 uses a single-wire digital signal for communication. You check your microcontroller's capabilities and confirm it can support this protocol.
- **Look at Mechanical Characteristics:** The datasheet includes dimensions and pin

configuration, helping you plan the physical layout of your sensor in the project.

- **Analyze Environmental Specifications:** The sensor operates within a temperature range of -40°C to +80°C and a humidity range of 0% to 100%. You ensure these conditions are suitable for your intended use.
- **Follow Calibration Instructions:** The datasheet states the sensor comes factory calibrated, so you won't need to perform additional calibration, simplifying your setup.
- **Study the Application Circuit:** The provided schematic shows how to connect the sensor to your microcontroller, guiding you in the wiring process.

Points to Remember

Understanding Manuals and Datasheets

Manuals and datasheets are essential documents that provide crucial information about electronic components, devices, or systems. They serve as guides for installation, operati on, maintenance, and troubleshooting.

Components of Manuals and Datasheets

- ✓ **Introduction:** This section typically outlines the purpose of the document, provides a brief overview of the product, and lists any relevant safety warnings.
- ✓ **Specifications:** This section details the technical characteristics of the product, such as dimensions, weight, power consumption, operating temperature range, and in put/output specifications.
- ✓ **Installation Instructions:** This section provides step-by-step guidance on how to ins tall the product, including any necessary tools or equipment.
- ✓ **Operation Instructions:** This section explains how to use the product effectively, in cluding any specific procedures or precautions.
- ✓ **Maintenance and Troubleshooting:** This section offers advice on routine maintena nce tasks and troubleshooting steps to address common issues.
- ✓ **Warranty Information:** This section outlines the warranty terms and conditions, in cluding any limitations or exclusions.

Application of learning 1.5.

Gasabo Plaza is commercial building which their owner want install HVAC for temperature and Humidity conditions. As IoT technician you are asked to interpret the datasheet effectively to ensure that the selected device will meet your IoT project requirements and integrate smoothly into your system**.**

Learning outcome 1 end assessment

Theoretical assessment

1. **Which of the following is NOT a benefit of IoT?**

    a) Enhanced Efficiency

    b) Improved Decision Making

    c) Increased Manual Labor

    d) Cost Savings

2. **Which protocol is commonly used for low-power IoT devices to communicate?**

    a) HTTP

    b) MQTT

    c) FTP

    d) SMTP

3. **What is the primary purpose of calibration in IoT?**

    a) To improve the physical appearance of devices

    b) To ensure the accuracy and reliability of measurements

    c) To increase the speed of data transmission

    d) To reduce the size of IoT devices

4. **Match the IoT components with their descriptions:**

Column A: IoT System Components	**Column B: Functions**
1. Sensors	a) Execute actions based on data received
2. Actuators	b) Collect data from the environment
3. Connectivity Modules	c) Process data received from sensors
4. Microcontrollers/Microprocessors	d)Enable communication between devices

5. **Match the following:**

Column A: IoT System Components	**Column B: Functions**
1.Sensors and Actuators	a. Facilitates efficient energy usage in devices
2.Communication Protocols	b. Defines how devices communicate in the network
3.Data Storage	c. Stores and manages data collected from devices
4.Power Management	d. Collect and transmit data from the physical world

6. IoT devices always guarantee data privacy. True / False
7. Zigbee and Bluetooth are examples of large range IoT network technologies. True / False
8. IoT devices can help improve decision-making by providing real-time data. True / False
9. NFC and RFID are examples of large range IoT network technologies. True / False

Practical assessment

A&B is company in charge of Preparing IoT system installation. They need to prepare smart lights in a residential setting. Your focus is on the meticulous steps leading up to the actual installation of the smart lights. As a skilled technician, you've been assigned to prepare for the installation of an IoT smart lighting system in a residential. Your tasks involve the systematic preparation, including the identification of IoT network technology, description of IoT architecture and protocols, and the calibration of tools, equipment, and materials.

The duration of the work is 3 hours.

Resources

Tools	Plier, screwdriver and Web browser software
Equipment	IoT-enabled Smart Light Bulbs, Home Automation Hub (e.g., SmartThings Hub), Mobile Devices (Smartphones), Wi-Fi Network and Existing Lighting Fixtures
Material/Consumable	Internet bundles, power extension, electricity

END

References

"Internet of Things: Principles and Paradigms" *Edited by Rajkumar Buyya, Amir V

"The Internet of Things: A Look at Real-World Use Cases and the Future of IoT" *By Richard J. K. Liu*

"Internet of Things: Technologies and Applications for a New Age of Intelligence" *By Michael Miller*

"IoT Networks and Communications" By M. A. G. Nair, S. V. M. Chavan.

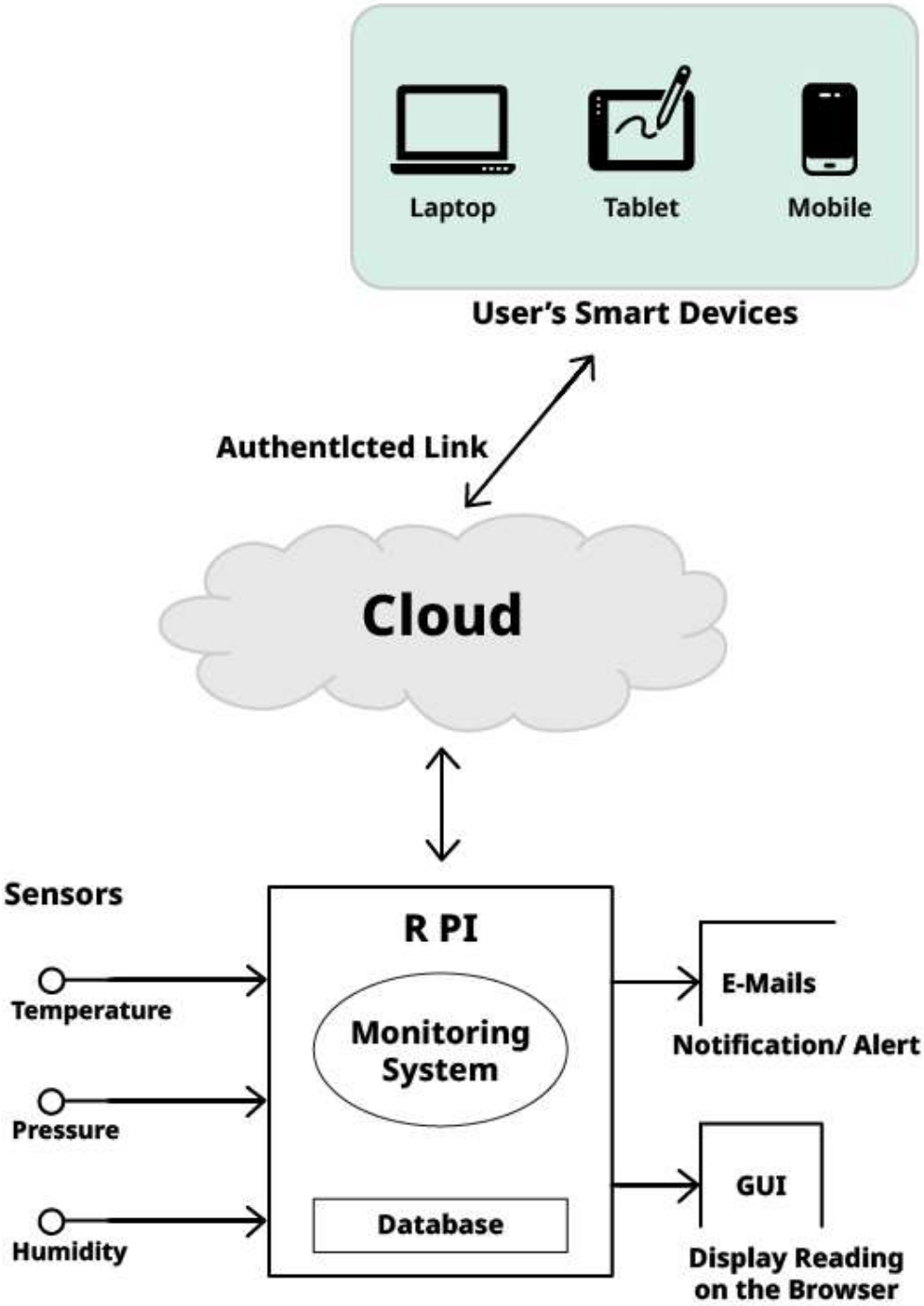
"Architecting the Internet of Things: State of the Art" *By Dieter Uckelmann, Mark Harrison, Florian Michahelles*

"Introduction to Measurement and Instrumentation" *By Robert G. Seipp*

"Precision Instrumentation and Calibration: Concepts, Techniques, and Applications"

By Gary R. Ruddell

"Measurement and Calibration: A Practical Approach" *By David W. Ziegler*


Laptop
Tablet
Mobile
User's Smart Devices
AuthentIcted Link
Cloud
Sensors
Temperature
Pressure
Humidity
R PI
Monitoring System
Database
E-Mails
Notification/ Alert
GUI
Display Reading on the Browser

Indicative contents
2.1 Performance of workplace Setup
2.2 Identification of IoT deployment levels
2.3 Assembling of IoT equipment
2.4. Configuration of IoT devices
2.5 Implementation of IoT system Security
2.6 Documentation of IoT installation report

Key Competencies for Learning Outcome 2: Deploy IoT Equipment

Knowledge	Skills	Attitudes
• Description Of Basics Of Iot • Description Of Communication Protocols Of IOT • Identification Of Iot Deployment Levels	• Assembling of IoT equipment • Networking Setup and Configuration • Making Integration system • Applying Firmware/Software Installation • Applying IoT Platform Configuration • Applying Security Implementation • Preparing Documentation of IoT installation report	• Having Collaboration Attitudes • Having time management • Being problem solver • Having a Perseverance • Having an Initiative • Having self confidence

Duration:10 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Set properly the workplace according to the installation design
2. Assemble correctly IoT equipment as per the manufacturer's guides
3. Customize appropriately the equipment settings based on the installation
4. Apply properly IoT system protection measures as per the installation manual
5. Perform correctly Functional testing according to the installation requirements
6. Report properly IoT system installation based on the installation requirements

Resources

Equipment	Tools	Materials
● Modem, ● Access Point, ● Computer, ● Microcontrollers ● Arduino Starter Kit	● Software platforms, ● simulation software, ● tape measure, ● multi-meter, ● screwdrivers, ● drilling machine, ● hammer, ● ladder, ● pliers	● Internet connectivity, ● pipes, ● cable trunks, ● electrical tapes, ● screws, ● Labelling tags

Indicative content 2.1: Performance of Workplace Setup

Duration: 1 hr

Theoretical Activity 2.1.1: Study the workplace environment

Tasks:

1: In small groups, you are requested to answer the following questions related to the Study the workplace environment

i. How does your commute distance impact your overall job satisfaction and punctuality?
ii. Are there any physical barriers in your workspace that make it difficult for you to communicate or move around?
iii. Do you feel that the current lighting and HVAC systems in your workplace provide a comfortable and productive environment?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.1.1.

5: In addition, ask questions where necessary.

Key readings 2.1.1.: Study the workplace environment

- **Distance**
  - **Commute Distance**: Assess the average distance employees travel to work. This can impact punctuality, stress levels, and overall job satisfaction.
  - **Workstation Proximity**: Evaluate the distance between workstations, departments, and facilities (like restrooms, break rooms, etc.). Proper spacing can promote efficiency and collaboration, while excessive distances can hinder communication and workflow.
  - **Emergency Exits**: Ensure that emergency exits are easily accessible from all work areas.
- **Physical Obstacles**
  - **Barriers and Layout**: Identify any physical barriers (walls, partitions, furniture) that might impede movement or communication. An open layout can foster collaboration, but some barriers might be necessary for privacy and noise

reduction.

- **Accessibility**: Ensure that the workplace is accessible to everyone, including individuals with disabilities. This includes ramps, elevators, and wide corridors.
- **Ergonomics**: Assess the ergonomic design of workstations to prevent physical strain and injury. This includes the height of desks, the type of chairs, and the placement of computer monitors.

- **Existing Systems (Source of Power)**
  - **Electrical Outlets**: Ensure there are enough power outlets available in convenient locations for all necessary equipment. Consider the placement of outlets to avoid overloading circuits and minimize the need for extension cords.
  - **Lighting**: Assess the lighting system to ensure it provides adequate illumination for all tasks without causing glare or eye strain. Natural light should be maximized where possible.
  - **HVAC (Heating, Ventilation, and Air Conditioning)**: Evaluate the HVAC system to ensure it maintains a comfortable temperature and good air quality throughout the workplace.
  - **IT Infrastructure**: Ensure that the existing IT infrastructure (Wi-Fi, LAN, servers) can support the technological needs of the organization without frequent downtime or lag.
  - **Safety Systems**: Check for the presence and functionality of safety systems, including fire alarms, sprinklers, and emergency lighting.
- **Additional Considerations**
  - **Noise Levels**: Assess the noise levels in different areas of the workplace. High noise levels can be distracting and stressful, so consider soundproofing or white noise machines if necessary.
  - **Cleanliness and Maintenance**: Ensure regular cleaning and maintenance schedules are in place to keep the workplace safe and hygienic.
  - **Break Areas**: Provide adequate break areas where employees can relax and recharge. These should be comfortable and well-equipped.
  - **Decor and Ambience**: Consider the overall aesthetic of the workplace. A pleasant and well-designed environment can boost morale and productivity.

Practical Activity 2.1.2: Selection of requirements

Task:

1: Read the given task

I&B company ltd need to select Tools, Materials, and Equipment for an IoT Smart Home Automation System. The system will encompass: Lighting control, Climate control (heating and cooling), Security monitoring (cameras, door/window sensors, smart locks), Appliance control (smart plugs, connected appliances) and Energy monitoring and management. As an IoT system installer you are assigned to specify selection of requirements for this system.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to procedures provided on task 2, Perform the given tasks

4: Present your work to the trainer and whole class

5: Read key reading 2.1.2 and ask clarification where necessary Perform the task provided in application of learning 2.1

Key readings 2.1.2

Step-by-Step Instructions:

Step 1: Define Project Requirements

- ✓ **Objective**: Clearly state the goal of your IoT project.
- ✓ **Scope**: Determine the scale of your project (e.g., home automation, industrial monitoring).
- ✓ **Specifications**: List the specific requirements, such as data types, frequency of data collection, and response times.

Step 2: Identify Key Components

- ✓ **Sensors and Actuators**: Select sensors that match your data collection needs (e.g., temperature, humidity, motion). Choose actuators that will interact with the environment (e.g., motors, lights).
- ✓ **Microcontrollers/Microprocessors**: Choose a suitable processing unit (e.g., Arduino, Raspberry Pi) based on your project's computational needs and power constraints.

Step 3: Determine Connectivity Options

- ✓ **Wired Communication**: Evaluate if wired communication (e.g., Ethernet, RS-485) is feasible for your project.
- ✓ **Wireless Communication**: Select appropriate wireless technologies (e.g., Wi-Fi, Bluetooth, Zigbee, LoRaWAN) based on range, power consumption, and data rate requirements.

Step 4: Plan Power Supply

- ✓ **Power Sources**: Determine if your project will use batteries, AC power, or renewable energy sources.
- ✓ **Power Management**: Select voltage regulators, power converters, and backup power solutions to ensure consistent and reliable operation.

Step 5: Choose Software Tools

- ✓ **Development Environment**: Select Integrated Development Environments (IDEs) and programming languages suitable for your hardware (e.g., Arduino IDE, Python, Node-RED).
- ✓ **Cloud Platforms**: Decide on cloud services for data storage, processing, and analytics (e.g., AWS IoT, Google Cloud IoT, Azure IoT).
- ✓ **Security Measures**: Identify security protocols and tools to protect data and devices (e.g., encryption, secure boot, firmware updates).

Step 6: Source Materials and Equipment

- ✓ **Component Suppliers**: Identify reliable suppliers for electronic components, sensors, and boards (e.g., Mouser, Digi-Key, Adafruit).
- ✓ **Prototyping Tools**: Gather essential prototyping tools (e.g., breadboards, jumper wires, soldering kits).
- ✓ **Testing Equipment**: Acquire testing and debugging tools (e.g., multimeters, oscilloscopes, logic analyzers).

Theoretical Activity 2.1.3: Mapping the workplace

Tasks:

1: In small groups, you are requested to answer the following questions related to mapping the workplace.

i. What is mapping workplace?

ii. Why is necessary to map the workplace?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 2.1.3

Key readings 2.1.3

- Workplace mapping is one of the most effective ways of examining the strength and weaknesses of your branch. Mapping is the process of obtaining accurate and relevant information about the workforce in a systematic way. If done properly it can form the basis of most successful union activity, including recruiting, communications, developing activists and campaigning around issues

Practical Activity 2.1.4: Setting up network connectivity

Task:

1: Read the given task

In Small Office, they want to setup network connectivity for IoT devices. You are tasked with setting up network connectivity for a smart office environment, integrating IoT devices to enhance efficiency and connectivity among multiple devices

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present your work to the trainer and whole class

5: Read key reading 2.1.4 and ask clarification where necessary Perform the task provided in application of learning 2.1

Key readings 2.1.4

- **Step1:** Begin by configuring the router to establish a smart network backbone for the office.
    - ✓ Connect the router to the ISP's modem using an Ethernet cable to ensure reliable internet connectivity.
    - ✓ Access the router's web interface through a web browser using the default IP address (e.g., 192.168.1.1).
    - ✓ Follow the setup wizard to configure essential settings such as network name (SSID), Wi-Fi password, and administrative credentials.
    - ✓ Implement WPA3 encryption for advanced Wi-Fi security to protect against unauthorized access.
    - ✓ Set up strong administrative passwords and enable router firewall settings to safeguard IoT devices and data.
- **Step2:** Integrate IoT devices to automate office tasks and enhance productivity.
    - ✓ Connect IoT devices such as smart lights, sensors (temperature, occupancy), and smart plugs to the office network.
    - ✓ Ensure each IoT device is compatible with the chosen Wi-Fi network and can communicate seamlessly.
    - ✓ Use manufacturer-provided apps or web interfaces to configure IoT device settings, including automation schedules and sensor thresholds.
    - ✓ Test IoT device functionality to ensure they operate efficiently and respond appropriately to commands.
- **Step3:** Establish both wired and wireless connections to support a variety of office devices.
    - ✓ Connect desktop computers, printers, and other stationary devices to the router via Ethernet cables for stable and high-speed connectivity.
    - ✓ Configure DHCP or assign static IP addresses to manage device networking within the office environment.

- ✓ Configure Wi-Fi settings to provide seamless connectivity for laptops, smartphones, and mobile devices.
- ✓ Optimize Wi-Fi coverage by positioning the router centrally and consider using Wi-Fi extenders for expanded coverage in larger office spaces.

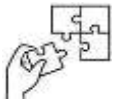
- **Step4:** Implement robust security measures to protect the smart office network and IoT ecosystem.
  - ✓ Segment IoT devices on a separate network or VLAN (Virtual Local Area Network) to isolate potential security risks from office computers and sensitive data.
  - ✓ Regularly update IoT device firmware and apply security patches to mitigate vulnerabilities.
  - ✓ Consider setting up a VPN (Virtual Private Network) for secure remote access to office resources and IoT devices.
  - ✓ Ensure VPN clients are configured on employee devices to encrypt data transmissions and enhance network security.
- **Step5:** Conduct comprehensive testing to ensure the smart office IoT network meets performance expectations.
  - ✓ Test network speeds, latency, and throughput to optimize network performance and ensure efficient data transfer.
  - ✓ Verify seamless communication between IoT devices and office computers for tasks such as file sharing, printing, and collaborative work.
  - ✓ Fine-tune router settings and Wi-Fi configurations based on testing results to enhance network reliability and minimize potential downtime.
  - ✓ Monitor network traffic and IoT device performance to proactively identify and resolve any connectivity issues.

Points to Remember

- **Study the Workplace Environment**
  - Distance: Measure the distances between where IoT devices will be installed and where they need to communicate (e.g., with a central hub or each other). This helps determine the type of communication protocol (e.g., Wi-Fi, Zigbee, LoRaWAN) and whether signal boosters or repeaters are needed.

- Physical Obstacles: Identify any physical barriers (e.g., walls, furniture, machinery) that could obstruct wireless signals. Materials like metal and concrete can significantly reduce signal strength, so their impact on communication must be considered.
- Existing Systems (Source of Power): Evaluate existing infrastructure, such as power sources, to determine where IoT devices can be easily connected. Assess whether there are adequate power outlets, or if additional wiring or battery-powered solutions are necessary. Also, consider the compatibility and integration with existing systems (e.g., HVAC, lighting).

- **Selection of Requirements**
  - Tools: List and gather the necessary tools for installation, such as screwdrivers, drills, crimping tools, network testers, and multimeters. Ensure that all tools are suited for the specific equipment being installed.
  - Equipment: Select the appropriate IoT devices (sensors, actuators, controllers, communication modules) based on the environment's requirements. Consider factors like durability, environmental resistance (e.g., waterproofing), and compatibility with the overall system.
  - Materials: Identify all required materials such as cabling, connectors, mounting brackets, and enclosures. Make sure you have the correct types and quantities to avoid interruptions during installation.
- Mapping the Workplace: Create a detailed map or layout of the workplace, marking the locations of all IoT devices, power sources, and network infrastructure. This visual guide helps in planning the installation process and ensuring that all components are optimally placed for both functionality and ease of maintenance.
- **Setup Network Connectivity**
  - Network Configuration: Plan and configure the network to ensure reliable connectivity for all IoT devices. Choose the appropriate network type (e.g., wired, Wi-Fi, mesh network) based on the environment. Ensure that the network can handle the data load and that all devices are within the coverage area.
  - Security Setup: Implement robust security measures, such as encryption, firewalls, and secure passwords, to protect the IoT network from unauthorized access and potential cyber threats.
  - Testing: Conduct tests to verify network connectivity and signal strength throughout the workplace. Ensure that all IoT devices can communicate effectively and that there are no dead zones or weak signals.



Application of learning 2.1

KGL company want to set up the new office space, it has the role of studying the environment to ensure optimal setup for efficiency and productivity. Choose the right tools, equipment, and materials necessary for setting up a functional and efficient workplace. Establish a reliable and secure network infrastructure to perform the workplace setup for the new office operations.

Indicative content 2.2: Identification of IoT Deployment Levels

Duration: 2 hrs

Theoretical Activity 2.2.1: Description of IoT deployment levels

Tasks:

1: In small groups, you are requested to answer the following questions related to

i. Description of IoT deployment levels List and explain IoT levels

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 2.2.1

Key readings 2.2.1.: Description of IoT deployment levels

Level-1: Device Connectivity: The foundational level where IoT begins, focusing on connecting physical devices to the internet or a local network.

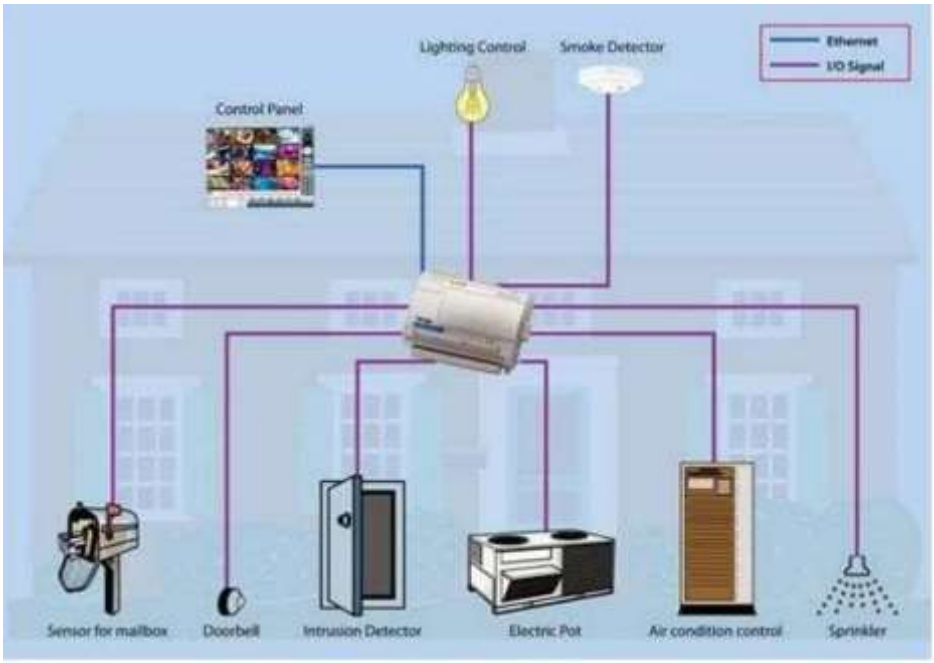
Characteristics:

Basic sensors and actuators are connected.

Devices transmit data to a centralized system or platform.

Limited data processing capability on the device itself.

Examples: Smart home devices (like thermostats and lights), basic industrial sensors.



- **Level-2: Device Management and Monitoring:** Building on Level-1, this level emphasizes managing and monitoring connected devices efficiently.

  Characteristics:

  ✓ Remote monitoring of device status and health.

  ✓ Basic device management functionalities like firmware updates and configuration changes.

  ✓ Simple security measures implemented.

  Examples: Smart irrigation

- **Level-3: Data Integration and Analytics:** Focuses on integrating data from multiple devices and applying basic analytics for insights.

  Characteristics:

  ✓ Data aggregation from various IoT devices into a centralized platform or cloud.

  ✓ Basic analytics and visualization tools used to derive insights.

  ✓ Data used for monitoring and simple automation rules.

  Examples: Energy management systems, predictive maintenance applications.

Sensors used

Accelrometer

sense movement or vibrations

Gyroscope

Gives orientation info

- **Level-4: Advanced Analytics and Automation**: Integrates advanced analytics techniques and automation to optimize processes based on IoT data.

  Characteristics:

  ✓ Utilization of machine learning and predictive analytics for deeper insights.

  ✓ Real-time decision-making capabilities based on IoT data.

  ✓ Integration of IoT data with enterprise systems (ERP, CRM) for operational optimization.

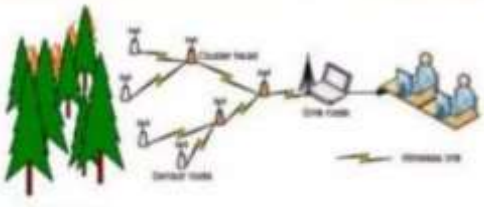
  Examples: Noise monitoring

Sound Sensors are used

- **Level-5: Autonomous Systems:** The highest level where IoT systems operate autonomously with minimal human intervention.

Characteristics:

- ✓ AI-driven decision-making and autonomous actions based on IoT data.
- ✓ Closed-loop systems that continuously optimize operations.
- ✓ Adaptive systems that learn and improve over time.
- ✓ Examples: Autonomous vehicles, smart cities infrastructure, advanced healthcare monitoring.



- **Level-6: Integrated Ecosystems:** This level involves fully integrated ecosystems where IoT systems are seamlessly interconnected across multiple domains.

Characteristics:

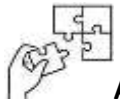
- ✓ Comprehensive integration of IoT devices, systems, and platforms.
- ✓ Interoperability across different IoT technologies and standards.
- ✓ Scalable architectures supporting large-scale deployments.

Examples: Weather monitoring system

Points to Remember

- Identification of IoT deployment levels is essential for planning and managing the deployment of an IoT system. These levels represent the different stages or layers at which IoT components are deployed and integrated within a system. Understanding

these levels helps in organizing the deployment process, ensuring that each component functions optimally within the larger system.



Application of learning 2.2

QZ company is a large-scale farm which wants to implement a smart irrigation system to optimize water usage, increase crop yield, and reduce labor costs. The farm is divided into multiple zones, each growing different crops with varying water needs. The goal is to automate the irrigation process based on real-time data from the field. Describe the IoT deployment levels that will be applied.

Indicative content 2.3: Assembling of IoT Equipment

Duration: 2 hrs

Theoretical Activity 2.3.1: Manufacturer's guide interpretation

Tasks:

1: In small groups, you are requested to answer the following questions related to

i. Define the manufacturer's guides
ii. What is the importance of manufacturer's guides

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.3.1.

5: In addition, ask questions where necessary.

Key readings 2.3.1.: Manufacturer's guide interpretation

- **Definition of Manufacturer's Guides:** Manufacturer's guides are documents provided by product manufacturers that contain instructions, specifications, and recommendations for the installation, operation, and maintenance of their products.
- **Importance of Manufacturer's Guides:** Manufacturer's guides provide crucial information on how to correctly install, operate, and maintain products, ensuring optimal performance and longevity. They help users avoid errors, accidents, and damage to the product, as well as ensure compliance with safety regulations and warranty requirements

Practical Activity 2.3.2: Fixing of IoT equipment

Task:

1: Read the given task

We want to mount and configure IoT devices in a smart office environment for energy efficiency, space utilization, and employee well-being.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present your work to the trainer and whole class

5: Read key reading 2.3.2 and ask clarification where necessary Perform the task provided in application of learning 2.3.

Key readings 2.3.2

- **Steps to follow when fixing IoT devices:**
  - ✓ Evaluate the office layout, identifying key areas for deploying IoT devices, such as workstations, meeting rooms, and common areas.
  - ✓ Choose IoT devices based on the office requirements, including smart lighting for energy efficiency, occupancy sensors for workspace utilization, and environmental sensors for comfort monitoring.
  - ✓ Mount smart lighting fixtures in common areas and workstations, ensuring even distribution.
  - ✓ Mount occupancy sensors in strategic locations, such as above workstations and in meeting rooms.
  - ✓ Install temperature and humidity sensors in areas where environmental conditions may impact employee comfort. Consider mounting sensors away from direct airflow or heat sources for accurate readings.
  - ✓ Place the IoT gateway in a central location within the office to ensure effective communication with all deployed devices.
  - ✓ Connect sensors to the IoT gateway using appropriate wiring and connectors. Conceal wiring where possible to maintain a clean and

organized appearance.

- ✓ Configure each IoT device through the manufacturer's application or a centralized control app. set up automation rules, such as adjusting lighting based on occupancy or optimizing HVAC settings for comfort.
- ✓ Test each device individually to ensure proper functionality. Verify that sensors accurately detect occupancy, control lighting, and provide real-time environmental data.

Points to Remember

- Assembling IoT equipment involves understanding the manufacturer's instructions and properly installing and securing the devices in their designated locations. Here's a guide to help you through this process:
  - ✓ **Manufacturer's Guide Interpretation**

- **Understanding the Components**: Begin by familiarizing yourself with all the components provided in the IoT equipment package. The manufacturer's guide usually includes a list of parts, detailed diagrams, and descriptions that help identify each component.

- **Assembly Instructions**: Carefully read through the step-by-step instructions provided by the manufacturer. Pay attention to the order of assembly, as following the correct sequence is crucial for proper device operation. Take note of any special tools required for assembly, such as specific screwdrivers, wrenches, or crimping tools.

- **Safety Guidelines**: Review any safety precautions listed in the guide to avoid potential hazards during assembly. This may include guidelines on handling sensitive electronic components, avoiding static discharge, and ensuring devices are powered off before assembly.

- **Technical Specifications**: Interpret the technical specifications provided for each component, such as power requirements, communication interfaces, and environmental conditions. This ensures that the equipment is assembled and deployed in a way that meets these specifications.

- **Troubleshooting Tips**: The guide often includes troubleshooting tips for common issues that may arise during assembly. Understanding these can help resolve problems quickly without damaging the equipment.

✓ **Fixing of IoT Equipment**

- **Mounting the Equipment**: Identify the correct mounting locations for the IoT devices as specified in the manufacturer's guide. Ensure that the location is suitable in terms of accessibility, signal strength, and environmental conditions. Use the recommended mounting brackets, screws, or adhesives provided or specified in the guide. Ensure that the equipment is securely fastened to prevent it from moving or falling, which could cause damage or impact performance.

- **Connecting Power**: Connect the IoT equipment to the appropriate power source, following the manufacturer's guidelines. If the device is battery-powered, insert the batteries as directed. For wired devices, ensure that the power cables are securely connected and protected from potential damage. Verify that the power specifications match the requirements of the device to avoid overloading or underpowering the equipment.

- **Wiring and Cabling**: Properly connect all necessary wires and cables as per the instructions. This includes power cables, communication cables (e.g., Ethernet, serial connections), and any antennae or external sensors. Organize and secure cables to prevent tangling or accidental disconnection. Use cable ties or clips to keep wiring neat and out of the way.

- **Device Configuration**: After fixing the equipment in place, proceed with any initial configuration required. This may involve setting up communication parameters, calibrating sensors, or assigning device IDs. Refer back to the manufacturer's guide for specific configuration instructions and settings.

- **Testing the Installation**: Once the equipment is fixed and powered, perform initial tests to ensure that it is functioning correctly. This may involve checking sensor readings, verifying communication with the network, and ensuring that actuators respond to commands. Address any issues that arise during testing, using the troubleshooting section of the manufacturer's guide as needed.

Application of learning 2.3.

Assemble an IoT-based temperature monitoring system for a smart home that collects real-time temperature data and sends it to a central hub, which can be accessed via a smartphone app. Components Required are Microcontroller, Temperature Sensor, Breadboard and Jumper Wires, 5V USB power supply, Wi-Fi Router, IoT Platform and a Smartphone with IoT App: Blynk app or a custom-built app to monitor temperature.

Indicative content 2.4: Configuration of IoT devices

Duration: 2 hrs

Theoretical Activity 2.4.1: Selection of IoT platform

Tasks:

1: In small groups, you are requested to answer the following questions related to select IoT Platform

i. Explain the on-premise IoT platform is an Internet of Things
ii. State the advantages of on-premise IoT platform
iii. Differentiate on premise to cloud IoT platform

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.4.1.

5: In addition, ask questions where necessary.

Key readings 2.4.1.: Selection of IoT platform

- **On-premise**: On-premise is the IT infrastructure and software located within an organization's physical office and hosted on-site. In other words, on-premise means the software is installed on physical hardware that is owned by an organization, located in the physical premises of the organization, usually in the organization's own data center. On-premise is also called on premises or on-prem. With On-Premise, IT staff have more control over the server hardware and the data configuration, security, and management because they can access the data physically. This means your internal teams have access to data and important information, and no third party can access it remotely.

- **The Benefits**
  - ✓ **Compliance:** In-house computing can be more suitable for businesses that need to comply with strict industry regulations, as you have more control over your data and systems. For example, firms in the financial industry may be required to keep all data on-premises.
  - ✓ **Customization:** For businesses with unique requirements, this solution allows you to customize your hardware and software to meet your specific needs.
  - ✓ **Performance:** This computing can offer better performance for specific applications, such as those that require a lot of processing power or need to be accessed offline.

- **Cloud based:** cloud refers to the software, servers, and services that run over the internet rather than locally on the computers and hardware of the organization. Cloud servers are located all around the world in different big data centers. You can access cloud services through your web browsers, such as Google Chrome and Firefox. Some cloud service providers also have dedicated mobile apps to access cloud services.

- **The Benefits**

  - ✓ **Lower Cost:** This solution is typically less expensive than on-premises computing, as you only pay for the resources that you use. This upside can be a significant cost savings for businesses of all sizes.
  - ✓ **Scalability:** Cloud technology is highly scalable, so businesses can easily add or remove resources as needed.
  - ✓ **Accessibility:** Cloud-based applications and data can be accessed from anywhere with an internet connection, which can be helpful for businesses with remote employees or customers

Cloud Vs On Premises Comparison

This table answers the ” What is the difference between on premises and cloud” question.

CLOUD	FEATURE	ON-PREMISES
Software is hosted and managed by a cloud provider.	Deployment	Software is installed and executed on the organization's servers.
Typically, pay-as-you-go subscription model.	Cost	Upfront capital expenditures for hardware and software, ongoing maintenance, and support costs.
It is easy to scale resources up or down as needed.	Scalability	More complicated and expensive to scale.
Applications and data can be accessed from anywhere with an internet connection.	Accessibility	Applications and data are only accessible from within the organization's network.
Cloud providers offer a wide range of security features and certifications.	Security	Security is the responsibility of the organization.
Cloud providers offer compliance solutions for a variety of industry regulations.	Compliance	The organization is responsible for ensuring compliance with all applicable regulations.
Cloud providers have a team of experts who manage and maintain the cloud infrastructure.	Expertise	The organization needs an IT team to manage and maintain its on-premises infrastructure.

Practical Activity 2.4.2: Installation of IoT applications

Task:

1: Read the given task

Download and install the Smart Home IoT software application on your smartphone, enabling you to control and monitor your smart devices.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present your work to the trainer and whole class

5: Read key reading 2.4.2 and ask clarification where necessary Perform the task provided in application of learning 2.4

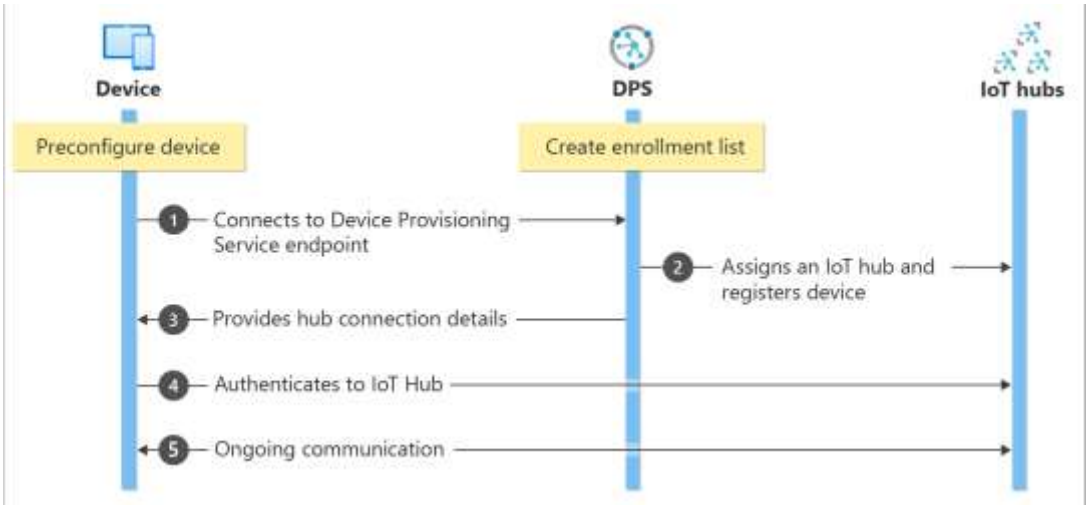
Key readings 2.4.2

- **IoT Device provisioning**

  IoT device provisioning is the process of onboarding and configuring IoT devices so that they can securely connect to a network, communicate with other devices or services, and perform their intended functions. Proper device provisioning is critical for the successful deployment and operation of IoT solutions.

  Proper IoT device provisioning is essential for the security, reliability, and efficient operation of IoT solutions. It ensures that devices are correctly configured, integrated with the IoT platform, and equipped with necessary security measures.

  The following diagram describes what goes on behind the scenes to provision a device with DPS.



Before the device provisioning flow begins, there are two manual steps to prepare:

- ✓ On the device side, the device manufacturer prepares the device for provisioning by preconfiguring it with its authentication credentials and assigned Device Provisioning Service ID and endpoint.
- ✓ On the cloud side, you or the device manufacturer prepares the Device Provisioning Service instance with individual enrollments and enrollment groups that identify valid devices and define how they should be provisioned.

Once the device and cloud are set up for provisioning, the following steps kick off automatically as soon as the device powers on for the first time:

- ✓ The device powers on for the first time, then connects to the DPS endpoint and presents it authentication credentials.
- ✓ The DPS instance checks the identity of the device against its enrollment list. Once the device identity is verified, DPS assigns the device to an IoT hub and registers it in the hub.
- ✓ The DPS instance receives the device ID and registration information from the assigned hub and passes that information back to the device.
- ✓ The device uses its registration information to connect directly to its assigned IoT hub and authenticate.
- ✓ The device and IoT hub begin communicating directly. The DPS instance has no further role as an intermediary unless the device needs to reprovision.

- **IoT Management (Future Ready device management eg: remote configuration, Unified Device Management)**
  - ✓ **Prepare Your Smartphone:** Ensure that your smartphone is connected to a stable Wi-Fi network or has an active mobile data connection. Make sure your smartphone has sufficient storage space for the application.
  - ✓ **Identify the Smart Home IoT Application:** Determine the specific Smart Home IoT application that corresponds to your smart devices. This information is usually provided by the manufacturer or can be found on their official website.
  - ✓ **Access App Store (iOS) or Google Play Store (Android):** Open the App Store if you are using an iPhone (iOS) or the Google Play Store if you are using an Android device.
  - ✓ **Search for the Smart Home IoT Application**: In the search bar, type the name of the Smart Home IoT application you identified in step 2.
  - ✓ **Select the App:** From the search results, select the correct Smart Home IoT application. Ensure that it is developed by the official manufacturer or a reputable developer.
  - ✓ **Check Compatibility:** Verify that the application is compatible with your smartphone's operating system version (iOS or Android). This information is typically visible on the app's store page.
  - ✓ **Read Reviews and Ratings:** Before downloading, check user reviews and ratings to get an idea of the application's performance and reliability.
  - ✓ **Download the Application**: Tap the "Download" or "Install" button on the app's store page. The application will begin to download and install on your smartphone.
  - ✓ **Wait for Installation:** Allow the application to complete the download and installation process. This may take a few minutes, depending on your internet connection speed.
  - ✓ **Open the Application:** Once the installation is complete, tap the "Open" button to launch the Smart Home IoT application.
  - ✓ **Create an Account (if required):** Some Smart Home IoT applications may require you to create an account. Follow the on-screen instructions to set up an account if needed.
  - ✓ **Log In (if applicable):** If you created an account, log in with your credentials. If not, proceed with the provided options, such as connecting

to your smart home devices

- ✓ **Add Smart Devices:** Follow the application's instructions to add and connect your smart devices to the app. This often involves scanning QR codes, pressing buttons on devices, or entering device-specific information.
- ✓ **Configure Settings:** Customize settings within the Smart Home IoT application according to your preferences. This may include naming devices, setting automation rules, or adjusting security settings.
- ✓ **Start Controlling and Monitoring:** Once your smart devices are added and configured, you can start using the Smart Home IoT application to control and monitor them from your smartphone

Practical Activity 2. 4.3: Functional testing

Task:

1: Read the given task

You are a network engineer responsible for conducting functional testing on an IoT system designed for real-time data transmission in a smart manufacturing environment. The goal of this testing is to assess the system's network performance, focusing on speed, latency, jitter, and quality of service (QoS) to ensure it meets the requirements of the manufacturing process. To perform functional testing to evaluate the IoT network's speed, latency, jitter, and QoS parameters to determine if it can support real-time data transmission in a smart manufacturing environment.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present the findings/answers to the whole class

5: For more clarification, read the key readings 2.4.3

6: In addition, ask questions where necessary.

Key readings 2.4.2

- **IoT Functional testing;** Functional testing in the context of IoT Cloud

Applications includes the testing of the scenarios, such as user actions on the applications, data and events coming from the devices, and user actions

- **Speed:** Speed refers to the maximum rate you can transmit data, typically measured as megabits per second (Mbps). Bandwidth refers to the maximum amount of data your connection can handle at any moment, also measured as Mbps (and increasingly Gbps, for gigabyte connections).
- **Latency:** If you are unfamiliar with latency, it is the delay of time between the initiation of a command or input from one side to the reception from the other. It is usually measured in milliseconds (ms).
- **Jitter:** Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and sometimes route changes.
- **QoS:** Quality of service refers to the effectiveness of a network to provide more suitable or appropriate service to the application**.**

Points to Remember

- Speed: Focus on data transmission, processing times, and user interaction responsiveness.
- Latency: Measure round-trip time, command execution time, and data processing delays.
- Jitter: Assess packet delay variation and network stability.
- QoS: Evaluate bandwidth allocation, error rates, and adherence to service levels.

Application of learning 2.4.

Download and install the Smart Home IoT software application on your smartphone, enabling you to control and monitor your smart devices. You, the homeowner, will be responsible for downloading and installing the application on your smartphone.

Indicative content 2.5: Implementation of IoT System Security

Duration: 2 hrs

Theoretical Activity 2.5.1: Setup the security measures

Tasks:

1: In small groups, you are requested to answer the following questions related to Setup the security measures

i. Differentiate Physical from Logical Setup the security measures

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.5.1.

5: In addition, ask questions where necessary.

Key readings 2.5.1.: Setup the security measures

- Setting up security measures for an IoT (Internet of Things) system is crucial to protect data, devices, and the overall ecosystem from various threats and vulnerabilities
  - **Physical:** Physical security involves the use of multiple layers of interdependent systems that can include CCTV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, deterrent systems, fire protection, and other systems designed to protect persons and property.
  - **Logical:** Logical access control is the means by which organizations implement security constraints over proprietary data and broader digital environments. Various logical access control measures at the individual and team levels make up a broader logical security policy at the organizational level. By regulating access in this way, a business can prevent any single user from having too much control over an entire enterprise's digital assets.

Practical Activity 2.5.2: Perform IoT device firmware Update

Task:

1: Read the given task

You are the IoT administrator for a residential complex that uses smart thermostats to control heating and cooling in individual units. It has been determined that a firmware update is necessary to enhance security and add new features to the smart thermostats. As an IoT administrator you are tasked to perform versioning and control IoT firmware update for the smart thermostats.

2 Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks

4: Present the findings/answers to the whole class

5: For more clarification, read the key readings 2.5.2

6: In addition, ask questions where necessary.

Key readings 2.5.2

- **Performing IoT Device Firmware Update**
  - ✓ **Check for Updates**: Regularly check for firmware updates from the device manufacturer.
  - ✓ **Download Update**: Securely download the firmware update package.
  - ✓ **Backup Configuration**: Backup the current configuration and settings of the device.
  - ✓ **Authenticate Update**: Verify the authenticity of the firmware using digital signatures or checksums.
  - ✓ **Deploy Update**: Upload the firmware to the device, either through a management console or over-the-air (OTA) updates.
  - ✓ **Validate Update**: Confirm the update was successful by checking the device

status and functionality.

- ✓ **Restore Configuration**: If necessary, restore the previous configuration and settings.
- ✓ **Monitor Device**: Ensure the device operates correctly post-update and monitor for any issues.

- **Firmware Versioning**
  - **Semantic Versioning**: Use a versioning scheme like Semantic Versioning (MAJOR.MINOR.PATCH):
    - ✓ **MAJOR**: Increases when there are incompatible API changes.
    - ✓ **MINOR**: Increases when functionality is added in a backward-compatible manner.
    - ✓ **PATCH**: Increases for backward-compatible bug fixes.
  - **Version Tracking**: Keep detailed records of all firmware versions, including release notes and changes made in each version.
  - **Deprecation Policy**: Establish a policy for deprecating old firmware versions and communicate it clearly to users.
- **Firmware Control**
  - **Centralized Management**: Use a centralized management system to control and deploy firmware updates across multiple devices.
  - **Staged Rollout**: Implement staged rollouts to deploy updates to a subset of devices first, monitor for issues, and then proceed to a wider deployment.
  - **Rollback Mechanism**: Ensure there is a mechanism to roll back to the previous firmware version if the update causes issues.
  - **Secure Distribution**: Distribute firmware updates securely to prevent tampering. This includes using encrypted channels and verifying firmware integrity.
  - **Compliance and Policies**: Adhere to regulatory requirements and internal policies regarding firmware updates and management.
- **Tools and Technologies**
  - ✓ **Firmware Over-the-Air (FOTA)**: Solutions like AWS IoT Device Management, Azure IoT Hub, and Google Cloud IoT provide OTA update capabilities.
  - ✓ **Device Management Platforms**: Platforms such as Balena, Mender, and

Particle offer comprehensive device management and firmware update features.

- ✓ **Version Control Systems**: Use version control systems (e.g., Git) for managing firmware source code and changes.

Points to Remember

- **Firmware Versioning:** Firmware versioning refers to the systematic labeling of firmware updates using a version number or code to differentiate between different iterations of the firmware.
- **Firmware Control:** Firmware control encompasses the processes, tools, and strategies used to manage the deployment, security, and overall lifecycle of firmware updates across IoT devices.

Comparison

Aspect	**Firmware Versioning**	**Firmware Control**
Focus	Systematic labeling and tracking of firmware versions	Management, security, and deployment of firmware updates
Scope	Version numbering, release notes, compatibility, deprecation	Centralized management, staged rollout, security, compliance
Purpose	Differentiates between firmware iterations	Ensures secure, efficient, and controlled deployment
Tools	Version control systems (e.g., Git)	IoT management platforms (e.g., AWS IoT, Azure IoT, Balena)
Processes	Versioning schemes, record keeping, documentation	Deployment workflows, rollback mechanisms, monitoring
Key Benefits	Clear version history, easier troubleshooting, compliance	Enhanced security, reduced downtime, efficient updates
Challenges	Maintaining compatibility, managing multiple versions	Securing updates, managing large-scale deployments

Application of learning 2.5

A company that manufactures smart home devices, including smart thermostats and security cameras, has released a new firmware update. This update includes security patches, performance enhancements, and new features like improved voice control and automated scheduling. You as IoT technician you are asked to update the firmware on all smart home devices in customers' homes to ensure they benefit from the latest improvements and security patches.

Indicative content 2.6: Documentation of IoT installation report

Duration: 1 hr

Theoretical Activity 2.6.1: Data and facts recording

Tasks:

1: In small groups, you are requested to answer the following questions related to Data and facts recording

i. What information should be recorded about the IoT devices installed, and why is it important?

ii. What details should be captured regarding network connectivity during an IoT installation?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 2.6.1.

5: In addition, ask questions where necessary.

Key readings 2.6.1.: Data and facts recording

- **Project Overview**
  - **Project Information**
    - ✓ Project Name: [e.g., Smart Thermostat Installation for ABC Residential Complex]
    - ✓ Location: [e.g., ABC Residential Complex, Building 1]
    - ✓ Installation Date: [e.g., July 29, 2024]
    - ✓ IoT Devices Installed: [e.g., 20 Smart Thermostats]
  - **Installation Team**
    - ✓ Lead Technician: [Name, Contact Information]
    - ✓ Team Members: [Names, Roles, Contact Information]
    - ✓ Project Manager: [Name, Contact Information]
  - **Installation Purpose**
    - ✓ Objective: [e.g., To enhance energy efficiency and automate climate

control in individual units]

- **Device Details**
  - **Device Specifications**
    - ✓ Device Type: [e.g., Smart Thermostat]
    - ✓ Manufacturer: [e.g., ThermoTech Inc.]
    - ✓ Model Number: [e.g., TT-3000]
    - ✓ Serial Number(s): [e.g., SN12345678, SN12345679, etc.]
    - ✓ Firmware Version: [e.g., v2.1.5]
  - **Installation Location**
    - ✓ Units Installed: [e.g., Units 201-220]
    - ✓ Exact Placement: [e.g., Central wall in living areas]
  - **Mounting and Power Details**
    - ✓ Mounting Method: [e.g., Wall-mounted with brackets]
    - ✓ Power Source: [e.g., Standard 120V AC]
    - ✓ Power Wiring: [Details of wiring, if applicable]
  - **Network Connectivity**
    - ✓ Connectivity Type: [e.g., Wi-Fi, 2.4 GHz band]
    - ✓ Network Configuration: [e.g., SSID, IP Address Allocation]
    - ✓ Network Security: [e.g., WPA2 encryption, password]
- **Configuration Details**
  - **Initial Configuration**
    - ✓ Network Settings: [e.g., IP Address: 192.168.1.101, Subnet Mask: 255.255.255.0, Gateway: 192.168.1.1]
    - ✓ Device Settings:
    - ✓ Temperature Range: [e.g., 60°F - 80°F]
    - ✓ Schedule Settings: [e.g., Heating from 6 AM to 8 AM, Cooling from 4 PM to 8 PM]
    - ✓ User Preferences: [e.g., Preferred temperature settings for different

times of day]

- **Integration**
  - ✓ System Integration: [e.g., Integrated with building management system]
  - ✓ Software Installed: [e.g., ThermoTech IoT Management Software, Version 3.2.1]

- **Testing and Validation**
  - **Testing Procedures**
    - ✓ Connectivity Tests: [e.g., Verified Wi-Fi connection and IP address assignment]
    - ✓ Operational Tests: [e.g., Adjusted temperature settings and verified response from each thermostat]
    - ✓ Performance Tests: [e.g., Checked accuracy of temperature readings and response times]
  - **Validation Checks**
    - ✓ Validation Methods: [e.g., Random unit checks, verification against expected performance metrics]
    - ✓ Validation Results: [e.g., All devices confirmed operational, no issues reported]

- **Issues and Resolutions**
  - **Issues Encountered**
    - ✓ Issue 1: [e.g., Network connectivity issue with one unit]
    - ✓ Resolution: [e.g., Reconfigured network settings and restarted device]
  - **Recommendations**
    - ✓ Short-term Recommendations: [e.g., Regularly monitor network stability]
    - ✓ Long-term Recommendations: [e.g., Schedule firmware updates for enhanced features
  - **Documentation and Appendices**
  - **Installation Diagrams and Photos**

- ✓ Diagrams: [e.g., Installation diagrams showing device placements]
- ✓ Photos: [e.g., Photos of installed devices and their locations]

Device Manuals and Specifications

- ✓ Manuals: [e.g., User manuals for installed devices]
- ✓ Specifications: [e.g., Technical specifications for each device]

Test Results and Validation Documents

- ✓ Test Results: [e.g., Summary of test results, any anomalies]
- ✓ Validation Documents: [e.g., Checklists used during validation]

Practical Activity 2.6.2: Report generation

Task:

1: Read the given task
You are asked to generate a report for any IoT system

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks
4: Present the findings/answers to the whole class

5: For more clarification, read the key readings 2.5.2

6: In addition, ask questions where necessary.

Key readings 2.6.2

Project Overview

- ✓ Project Name:
- ✓ Client/Organization:
- ✓ Location:

- ✓ Installation Date:
- ✓ Report Prepared By:
- ✓ Contact Information:

Objectives

- ✓ Objective 1:
- ✓ Objective 2:
- ✓ Objective 3:

System Description

- ✓ IoT Devices Installed:
  - Device 1: (e.g., Sensors, Cameras, Actuators)
  - Device 2:
  - Device 3:
- ✓ **Connectivity:**
  - Network Type: (e.g., Wi-Fi, Bluetooth, Zigbee)
  - Connectivity Protocols: (e.g., MQTT, HTTP, CoAP)
- ✓ **Software Used:**
  - IoT Platform: (e.g., AWS IoT, Azure IoT)
  - Data Analytics Tools: (e.g., Power BI, Tableau)

Installation Details

- ✓ **Installation Team:**
  - Team Member 1:
  - Team Member 2:
  - Team Member 3:
- ✓ **Installation Process:**
  - Step 1: (e.g., Site Survey)
  - Step 2: (e.g., Device Placement)
  - Step 3: (e.g., Network Configuration)

- Step 4: (e.g., Testing and Calibration)

✓ **Challenges Faced:**

- Challenge 1: (e.g., Network Interference)
- Challenge 2: (e.g., Hardware Malfunction)

Data Collection and Analysis

✓ **Data Points Collected:**

- Data Point 1: (e.g., Temperature, Humidity)
- Data Point 2:
- Data Point 3:

✓ **Data Storage:**

- Storage Type: (e.g., Cloud, Local)
- Storage Capacity:

✓ **Data Analysis Results:**

- Key Insight 1:
- Key Insight 2:
- Key Insight 3:

Maintenance and Support

✓ **Scheduled Maintenance:**

- Frequency: (e.g., Monthly, Quarterly)
- Tasks: (e.g., Firmware Updates, Device Cleaning)

✓ **Support Contact:**

- Name:
- Email:
- Phone:

Conclusions and Recommendations

✓ **Summary of Installation:**

✓ **Effectiveness of the System:**

- ✓ **Recommendations for Future:**
  - Recommendation 1:
  - Recommendation 2:
  - Recommendation 3:

Appendices

- ✓ **Appendix A: Site Maps**
- ✓ **Appendix B: Device Specifications**
- ✓ **Appendix C: Configuration Settings**

Points to Remember

- **Report Generation in IoT Systems:** Report generation in IoT (Internet of Things) systems refers to the process of collecting, organizing, analyzing, and presenting data gathered from various IoT devices and sensors into structured documents. These reports provide insights, summaries, and detailed accounts of the system's performance, issues, configurations, and other relevant metrics. They are used for monitoring, decision-making, maintenance, and auditing purposes.
- **Importance of Report Generation in IoT Systems**
  - ✓ **Performance Monitoring:** Helps in monitoring the performance of IoT devices and systems, ensuring they operate optimally.
  - ✓ **Issue Identification:** Identifies issues and anomalies in the system, facilitating timely troubleshooting and maintenance.
  - ✓ **Data-Driven Decisions:** Provides data-driven insights that aid in making informed decisions.
  - ✓ **Compliance and Auditing:** Ensures compliance with industry standards and regulatory requirements through detailed documentation.
  - ✓ **Historical Records:** Maintains historical records of system performance and changes, useful for future reference.

Application of learning 2.6.

A large farm uses an IoT-based smart agriculture system to monitor soil moisture, weather conditions, crop health, and irrigation levels across different zones. The farm manager needs to generate a detailed report at the end of the growing season to analyze the performance of the crops, assess the efficiency of water usage, and make data-driven decisions for the next season. You as IoT technician generate the report for this large farm.

Learning outcome 2: End assessment

Theoretical assessment

Choose the letter corresponding to the correct answer:

1. **What is the primary purpose of IoT (Internet of Things)?**

   A. To provide internet access to rural areas
   B. To connect and exchange data between devices
   C. To enhance social media interactions
   D. To improve video streaming quality

2. **Which of the following is not a common IoT communication protocol?**

   A. Bluetooth
   B. Zigbee
   C. SMTP
   D. Wi-Fi

3. **In an IoT setup, what is the role of a gateway?**

   A. To act as a central point for data storage
   B. To connect different sensors and devices to the internet
   C. To provide user interfaces for device control
   D. To encrypt data for security purposes

4. **Which IoT platform is commonly used for cloud-based device management?**

   E. Windows Server
   F. AWS IoT
   G. Apache Hadoop
   H. Oracle Database

5. **Match the IoT term with its correct description:**

IoT devices	**Description**
1. Sensor	A. Executes actions based on received signals
2. Actuator	B. Collects data from the environment
3. Gateway	C. Connects devices to the internet

4. Cloud Platform	D. Provides storage and processing capabilities

Answer by True if the statement is correct and False if the statement is wrong.

6. IoT devices only operate using Wi-Fi connectivity.
7. Firmware updates are essential for maintaining the security and functionality of IoT devices.
8. Cloud platforms are used in IoT systems primarily for data storage and processing.

Practical assessment

A BUGARAMA Rice Valley Company wants to implement an IoT system for smart irrigation in an agricultural farm to enhance control, conserve water, and improve overall connectivity. Your tasks as technician covers the performance of workplace setup, identification of IoT deployment levels, assembling of IoT equipment, configuration of IoT devices, implementation of IoT system security, and documentation of an IoT installation report. The duration of the work is 3 hours. Resources	
Tools	Software platforms, simulation software, tape measure, multi-meter, screwdrivers, drilling machine, hammer, ladder, pliers,
Equipment	IoT-enabled Soil Moisture Sensors, Automated Watering System, Centralized IoT Hub, Weather Station Integration and Mobile Application for Monitoring and Control
Material/ Consumable	Internet bundles, power extension, electricity, sensors

END

References

IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things" by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, and Jerome Henry

"Practical Internet of Things Security" by Brian Russell and Drew Van Duren

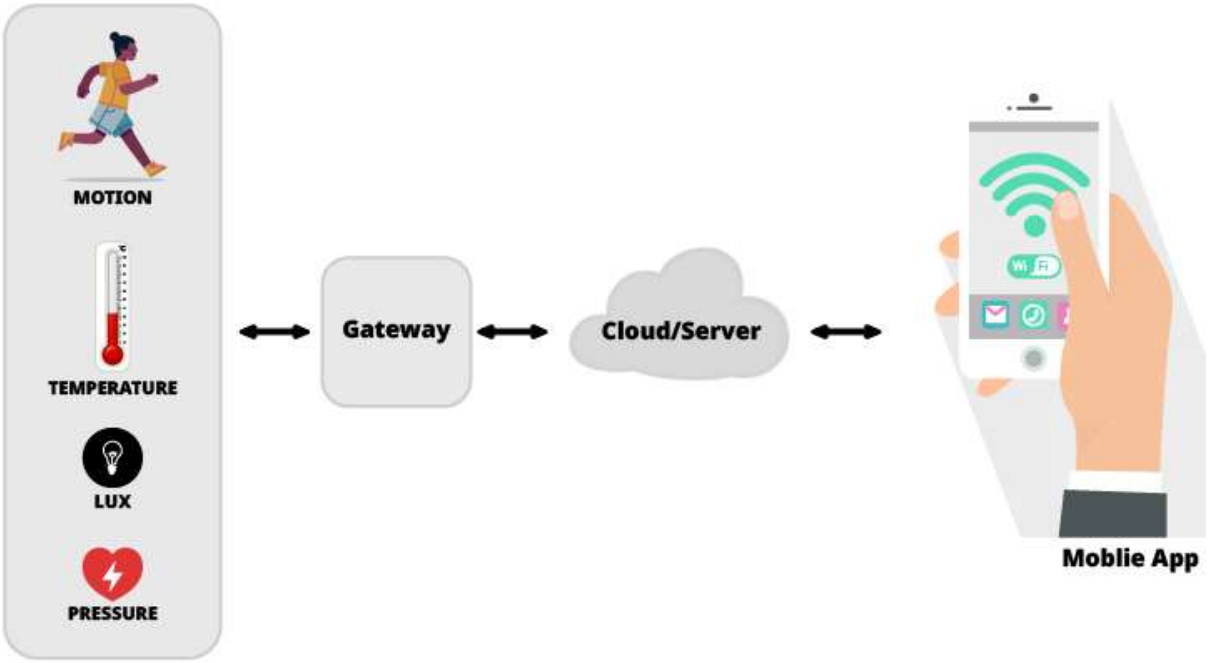
Internet-of-Things Device Set Configuration for Connection to Wireless Local Area Network

Bovell, M.C., Devlin, T.P., Goodner, A.S., Northway, T.N., Usery, P.H.: Wireless deviceconfiguration management. US Patent US8180860B2, 15 May 2012.

"Practical Internet of Things Security" by Brian Russell and Drew Van Duren

Architecting the Internet of Things,Dieter Uckelmann, Mark Harrison, Michahelles and Florian (Eds), Springer,2011.

Recipes to Begin, Expand, and Enhance Your Projects, 2nd Edition,Michael Margolis,Arduino Cookbook and O‟Reilly Media,2011.


MOTION
TEMPERATURE
LUX
PRESSURE
Gateway
Cloud/Server
Moblie App

Indicative contents
3.1 Identification of IoT systems Types
3.2 Implementation of IoT system Backup and restoration
3.3 Identification of IoT features
3.4 Management of IoT device service
3.5 Monitoring of IoT system

Key Competencies for Learning Outcome 3: Operate IoT System

Knowledge	Skills	Attitudes
• Identification of of IoT System Installation Types • Identification of IoT System features • Description of data Backup • Description of Results Interpretation	• Differentiating Types of IoT System Installation • Selecting IoT System Features • Creating Data Backup • Monitoring Of IoT System Interpretation	• Having Self Confidence • Being Problem-Solver • Being Critical Thinker • Having Time Management

Duration:20 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify properly IoT systems Types according to the installation manual
2. Identify properly IoT features according to the IoT system requirements
3. Monitor properly IoT system according to the IoT system requirements
4. Perform correctly Data backup as per the backup guideline
5. Interpret properly IoT system status as per the installation manual

   Report properly IoT system incidents as per the monitoring results

Resources

Equipment	Tools	Materials
● Modem, ● Access Point, ● Computer ● microcontrollers, ● Arduino Starter Kit	● Software platforms, ● simulation software, ● tape measure, ● multi-meter ● screwdrivers ● drilling machine ● hammer, ● ladder ● pliers	● Internet connectivity ● Pipes ● cable trunks ● electrical tapes ● screws ● Labelling tags

Indicative content 3.1: Identification of IoT Systems Types

Duration: 4 hrs

Theoretical Activity 3.1.1: Description of Consumer IoT (IoCT) Devices

Tasks:

1:In small groups, you are requested to answer the following questions related to Identification of Consumer IoT (CIoT) Devices.

i. What is Consumer IoT devices?
ii. How do they enhance our daily routines?
iii. Provide examples of CIoT devices.

2: Provide the answer for the asked questions and write them on papers.

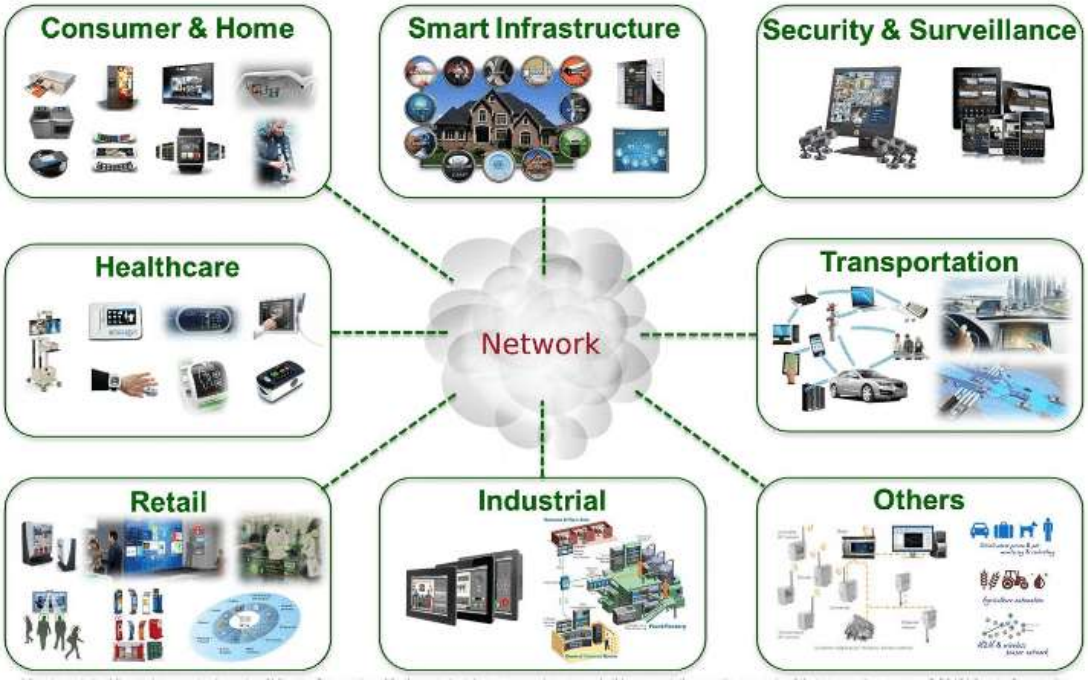
3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.1.1.

5: In addition, ask questions where necessary.

Key readings 3.1.1.: Description of Consumer IoT (IoCT) Devices

- **Consumer IoT (CIoT)** refers to the Internet of Things devices used by individuals in their everyday lives. These devices are designed to enhance convenience, entertainment, and health management for consumers. Typically, CIoT solutions leverage Wi-Fi, Bluetooth, and ZigBee to facilitate connectivity. These technologies offer short-range communication suitable for deployments in smaller venues, such as homes and offices.



Examples:

- Smart home devices (e.g., smart thermostats, smart lights, smart locks)
- Wearable technology (e.g., fitness trackers, smartwatches)
- Personal health devices (e.g., smart scales, blood pressure monitors)
- Consumer electronics (e.g., smart TVs, voice assistants)

Theoretical Activity 3.1.2: Description Commercial IoT

Tasks:

1: In small groups, you are requested to answer the following questions related to the describing Commercial IoT (CoIoT) Use Cases.

i. What is Commercial IoT (CoIoT), and why is it important for different industries?

ii. Can you name one industry where Commercial IoT is commonly used, and provide an example of how it benefits that industry?

2: Provide the answer for the asked questions and write them on papers.

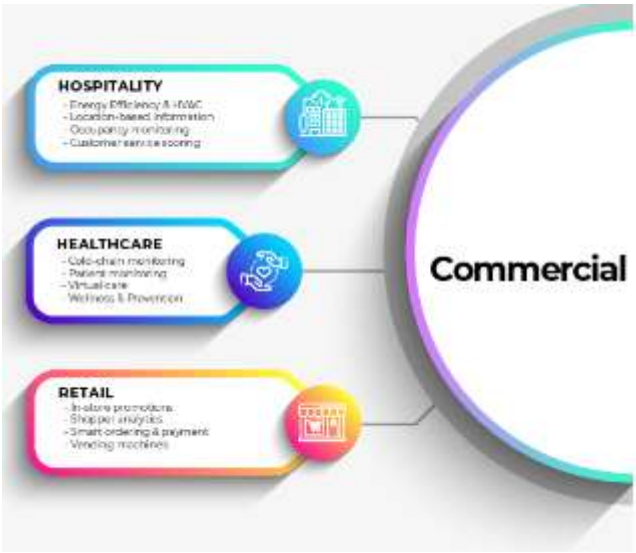
3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.1.2

5: In addition, ask questions where necessary.

Key readings 3.1.2: Description Commercial IoT

- **Commercial IoT** encompasses IoT devices and systems used in business and commercial settings to improve efficiency, customer experience, and operational management.



Examples:

- ✓ Smart retail systems (e.g., inventory management, smart shelves)
- ✓ Building automation (e.g., smart HVAC, lighting control systems)
- ✓ Asset tracking and management (e.g., RFID tags, GPS trackers)
- ✓ Connected payment systems (e.g., contactless payments, mobile wallets)

Theoretical Activity 3.1.3: Description of Industrial IoT (IIoT)

Tasks:

1: In small groups, you are requested to answer the following questions related to Examine Industrial IoT (IIoT) Applications.

i. What is IoT, and why is it important in industries?

ii. Can you name one type of industry where IoT is commonly used, and give an example of how it helps that industry?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.1.3

5: In addition, ask questions where necessary.

Key readings 3.1.3.: Description of Industrial IoT (IIoT)

- **Industrial IoT (IIoT)** involves the use of IoT technologies in industrial sectors such as manufacturing, energy, and logistics. It aims to optimize industrial processes, enhance productivity, and improve safety.

Examples:

- ✓ Predictive maintenance (e.g., monitoring equipment health to prevent failures)
- ✓ Smart factories (e.g., automated production lines, robotic systems)
- ✓ Energy management systems (e.g., smart grids, energy monitoring)
- ✓ Supply chain management (e.g., real-time tracking of goods and materials)

Theoretical Activity 3.1.4: Description of Infrastructure IoT (IIoT)

Tasks:

1: In small groups, you are requested to answer the following questions related to Examine Industrial IoT (IIoT) Applications.

i. What is Infrastructure IoT (IIoT),

ii. Why is it important for utilities like water, energy, and transportation systems?

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 3.1.4

Key readings 3.1.4.: Description of Infrastructure IoT (IIoT)

- **Infrastructure IoT** focuses on the use of IoT in infrastructure systems to enhance the efficiency, safety, and sustainability of public services and facilities. Infrastructure IoT is concerned with the development of smart infrastructures that incorporate IoT technologies to boost efficiency, cost savings, maintenance, etc. This includes the ability to monitor and control operations of urban and rural infrastructures, such as bridges, railway tracks, and on- and offshore windfarms.

Examples:

- ✓ Smart cities (e.g., intelligent traffic management, smart street lighting)
- ✓ Water management systems (e.g., smart meters, leak detection systems)
- ✓ Transportation systems (e.g., connected public transport, smart parking)
- ✓ Environmental monitoring (e.g., air quality sensors, weather stations)

Theoretical Activity 3.1.5: Description of Internet of Military Things

Tasks:

1: In small groups, you are requested to answer the following questions related to of Internet of Military Things .

i. What is the Internet of Military Things (IoMT)?
ii. Why is it important for military and defense applications?
iii. Can you think of any military or defense situations where technology plays a crucial role? How do you think IoMT might fit into these situations

2: Provide the answers for the asked questions and write them on flipchart/paper.

3: Present the findings/answers to the whole class

4: Ask questions or clarification if necessary.

5: For more clarification, read the key readings 3.1.5

Key readings 3.1.5: Description of Internet of Military Things

- **Internet of Military Things (IoMT)** refers to the application of IoT technologies in military and defense contexts. It aims to enhance situational awareness, operational efficiency, and decision-making capabilities. Internet of Military Things (IoMT), often referred to as Battlefield IoT, the Internet of Battlefield Things, or simply IoBT. IoMT is precisely what it sounds like — the use of IoT in military settings and battlefield situations. It is chiefly aimed at increasing situational awareness, bolstering risk assessment, and improving response times.

  Common IoMT applications include connecting ships, planes, tanks, soldiers, drones, and even Forward Operating Bases via an interconnected system. In addition, IoMT produces data that can be leveraged to improve military practices, systems, equipment, and strategy.

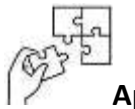
Examples:

- ✓ Connected vehicles and drones (e.g., UAVs, autonomous ground vehicles)
- ✓ Battlefield sensors (e.g., surveillance systems, motion detectors)
- ✓ Wearable technology for soldiers (e.g., health monitoring, communication devices)
- ✓ Smart weapon systems (e.g., precision-guided munitions, remote weapon stations)

Points to Remember

- **Consumer IoT (CIoT)** refers to the Internet of Things devices used by individuals in their everyday lives. These devices are designed to enhance convenience, entertainment, and health management for consumers.
- **Commercial IoT** encompasses IoT devices and systems used in business and commercial settings to improve efficiency, customer experience, and operational management.
- **Industrial IoT (IIoT)** involves the use of IoT technologies in industrial sectors such as manufacturing, energy, and logistics. It aims to optimize industrial processes, enhance productivity, and improve safety.
- **Infrastructure IoT** focuses on the use of IoT in infrastructure systems to enhance the efficiency, safety, and sustainability of public services and facilities. Infrastructure IoT is concerned with the development of smart infrastructures that incorporate IoT technologies to boost efficiency, cost savings, maintenance, etc.

- **Internet of Military Things (IoMT)** refers to the application of IoT technologies in military and defense contexts. It aims to enhance situational awareness, operational efficiency, and decision-making capabilities.



Application of learning 3.1.

A mid-sized city is experiencing rapid population growth, leading to increased traffic congestion and longer commute times. The city government has decided to implement a smart traffic management system using IoT to address these challenges. Illustrates how different IoT system types can be integrated to manage a complex urban environment, improving traffic flow, enhancing public safety, and creating a more efficient and responsive city infrastructure.

Indicative content 3.2: Implementation of IoT system Backup and restoration

Duration: 4 hrs

Theoretical Activity 3.2.1: Identification of backup types

Tasks:

1: In small groups, you are requested to answer the following questions related to the Identification IoT System Backup

i. What do you understand about IoT system backup and restoration?
ii. Why is Full backup of IoT systems?
iii. Differentiate the differential backup from incremental backup

2: Provide the answer for the asked questions and write them on papers.
3: Present the findings/answers to the whole class
4: For more clarification, read the key readings 3.2.1
5: In addition, ask questions where necessary.

Key readings 3.2.1.: Identification of backup types

- **Full Back up:** A full backup involves copying all selected data at a specific point in time. It creates a complete copy of the entire dataset, regardless of whether the data has changed since the last backup.
  - **Characteristics:**
    - ✓ Captures all data, providing a comprehensive backup.
    - ✓ Independent of other backups; each full backup is standalone.
    - ✓ Simplifies the restoration process but may consume more storage space.
  - **Use Cases:**
    - ✓ Initial backup when setting up a new system.
    - ✓ Periodic or scheduled backups for critical data.
- **Differential Backup:** A differential backup copies only the data that has changed

since the last full backup. It captures the incremental changes from the last full backup, creating a cumulative set of changes since that point.

- **Characteristics:**
  - ✓ Requires the presence of the last full backup to be effective.
  - ✓ Faster than a full backup, as it only backs up changes since the last full backup.
  - ✓ Restoration involves applying the last full backup and the latest differential backup.
- **Use Cases:**
  - ✓ Daily or regular backups to capture changes since the last full backup.
  - ✓ Situations where a balance between storage space and backup speed is crucial.

- **Incremental Backup:** An incremental backup captures only the data that has changed since the last backup, whether it's a full or incremental backup. It creates a chain of incremental backups, each building on the previous one.
  - **Characteristics:**
    - ✓ Requires the presence of the last backup (full or incremental) to be effective.
    - ✓ Generally faster and requires less storage space compared to a full or differential backup.
    - ✓ Restoration involves applying the last full backup and all subsequent incremental backups in the correct order.
  - **Use Cases:**
    - ✓ Regular, frequent backups for capturing changes since the last backup.
    - ✓ Situations where storage space is a significant consideration.

Practical Activity 3.2.2: Creation of Backup

Task:

1: Read the given task

Envision a smart home system that integrates multiple IoT devices, including smart thermostats, security cameras, and home automation controllers. This system gathers information on temperature, security incidents, and user preferences. Considering the importance of this data and the necessity for system reliability, your responsibility is to develop both automated and manual backup procedures for the smart home IoT system.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 3.2.2 and ask clarification where necessary Perform the task provided in application of learning3.2

Key readings 3.2.2: Creation of Backup

- **Steps guide for creating an effective backup**

Step 1: Identify Critical Data

- ✓ Determine what data needs to be backed up: Identify which files, databases, and system configurations are essential.
- ✓ Classify data: Prioritize data based on its importance and frequency of change.

Step 2: Choose Backup Types

- ✓ Full Back up: A complete copy of all data.
- ✓ Incremental Backup: Only backs up data that has changed since the last backup.
- ✓ Differential Backup: Backs up data that has changed since the last full backup.

Step 3: Select Backup Methods

- ✓ Local Backup: Store backups on local storage devices (e.g., external hard

drives, NAS).

- ✓ Cloud Backup: Use cloud storage solutions (e.g., AWS, Google Cloud, Azure).
- ✓ Hybrid Backup: Combine local and cloud backups for redundancy.

Step 4: Determine Backup Frequency

- ✓ Daily Backups: For critical data that changes frequently.
- ✓ Weekly/Monthly Backups: For less critical data or data that doesn't change often.
- ✓ Real-Time Backups: Continuous data protection for highly critical systems.

Step 5: Implement Backup Solutions

- ✓ Automated Backup Software: Use software to automate the backup process (e.g., Acronis, Veeam, Backblaze).
- ✓ Manual Backups: Regularly schedule and perform manual backups, ensuring consistency.

Step 6: Verify and Test Backups

- ✓ Regular Checks: Verify that backups are being performed correctly and data integrity is maintained.
- ✓ Restore Tests: Periodically test the restoration process to ensure data can be successfully recovered.

Practical Activity 3.2.3: Restoration of IoT system

Task:

1: Read the given task

A smart factory uses IoT devices for monitoring and managing production processes. These devices include sensors on machinery, automated conveyor belts, and environmental monitors. The factory relies on real-time data for optimal operation and efficiency. A power surge occurs, causing a network failure and disrupting the connectivity of IoT devices across the factory floor. Several

devices lose their configurations, and the central IoT platform stops receiving data. You are assigned to restore the system.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 3.2.3 and ask clarification where necessary Perform the task provided in application of learning3.2

Key readings 3.2.3: Restoration of IoT system

- **Assess the Situation**
  - ✓ Identify the cause of the disruption (e.g., power outage, device malfunction).
  - ✓ Determine which devices and services are affected.
- **Restore Network Connectivity**
  - ✓ Check the status of routers and switches.
  - ✓ Reconnect all IoT devices to the network.
- **Device Restoration**
  - ✓ Restart all IoT devices.
  - ✓ Check for and apply firmware updates.
  - ✓ Reconfigure any devices that lost settings.
- **Data Restoration**
  - ✓ Restore configuration files and sensor data from backups.
  - ✓ Restore the central database from the latest backup.
  - ✓ Verify data integrity.
- **Application and Software Restoration**
  - ✓ Reinstall IoT platform software.
  - ✓ Reconfigure integrations with cloud services and analytics tools.
- **Security Verification**
  - ✓ Check encryption settings and access controls.

- ✓ Apply security patches.

- **Testing and Validation**
  - ✓ Test each IoT device to ensure functionality.
  - ✓ Perform system-wide tests to confirm overall performance.
  - ✓ Verify data collection and processing.
- **Documentation and Reporting**
  - ✓ Document the cause of the disruption and the restoration steps taken.
  - ✓ Update restoration procedures to include any new insights.
  - ✓ Inform stakeholders of the incident and resolution.

Points to Remember

- A full backup is a complete copy of all the data in a system. Every time a full backup is performed, all selected files, databases, or other data are copied in their entirety, regardless of whether they have changed since the last backup.
- A differential backup includes only the data that has changed since the last full backup. Each differential backup will include all changes made since the last full backup, growing in size with each subsequent differential backup until the next full backup is taken.
- An incremental backup includes only the data that has changed since the last backup, whether it was a full or incremental backup. This means each incremental backup is typically much smaller and quicker than full or differential backups
- **Automatic Backup:** Provides a continuous and reliable backup solution with minimal user intervention.
- **Manual Backup:** Offers users control over when to initiate backups, especially before critical system events.

Application of learning 3.2.

A smart home system includes various IoT devices such as smart lights, thermostats, security cameras, door locks, and voice assistants. These devices are interconnected and managed via a central hub or cloud platform, providing convenience and automation for the homeowner. A severe storm causes a prolonged power outage, leading to the malfunction of several IoT devices. Some devices lose their settings, and the central hub is unable to connect to the cloud platform. The homeowner needs backup and restore the system to its fully functional state.

Indicative content 3.3: Identification of IoT Features

Duration: 4 hrs

Theoretical Activity 3.3.1: Identification of IoT features

Tasks:

1: In small groups, you are requested to answer the following questions related to the Identification of IoT features

i. Enumerate IoT features

ii. What are the importance for each in IoT system installation?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.3.1

5: In addition, ask questions where necessary.

Key readings 3.3.1.: Identification of IoT features

To identify and understand the features of IoT, let's expand on each of the items listed:

- **Connectivity**: The ability of devices to connect and communicate with each other and the internet. Enables data exchange and remote control of devices, forming the backbone of IoT systems. They use Wired and wireless communication protocols such as Wi-Fi, Bluetooth, Zigbee, cellular networks (3G, 4G, 5G), LoRa, and more
- **Sensing**: The use of sensors to gather data from the physical environment. Provides the necessary data for analysis, monitoring, and automation.
- **Active Engagements**: The ability for continuous and real-time interaction between devices and users. Ensures timely responses and actions based on real-time data, enhancing user experience and system performance.
- **Scale**: The capability to handle a large number of devices and vast amounts of data. Allows the IoT system to grow and manage increasing numbers of connected devices and data points. They use Cloud computing, edge computing, and robust data management systems

- **Dynamic Nature**: The adaptability of IoT systems to changing conditions and environments. Ensures that IoT systems remain functional and relevant even as circumstances evolve.
- **Intelligence**: The use of advanced algorithms and machine learning to process data and make decisions. Enables predictive analytics, automated decision-making, and smarter system responses. They use Sensors, machine learning algorithms, and context-aware computing
- **Energy**: Efficient energy management and low power consumption of IoT devices. Extends the lifespan of battery-operated devices and reduces the overall energy footprint of the system. Helps in identifying inefficiencies, optimizing energy usage, and planning for future energy needs.
- **Safety**: Measures to ensure the safe operation of IoT devices and protect users from harm. Prevents accidents and ensures the reliability and trustworthiness of IoT systems. They use Encryption, authentication protocols, secure hardware, and software updates.
- **Integration**: The ability to integrate IoT devices with existing systems and technologies. Facilitates seamless operation and enhances the functionality of the entire system by leveraging existing infrastructure. They use APIs, middleware, and integration platforms **c**omponents.

Points to Remember

- The features of IoT are Connectivity, Sensing, Active Engagements Scale, Dynamic Nature, Intelligence Energy' Safety and Integration

Application of learning 3.3.

Consider a smart building management system that has components includes sensors (temperature, humidity, motion), actuators (lights, HVAC systems), a central controller, cloud storage, and a user interface identify IoT features.

Indicative content 3.4: Management of the IoT device service

Duration: 4 hrs

Theoretical Activity 3.4.1: Description of Event triggering

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Event triggering

i. Define Event triggering in the context of computer programming
ii. List example of electronics triggers?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.4.1

5: In addition, ask questions where necessary.

Key readings 3.4.1: Description of Event triggering

- **Event Triggering:** The process of initiating an action or series of actions in response to specific events or conditions detected by IoT devices. Enables real-time responses to changes in the environment, enhancing the functionality and utility of IoT systems.
- **Examples:**
  - ✓ Sensor Data: Triggering an alarm if a smoke detector senses smoke.
  - ✓ Time-Based Events: Turning on lights at a specific time or when it gets dark.
  - ✓ User Actions: Sending a notification when a user enters a geo-fenced area**.**
- **Benefits of Effective IoT Device Service Management**
  - ✓ Increased Efficiency: Automating responses to events and conditions reduces the need for manual intervention, streamlining operations.
  - ✓ Enhanced User Experience: Tailored actions and configurations improve the usability and convenience of IoT systems.

- ✓ Cost Savings: Efficient energy management and reduced operational overheads lower costs.
- ✓ Improved Security: Automated actions enhance security by ensuring timely responses to potential threats.
- ✓ Scalability: Flexible management systems support the growth and scaling of IoT networks.

Theoretical Activity 3.4.2: Conditional actions

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Conditional actions

i. Define the conditional actions in context of IoT?
ii. What are the Key Aspects Conditional actions?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.4.2

5: In addition, ask questions where necessary.

Key readings 3.4.2: Conditional actions

- **Conditional Actions**: Performing specific actions based on predefined conditions or criteria. Allows for tailored responses and automation, making IoT systems more intelligent and adaptive to user needs. Utilize rule engines like Node-RED or IFTTT (If This Then That) to define and manage conditional actions.
- **Examples:**
  - ✓ Temperature Control: Adjusting the thermostat if the temperature falls below or exceeds a set threshold.
  - ✓ Security: Locking doors automatically when no movement is detected in a building for a certain period.

- ✓ Energy Management: Switching off devices when they are not in use to save energy.

Theoretical Activity 3.4.3: Description of Conditional configurations

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Conditional configurations

i. What mean the conditional configurations in IoT
ii. What are the examples of Conditional Configurations

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.4.3

5: In addition, ask questions where necessary.

Key readings 3.4.3: Description of Conditional configurations

- **Conditional Configurations**: Changing the configuration or settings of IoT devices based on specific conditions or criteria. Enhances the flexibility and adaptability of IoT systems, ensuring devices operate optimally under varying conditions.
- **Examples**:
  - ✓ **Network Settings**: Switching to a backup network if the primary connection fails.
  - ✓ **Device Behavior**: Adjusting the sensitivity of a motion sensor during night hours to reduce false alarms.
  - ✓ **Operational Modes**: Switching devices to power-saving mode during off-peak hours.

Points to Remember

- **Event Triggering:** The process of initiating an action or series of actions in response to specific events or conditions detected by IoT devices. Enables real-time responses to changes in the environment, enhancing the functionality and utility of IoT systems.
- **Conditional Actions**: Performing specific actions based on predefined conditions or criteria. Allows for tailored responses and automation, making IoT systems more intelligent and adaptive to user needs. Utilize rule engines like Node-RED or IFTTT (If
- **Conditional Configurations**: Changing the configuration or settings of IoT devices based on specific conditions or criteria. Enhances the flexibility and adaptability of IoT systems, ensuring devices operate optimally under varying conditions.

Application of learning 3.4.

For managing a Smart Irrigation System for a Farm. You are requested to automate the irrigation process based on real-time environmental data and predefined conditions to optimize water usage and crop health.

Indicative content 3.5: Monitoring of IoT system

Duration: 4 hrs

Practical Activity 3.5.1: Monitoring of IoT system software

Task:

1: Read the given task

A large commercial building is equipped with a Smart Building Management System (SBMS) to enhance energy efficiency, security, and occupant comfort. The system integrates various IoT devices, including temperature and humidity sensors, smart lighting, HVAC (heating, ventilation, and air conditioning) systems, security cameras, access control systems, and energy meters. Your goal as IoT technician is to monitor the IoT system software to ensure optimal performance, security, reliability, and compliance with building regulations.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 3.5.1 and ask clarification where necessary Perform the task provided in application of learning3.5

Key readings 3.5.1: Monitoring of IoT system software

- **Steps for Monitoring software of IoT system**
  - ✓ **Identify Software Components:** List and identify the various software components in your IoT system. This may include IoT platform services, application servers, databases, communication middleware, and any custom software running on edge devices.
  - ✓ **Select Monitoring Tools:** Choose appropriate monitoring tools or platforms for tracking the performance and health of your software components. Tools like Prometheus, Grafana, Nagios, or commercial solutions may be suitable depending on your system's requirements.
  - ✓ **Define Key Metrics:** Determine the critical metrics you want to monitor for each software component. Examples include CPU and memory usage,

response times, error rates, database connection pool statistics, and network latency.

- ✓ **Instrument Code and Components:** Integrate monitoring agents, logging mechanisms, or instrumentation code into your software components. This may involve using logging libraries, APM (Application Performance Monitoring) tools, or built-in features of your programming language.
- ✓ **Configure Logging:** Set up centralized logging to aggregate logs from different software components. Tools like ELK Stack (Elasticsearch, Logstash, Kibana) or centralized logging services can be employed for efficient log management.
- ✓ **Implement Tracing (Optional):** If applicable, consider implementing distributed tracing for better visibility into the flow of requests across different components. Tools like Jaeger or Zipkin can assist in tracing requests.
- ✓ **Create Dashboards:** Use your chosen monitoring tools to design dashboards that provide a visual representation of key software metrics. This may involve creating charts, graphs, and tables for quick and easy interpretation.
- ✓ **Set Up Alerts:** Configure alerts based on predefined thresholds for each metric. Alerts should notify administrators or DevOps teams of potential issues before they impact the overall system performance.
- ✓ **Integrate with Notification Systems:** Connect your monitoring system with notification systems such as email, Slack, or other communication platforms to ensure timely alerts reach the responsible parties.
- ✓ **Perform Load Testing:** Simulate varying loads and scenarios to test how the software components behave under different conditions. Monitor the system during these tests to identify potential bottlenecks or areas for optimization.
- ✓ **Documentation and Training** Document the monitoring setup, including configurations, metric definitions, and troubleshooting procedures. Provide training to relevant personnel on interpreting monitoring data and responding to alerts.

Practical Activity 3.5.2: Monitoring of IoT system parameters

Task:

1: Read the given task

A large commercial building uses a Smart Building Management System (SBMS) that integrates various IoT devices to enhance energy efficiency, security, and occupant comfort. The system includes temperature and humidity sensors, smart lighting, HVAC systems, security cameras, access control systems, and energy meters. Your task is to monitor the IoT system parameters to ensure energy efficiency, security, and occupant comfort with building regulations.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 3.5.2 and ask clarification where necessary Perform the task provided in application of learning 3.5

Key readings 3.5.2: Monitoring of IoT system parameters

- **Steps of Monitoring of IoT system parameters**
  - ✓ Identify Parameters: List and categorize the parameters relevant to your system. This may include performance metrics, resource utilization, security indicators, and any other parameters critical to your system's operation.
  - ✓ Select Monitoring Tools: Choose appropriate monitoring tools or platforms that support the monitoring of the identified parameters. Tools like Prometheus, Grafana, Nagios, or specialized tools for specific domains may be suitable.
  - ✓ Define Key Metrics for Each Parameter: For each parameter, determine the key metrics you want to monitor. For example:
  - ✓ Performance Metrics: CPU usage, memory consumption, response times.
  - ✓ Resource Utilization: Disk space, network bandwidth, database connections.
  - ✓ Security Indicators: Failed login attempts, system vulnerabilities.

- ✓ Custom Parameters: Specific metrics relevant to your application or system.
- ✓ Instrumentation: Integrate monitoring agents or instrumentation code into your system to collect data for the identified parameters. This may involve adding code snippets, configuring agents, or using APIs provided by monitoring tools.
- ✓ Configure Data Collection: Set up data collection mechanisms to gather information from various components of your system. This could involve setting up APIs, log collectors, or other data gathering methods.
- ✓ Create Monitoring Dashboards: Design comprehensive dashboards using your selected monitoring tools. Organize the dashboards to present key metrics for each parameter in a clear and understandable manner. Utilize graphs, charts, and alerts for visualization.
- ✓ Set Thresholds and Alerts: Establish thresholds for each parameter, defining acceptable and unacceptable ranges. Configure alerting systems to notify relevant parties when a parameter breaches its defined threshold.
- ✓ Real-Time Monitoring: Monitor the parameters in real-time to gain insights into system behavior. Use the dashboards to quickly identify and respond to abnormal patterns or potential issues.
- ✓ Historical Data Storage: Configure a storage solution to retain historical data for trend analysis, capacity planning, and auditing purposes. This could involve using databases, data lakes, or cloud storage.
- ✓ Periodic Reviews and Adjustments: Regularly review the effectiveness of your parameter monitoring system. Make adjustments to thresholds, add or remove parameters based on evolving system requirements.
- ✓ Documentation and Training: Document the parameter monitoring setup, including configurations, metric definitions, and troubleshooting procedures. Provide training to relevant personnel on interpreting monitoring data and responding to alerts.

Theoretical Activity 3.5.3: Interpreting IoT System Status

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Conditional configurations

i. Define IoT system status interpretation
ii. What are some key aspects to consider for IoT system status interpretation?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.5.3

5: In addition, ask questions where necessary.

Key readings 3.5.3:

- Interpreting the status of an IoT system involves understanding the complex interplay of its various components and their performance metrics. This is crucial for ensuring system reliability, optimizing performance, and identifying potential issues.
- **Key Components of IoT System Status**
  - **Device Status:**
    - ✓ Connectivity: Online/offline, signal strength, network latency.
    - ✓ Battery level: Remaining charge, charging status.
    - ✓ Sensor readings: Temperature, humidity, motion, etc.
    - ✓ Actuator status: On/off, position, speed.
  - **Network Status:**
    - ✓ Network connectivity: Uptime, latency, packet loss.
    - ✓ Bandwidth utilization: Current usage, peak usage.
    - ✓ Security: Intrusion detection, unauthorized access.

- **Data Status:**
  - ✓ Data integrity: Accuracy, completeness, consistency.
  - ✓ Data quality: Noise, outliers, anomalies.
  - ✓ Data volume: Usage patterns, storage capacity.
- **Application Status:**
  - ✓ Performance: Response time, throughput, error rates.
  - ✓ User experience: Feedback, ratings, usage patterns.
  - ✓ System health: Resource utilization, error logs.

- **Interpretation Techniques**
  - ✓ **Threshold-Based Monitoring:** Defining predefined limits for system parameters and triggering alerts when exceeded.
  - ✓ **Statistical Analysis:** Identifying trends, correlations, and anomalies in data patterns.
  - ✓ **Machine Learning:** Building models to predict system behavior and detect anomalies.
  - ✓ **Visualization:** Creating visual representations of data to identify patterns and trends.
- **Common IoT System Status Indicators**
  - ✓ Uptime: Percentage of time the system is operational.
  - ✓ Response Time: Time taken for the system to respond to a request.
  - ✓ Error Rate: Frequency of system failures or errors.
  - ✓ Resource Utilization: How efficiently system resources (CPU, memory, storage) are used.
  - ✓ Data Quality: Accuracy and completeness of data.
  - ✓ Security Events: Unauthorized access attempts or breaches.
- **Challenges in Interpreting IoT System Status**
  - ✓ Data Volume: IoT systems generate massive amounts of data, making analysis challenging.
  - ✓ Data Variety: Data comes from different sources with varying formats and

structures.

- ✓ Data Velocity: Data is generated rapidly, requiring real-time processing.
- ✓ Complex Relationships: System components are interconnected, making it difficult to isolate issues.

Practical Activity 3.5.4: Monitoring results interpretation

Task:

1: Read the given task

You are an IoT technician responsible for monitoring results interpretation the Smart Building Management System (SBMS) in a large commercial building. The SBMS integrates various IoT devices including temperature and humidity sensors, smart lighting, HVAC systems, security cameras, access control systems, and energy meters. Your goal is to ensure energy efficiency, security, and occupant comfort while complying with building regulations.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 3.5.4 and ask clarification where necessary Perform the task provided in application of learning 3.5

Key readings 3.5.4

- **Interpreting Monitoring Results: A Comprehensive Guide**

  Interpreting monitoring results is a critical step in understanding system performance, identifying issues, and making informed decisions. It involves transforming raw data into actionable insights.

- **Steps in Interpreting Monitoring Results**
- **Data Preparation:**

- ✓ **Cleaning:** Remove errors, inconsistencies, and outliers.
- ✓ **Normalization:** Ensure data is consistent across different sources or time periods.
- ✓ **Aggregation:** Combine data into meaningful summaries (e.g., averages, totals).

- **Visualization:**
  - ✓ **Graphs and Charts:** Create visual representations of data (e.g., line charts, bar charts, histograms).
  - ✓ **Dashboards:** Combine multiple visualizations for a comprehensive overview.
  - ✓ **Anomaly Detection:** Identify unusual data points that may indicate problems.
- **Analysis:**
  - ✓ **Trend Analysis:** Identify patterns and changes over time.
  - ✓ **Correlation Analysis:** Determine relationships between different metrics.
  - ✓ **Root Cause Analysis:** Investigate the underlying reasons for issues or anomalies.
- **Actionable Insights:**
  - ✓ **Identify Problems:** Pinpoint areas requiring attention.
  - ✓ **Optimize Performance:** Make data-driven decisions to improve system efficiency.
  - ✓ **Predict Future Trends:** Anticipate potential issues or opportunities.
- **Common Monitoring Metrics and Their Interpretation**
  - ✓ **System Uptime:** Measures system availability. High uptime indicates reliability.
  - ✓ **Response Time:** Indicates how quickly the system responds to requests. Longer response times may signal performance issues.
  - ✓ **Error Rates:** Measures the frequency of errors. High error rates indicate problems.
  - ✓ **Resource Utilization:** Tracks CPU, memory, and disk usage. High utilization may indicate bottlenecks.

- ✓ **Network Traffic:** Monitors data transfer. Unusual patterns may indicate security threats or performance issues.

Theoretical Activity 3.5.5: Describing Incident management

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of Conditional configurations

i. Define Incident management
ii. Describe the Lifecycle of Incident management

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 3.5.5

5: In addition, ask questions where necessary.

Key readings 3.5.5:

- **Definition of IoT Incident Management**

  IoT incident management is a structured approach to identifying, responding to, and resolving disruptions or anomalies within an IoT system. It involves detecting issues with IoT devices, networks, or applications, understanding their impact on the overall system, and taking corrective actions to restore normal operations efficiently

- **IoT Incident Management Lifecycle**

  While the core principles of traditional incident management apply, IoT introduces unique challenges and considerations:

  - **Incident Detection:**
    - ✓ **Sensor Data Analysis:** Identify anomalies in sensor readings that indicate potential issues.
    - ✓ **Device Behavior Monitoring:** Detect deviations from normal device

behavior patterns.

- ✓ **Network Performance Monitoring:** Identify network congestion, latency, or outages.
- ✓ **User Feedback:** Collect and analyze user reports of system issues.

- **Incident Triage and Prioritization:**
  - ✓ **Impact Assessment:** Determine the potential impact of the incident on the system and business operations.
  - ✓ **Urgency Determination:** Prioritize incidents based on their severity and time-sensitivity.
  - ✓ **Resource Allocation:** Assign appropriate resources to address the incident.
- **Incident Investigation and Diagnosis:**
  - ✓ **Data Analysis:** Correlate sensor data, device logs, and network information to identify the root cause.
  - ✓ **Remote Diagnostics:** Utilize remote tools to troubleshoot device issues.
  - ✓ **Field Service Coordination:** Arrange on-site visits if necessary.
- **Incident Resolution:**
  - ✓ **Corrective Actions:** Implement solutions to address the root cause.
  - ✓ **Workarounds:** Provide temporary solutions to mitigate impact while permanent fixes are developed.
  - ✓ **Configuration Changes:** Modify system settings to prevent recurrence.
- **Incident Closure and Learning:**
  - ✓ **Knowledge Base Update:** Document incident details, root cause, and resolution.
  - ✓ **Process Improvement:** Identify opportunities to enhance incident response procedures.
  - ✓ **Preventive Measures:** Implement measures to prevent similar incidents in the future.

Points to Remember

- Monitoring an IoT system involves continuously observing and managing the various components and operations to ensure the system is functioning correctly, performing optimally, and meeting its intended objectives. Effective monitoring helps in identifying issues early, optimizing performance, and maintaining system reliability.
- Effective monitoring of an IoT system involves using specialized software to track and manage various parameters, interpreting system status and results, and implementing a robust incident management process.

Application of learning 3.5.

You are an IoT technician responsible for monitoring the Smart Building Management System (SBMS) in a large commercial building. The SBMS integrates various IoT devices including temperature and humidity sensors, smart lighting, HVAC systems, security cameras, access control systems, and energy meters. Your task is to monitor the IoT system

Learning outcome 3 end assessment

Theoretical assessment

Choose the letter corresponding to the correct answer

1. **Which of the following IoT system types focuses on managing and optimizing public infrastructure?**
    a) Consumer IoT
    b) Commercial IoT
    c) Industrial IoT
    d) Infrastructure IoT
2. **What is the main characteristic of an incremental backup?**
    a) Backs up all data every time.
    b) Backs up only data changed since the last full backup.
    c) Backs up only data changed since the last backup, full or incremental.
    d) Backs up only data changed since the last differential backup.
3. **Which of the following features is associated with IoT devices' ability to collect and process environmental data?**
    a) Connectivity
    b) Sensing
    c) Scale
    d) Safety

Answer by True if the statement is correct and False if the statement is wrong

4. **True or False:** Industrial IoT (IIoT) focuses on enhancing consumer experiences with smart home devices.
5. **True or False:** Automatic backups are initiated manually by the user or administrator as needed.
6. **True or False:** The "dynamic nature" feature of IoT refers to the system's ability to adapt and reconfigure in real-time based on environmental changes.
7. **Match the following IoT system types with their primary applications:**

IoT System Type:	Primary Applications:

1. Consumer IoT	A. Predictive maintenance and automated production lines
2. Commercial IoT	B. Smart home devices and wearables
3. Industrial IoT	C. Public transportation and smart grids
4. Infrastructure IoT	D. Inventory management and customer analytics
5. Internet of Military Things (IoMT)	E. Surveillance drones and battlefield sensors

Practical assessment

You have been hired as an IoT systems specialist for a smart manufacturing facility that is implementing a new IoT solution to enhance operational efficiency and safety. The facility includes various IoT devices such as environmental sensors, automated machinery, and a smart energy management system. Your task is to operate and manage the IoT system effectively, ensuring its smooth operation, efficient backup and restoration, and accurate monitoring.

The duration of the work is 3 hours.

Resources

Tools	Software platforms, simulation software, tape measure, multi-meter, screwdrivers, drilling machine, hammer, ladder, pliers,
Equipment	Environmental sensors, automated machinery, and a smart energy management system, Home Automation Hub, Mobile Devices (Smartphones, Tablets) and IoT-enabled Sensors
Material/ Consumable	Internet bundles, power extension, electricity, sensors

END

References

"Smart Homes and Their Users" by Springer

"Internet of Things: Concepts, Methodologies, Tools, and Applications" edited by Information Resources Management Association

"Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl, Zaigham Mahmood, and Ricardo Puttini

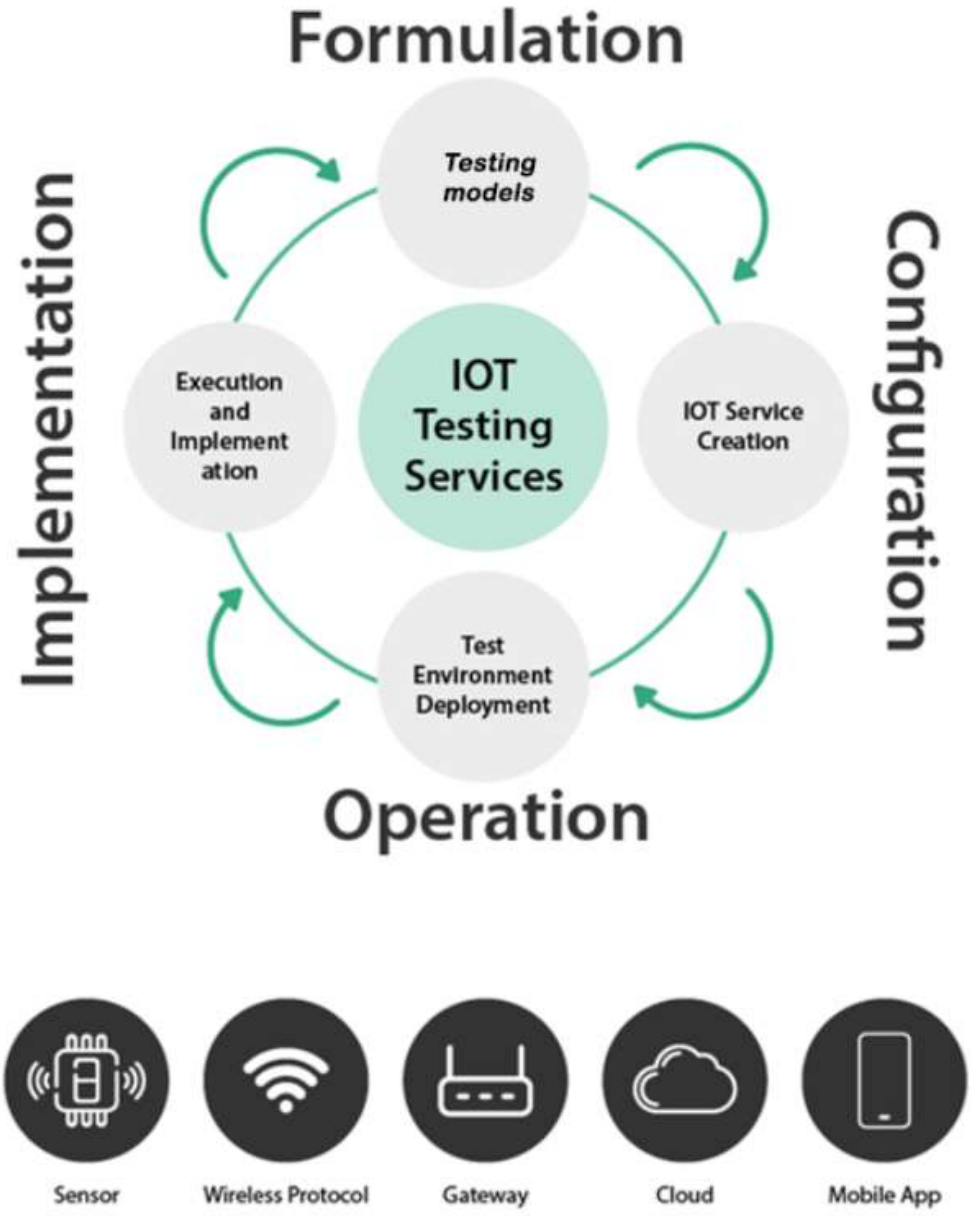
"The Definitive Guide to AWS Infrastructure Automation" by Michael Wittig and Andreas Wittig

"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things" by David Han

"Designing Connected Products: UX for the Internet of Things" by Claire Rowland, Elizabeth Goodman, and Martin Charlier

"Practical Internet of Things Security" by Brian Russell and Drew Van Duren

"Internet of Things: A Hands-On-Approach" by Arshdeep Bahga and Vijay Madisetti


Formulation
Testing models
Configuration
IOT Service Creation
Test Environment Deployment
Operation
Execution and Implement ation
Implementation
IOT Testing Services
Sensor
Wireless Protocol
Gateway
Cloud
Mobile App

Indicative contents
4.1 Identification of IoT Testing Types
4.2Performance of IoT Tests
4.3 Elaboration of testing report

Key Competencies for Learning Outcome 4: Test IoT system

Knowledge	Skills	Attitudes
● Description of IoT Testing ● Performance of IoT Tests ● Elaboration Of Testing Report	● Identifying IoT Testing ● Selecting of IoT Testing Tools ● Generating Of Report	● Having Communication ● Having Collaboration ● Having Problem-Solving ● Having Perseverance Initiative

Duration:10 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Describe correctly IoT testing types as used in IoT system installation
2. Perform correctly IoT testing tool as used in IoT system installation
3. Elaborate properly IoT testing report based on IoT system installation

Resources

Equipment	Tools	Materials
● Computer ● Multi-meter ● Digital Storage Oscilloscope	● Software platforms ● JTAG ● Software defined radio (SDR) ● Drilling machine ● hammer, ● ladder ● pliers	● Internet connectivity

Indicative content 4.1: Identification of IoT Testing Types

Duration: 3 hrs

Theoretical Activity 4.1.1: Description of IoT Testing Types

Tasks:

1: In small groups, you are requested to answer the following questions related to the description of IoT IoT Testing Types

i. What is Usability in IoT Testing?

ii. Define Reliability in IoT?

iii. Explain Security in IoT testing?

iv. What is the difference between Data integrity and Compatibility

v. Mention applications of Performance in IoT

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 4.1.1.

5: In addition, ask questions where necessary.

Key readings 4.1.1.: Description of IoT Testing Types

- **Usability Testing:** Ensuring the IoT device or application is user-friendly and intuitive. Key areas: User interface design, Device ergonomics and User experience across different platforms (mobile, web, etc.).
- **Reliability Testing:** Evaluating the system's ability to perform its intended function without failure over time**.** Key areas: Mean time between failures (MTBF), Device lifespan and System recovery capabilities.
- **Data Integrity Testing:** Ensuring data accuracy, completeness, and consistency throughout the IoT system. Key areas: Data validation and cleansing, Data encryption and protection, Data synchronization and consistency.
- **Security Testing:** Identifying vulnerabilities and weaknesses in the IoT system to

protect against threats. Key areas: Network security, Device security, Data privacy and protection, Authentication and authorization.

- **Compatibility Testing:** Verifying the IoT system's ability to interoperate with different hardware, software, and network environments. Key areas: Device compatibility, Network compatibility, Platform compatibility and Software compatibility.
- **Performance Testing:** Evaluating the system's response time, throughput, scalability, and stability under various workloads**.** Key areas: Load testing, Stress testing and Endurance testing.

Points to Remember

Usability testing ensures IoT devices are user-friendly across different platforms, while reliability testing evaluates durability and long-term performance. Data integrity testing verifies the accuracy and security of data within the system. Security, compatibility, and performance testing identify vulnerabilities, ensure interoperability, and assess system response under various conditions.

Application of learning 4.1

Perform the testing the security of a Smart Home System to ensure that the smart home system is secure against unauthorized access and data breaches.

Indicative content 4.2: Performance of IoT Tests

Duration: 4 hrs

Practical Activity 4.2.1: Perform Functional test

Task:

1: Read the given task

You are conducting a test on a smart home lighting system for a customer who wishes to confirm that their smart light bulbs can be operated via a mobile application. Perform Functional test to validate the essential functions of the smart home lighting system

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.2.1and ask clarification where necessary Perform the task provided in application of learning 4.2

Key readings 4.2.1: Perform Functional test

- **Step 1: Test Environment Setup:**
  - ✓ Hardware Setup: Connect the smart bulb and Hue Bridge to power sources.
  - ✓ Software Setup: Install and configure the Hue App on a smartphone.
  - ✓ Network Configuration: Ensure the Hue Bridge is connected to the home Wi-Fi network.
- **Step 2: Execution of Functional Tests:**
  - **TC-01 Execution:**
    - ✓ Step 1: Power on the smart bulb.
    - ✓ Step 2: Ensure the Hue Bridge is connected to the Wi-Fi.
    - ✓ Step 3: Use the Hue App to connect the bulb to the Bridge.
    - ✓ Expected Result: The bulb connects successfully and appears in the app.

- ✓ Actual Result: (Record the outcome after execution)

TC-02 Execution:

- ✓ Step 1: Open the Hue App.
- ✓ Step 2: Turn the bulb on/off using the app.
- ✓ Step 3: Change the bulb color.
- ✓ Step 4: Adjust the brightness.
- ✓ Expected Result: The bulb responds accurately to all commands.
- ✓ Actual Result: (Record the outcome after execution)

TC-03 Execution:

- ✓ Step 1: Add multiple bulbs to the Bridge using the app.
- ✓ Step 2: Group the bulbs in the app.
- ✓ Step 3: Control the group (turn on/off, change color, adjust brightness).
- ✓ Expected Result: All bulbs in the group respond simultaneously to controls.
- ✓ Actual Result: (Record the outcome after execution)

- **Step 3: Data Collection and Analysis:**
  - ✓ Logs and Reports: Capture logs from the Hue App during the test.
  - ✓ Issue Tracking: Note any issues or discrepancies found during testing and document them for further investigation**.**

Practical Activity 4.2.2: Performing Security test

Task:

1: Read the given task

You are conducting a test on a smart home lighting system for a customer who wishes to confirm that their smart light bulbs can be operated via a mobile application. The customer has set up Philips Hue smart bulbs throughout their home, connected to a Hue Bridge, and uses the Hue mobile app for control. The objective is to validate the essential functions of the smart home lighting system,

ensuring that the smart bulbs can connect to the Hue Bridge and be controlled through the Hue mobile app.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.2.2 and ask clarification where necessary Perform the task provided in application of learning 4.2

Key readings 4.2.2: Performing Security test

- **Step1:** Identification of Security Testing Tools
  - ✓ OWASP ZAP: An open-source web application security scanner.
  - ✓ Nmap: A network scanning tool to discover hosts and services on a computer network.
  - ✓ Wireshark: A network protocol analyzer to capture and analyze network traffic.
  - ✓ Burp Suite: An integrated platform for performing security testing of web applications.
  - ✓ Nessus: A vulnerability scanner to identify potential vulnerabilities in the system.
  - ✓ Metasploit: A penetration testing framework for discovering, exploiting, and validating vulnerabilities.
- **Step2: Perform Security Test**

  Test Case: Penetration Testing on IoT Device
  - Objective: To identify and exploit vulnerabilities in the IoT system to ensure it is secure.
  - Preconditions: IoT device is connected to the network, and all necessary tools are installed.
  - Test Steps:
    - Nmap: Perform a network scan to identify open ports and services running on the IoT device. Command: nmap -sV <IoT_device_IP>
      - ✓ Wireshark: Capture network traffic to analyze communication between the IoT device and other devices.

Start capturing packets, filter by the IoT device's IP, and analyze the traffic.

- ✓ OWASP ZAP: Conduct an automated scan for web application vulnerabilities if the IoT device has a web interface.

  Set up a proxy, configure the target, and initiate the scan.

- ✓ Nessus: Perform a vulnerability scan on the IoT device.

  Configure a scan policy, add the target, and run the scan.

- ✓ Metasploit: Attempt to exploit identified vulnerabilities to test their impact. Command: use <exploit_name> and follow the framework instructions.

- Expected Result: Identification of potential vulnerabilities and their impact. Device should be secure against common attacks.
- Actual Result: *(To be recorded during the test)*

Practical Activity 4.2.3: Perform Connectivity test

Task:

1: Read the given task

You are conducting a test on a smart home lighting system for a customer who wishes to confirm that their smart light bulbs can be operated via a mobile application. The customer has set up Philips Hue smart bulbs throughout their home, connected to a Hue Bridge, and uses the Hue mobile app for control. The objective is to validate the essential functions of the smart home lighting system, ensuring that the smart bulbs can connect to the Hue Bridge and be controlled through the Hue mobile app.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.2.3 and ask clarification where necessary Perform the task provided in application of learning 4.2.

Key readings 4.2.3: Perform Connectivity test

- **Step1:** Identification of Connectivity Testing Tools
  - ✓ Ping: A basic tool to test connectivity between devices.
  - ✓ Traceroute: A tool to trace the path packets take to reach a destination.
  - ✓ Wireshark: For capturing and analyzing network traffic.
  - ✓ iPerf: A tool to measure network bandwidth.
  - ✓ Netcat: A utility to test network connections and port communication.
- **Step2:** Perform Connectivity Test

  Test Case: Verify IoT Device Connectivity

✓ Objective: To ensure that the IoT device can reliably connect to the network and communicate with other devices.

✓ Preconditions: IoT device is powered on and connected to the network.

✓ Test Steps:

- Ping: Test basic connectivity to the IoT device.
  - Command: ping <IoT_device_IP>
- Traceroute: Trace the route packets take to reach the IoT device.
  - Command: traceroute <IoT_device_IP>
- Wireshark: Capture and analyze network traffic to ensure proper communication.
  - Steps: Start capturing packets, filter by the IoT device's IP, and analyze the traffic.
- iPerf: Measure network bandwidth between the IoT device and another host.
  - Command: iperf -c <host_IP> -t 60
- Netcat: Test port communication and ensure services are accessible.
  - Command: nc -zv <IoT_device_IP> <port>

- Expected Result: IoT device should have stable and reliable connectivity with no packet loss or significant delays.

- Actual Result: *(To be recorded during the test*

Practical Activity 4.2.4: Perform Performance test

Task:

1: Read the given task

You are conducting a test on a smart home lighting system for a customer who wishes to confirm that their smart light bulbs can be operated via a mobile application. The customer has set up Philips Hue smart bulbs throughout their home, connected to a Hue Bridge, and uses the Hue mobile app for control. The objective is to validate the essential functions of the smart home lighting system, ensuring that the smart bulbs can connect to the Hue Bridge and be controlled through the Hue mobile app.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.2.4 and ask clarification where necessary Perform the task provided in application of learning 4.2

Key readings 4.2.4: Perform Performance test

- **Step1: Identification of Performance Testing Tools**
  - ✓ Apache JMeter: A tool to measure performance and load.
  - ✓ Gatling: A tool for load and performance testing.
  - ✓ Locust: An open-source load testing tool.
  - ✓ Wireshark: To analyze network performance.
  - ✓ iPerf: To measure network bandwidth and performance.
- **Step2: Perform Performance Test**

  Test Case: Load Testing on IoT System

✓ Objective: To assess the performance of the IoT system under various load

conditions.

- ✓ Preconditions: IoT system is set up and connected to the network, and performance testing tools are installed.
- ✓ Test Steps:
  - Apache JMeter: Configure a test plan to simulate multiple users interacting with the IoT system.

    Create a thread group, add HTTP requests or MQTT samplers, configure listeners, and run the test.
  - Gatling: Create and execute a simulation to load test the IoT system.

    Write a simulation script, configure the load, and execute the test.
  - Locust: Simulate multiple users to test the system's load handling capabilities.

    Write a task script, configure the number of users, and start the test.
  - Wireshark: Capture and analyze network traffic to identify any performance bottlenecks.

    Start capturing packets, filter by the IoT device's IP, and analyze the traffic.
  - iPerf: Measure the network bandwidth and latency under load conditions.

    Command: iperf -c <host_IP> -t 60
- ✓ Expected Result: The IoT system should handle the load without significant performance degradation or failures.
- ✓ Actual Result: *(To be recorded during the test)*

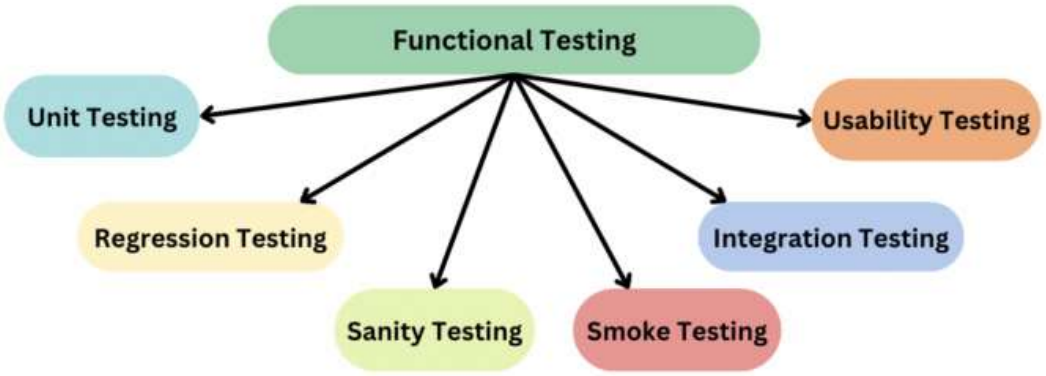
Points to Remember

- **A connectivity test** checks if two devices or networks can communicate with each other. It's a fundamental troubleshooting step for any network issue.
- **Connectivity Test Methods**
  - **Basic Connectivity Tests:**
    - ✓ **Ping:** Check if devices can communicate with the network or cloud.
    - ✓ **Port scanning:** Verify, if necessary, ports are open.
    - ✓ **Traceroute:** Analyze the network path to identify potential issues.

- **Network Simulation:**
  - ✓ Emulate different network conditions: Simulate weak signals, high latency, and packet loss.
  - ✓ Use network simulators: Tools like Wireshark can help analyze network traffic.
- **Field Testing:**
  - ✓ Deploy devices in real-world environments: Test connectivity in different locations and conditions.
  - ✓ Monitor device performance: Collect data on signal strength, latency, and data throughput.
- **IoT Testing Platforms:**
  - ✓ Utilize specialized platforms: Some platforms offer comprehensive IoT testing capabilities, including connectivity testing.

- **IoT performance testing** is a specialized form of software testing that evaluates the performance of Internet of Things (IoT) systems under various conditions. It focuses on assessing how efficiently IoT devices, networks, and cloud platforms interact to deliver data and services
- **Security testing** is a critical aspect of software development and system administration, designed to identify and address vulnerabilities that could be exploited by malicious actors. It involves evaluating a system's resilience against various threats, from unauthorized access to data breaches.
- **Functional testing** is a type of software testing that verifies the functionality of a software system or application. It focuses on ensuring that the system behaves according to the specified functional requirements and meets the intended business needs.

  Types of Functional Testing:



Application of learning 4.2

A smart factory is implementing an IoT-based monitoring system to oversee the performance of IoT Tests of industrial machines. The system involves sensors attached to each machine, which gather data on temperature, vibration, energy consumption, and operational status in real time. Your tasks are to perform the IoT Tests.

Indicative content 4.3: Elaboration of Testing Report

Duration: 3 hrs

Practical Activity 4.3.1: Generation of report

Task:

1: Read the given task

You are testing a smart home lighting system. As an IoT Technician, you are required to generate a report documenting all the tests conducted.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.3.1and ask clarification where necessary Perform the task provided in application of learning 4.3

Key readings 4.3.1: Generation of report

- **Generation of Report**

The primary objective of generating a testing report is to document the results of various tests conducted on IoT systems. This report provides a comprehensive overview of the system's performance, reliability, and security.

Components:

- Title Page:
  - ✓ Title of the Report
  - ✓ Project Name
  - ✓ Date of Report
  - ✓ Author/Tester Name
- Table of Contents: A list of sections and their respective page numbers for easy navigation.
- Executive Summary: A brief summary of the testing process, key findings, and overall assessment of the system.
- Introduction:
  - ✓ Purpose of the Report
  - ✓ Scope of Testing
  - ✓ Description of the IoT system under test

- Testing Methodology:
  - ✓ Types of Tests Conducted (e.g., functional, performance, security, usability)
  - ✓ Testing Environment (hardware and software used)
  - ✓ Test Cases and Test Scenarios
- Test Execution Details:
  - ✓ Schedule and timeline of the tests
  - ✓ Test execution logs
  - ✓ Any deviations from the planned testing process
- Test Results:
  - ✓ Summary of test outcomes (pass/fail status)
  - ✓ Detailed results for each test case
  - ✓ Screenshots or logs illustrating test results
- Defects and Issues:
  - ✓ List of identified defects
  - ✓ Severity and priority of each defect
  - ✓ Status of defects (open, resolved, in progress)
  - ✓ Steps to reproduce defects
- Performance Metrics:
  - ✓ System response time
  - ✓ Throughput
  - ✓ Resource utilization (CPU, memory, network)
- Security Findings:
  - ✓ Vulnerability assessment results
  - ✓ Penetration testing outcomes
  - ✓ Recommendations for addressing security issues
- Conclusion:
  - ✓ Overall assessment of the system
  - ✓ Summary of key findings
  - ✓ Recommendations for improvements
- Appendices: Additional data, logs, test scripts, and any other relevant documentation

Practical Activity 4.3.2: Interpretation of report

Task:

1: Read the given task

You are testing a smart home lighting system. As an IoT Technician, you are required to interpret the report generated from the tests conducted.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 4.3.2 and ask clarification where necessary Perform the task provided in application of learning 4.3

Key readings 4.3.2 Interpretation of report

- Interpretation of Report: The interpretation of the testing report involves analyzing the data and findings to derive meaningful insights about the system's performance and areas for improvement
- Steps:
  - Review Executive Summary: Understand the high-level outcomes and overall assessment provided by the tester.
  - Analyze Test Results:
    - Examine the detailed results for each test case.
    - Identify patterns or recurring issues that may indicate underlying problems.
  - Evaluate Defects and Issues:
    - Assess the severity and impact of identified defects.
    - Prioritize defects based on their criticality and impact on the system.
  - Assess Performance Metrics:
    - Compare performance metrics against predefined benchmarks or requirements.
    - Identify any bottlenecks or performance degradation.
  - Examine Security Findings:
    - Analyze vulnerabilities and security weaknesses.
    - Determine the potential risks and their implications for the system.
  - Draw Conclusions:
    - Synthesize findings from different sections of the report.
    - Determine the overall health and readiness of the system for deployment.
  - Provide Recommendations:
    - Suggest corrective actions for identified issues.
    - Recommend best practices for improving system performance and security.
  - Prepare Action Plan:
    - Develop a plan for addressing the identified issues.
    - Assign responsibilities and set timelines for resolution

Points to Remember

- **Generation of report**
  - ✓ Cover Page: Provides essential details about the report.
  - ✓ Introduction: Sets the context and defines the scope of the testing.
  - ✓ Testing Methodology: Describes the approach and methods used in testing.
  - ✓ Test Results Presents detailed findings from the testing.
  - ✓ Conclusion: Summarizes the overall assessment and readiness of the system.
- Interpreting an IoT testing report involves analyzing the findings to draw conclusions about the system's quality and performance.
  - ✓ Assessment of test coverage: Determine if the testing adequately covered the system's functionality.
  - ✓ Evaluation of test results: Assess the system's performance against defined acceptance criteria.
  - ✓ Identification of defects: Prioritize defects based on severity and impact.
  - ✓ Analysis of trends: Identify patterns in the test results to uncover potential issues.
  - ✓ Evaluation of recommendations: Assess the feasibility and impact of proposed improvements.

Application of learning 4.2

You are testing a smart home lighting system. As an IoT Technician, you are required to generate and interpret the report from the tests conducted.

Learning outcome 4 end assessment

Theoretical assessment

Choose the letter corresponding to the correct answer:

1. **Which of the following is NOT a type of IoT test?**

   A) Usability

   B) Compatibility

   C) Functionality

   D) Scalability

2. **Which tool is commonly used for security testing in IoT systems?**

   A) JMeter

   B) Wireshark

   C) LoadRunner

   D) OWASP ZAP

3. **What is the primary purpose of a connectivity test in IoT systems?**

   A) To evaluate the system's responsiveness

   B) To ensure devices can connect and communicate reliably

   C) To verify the accuracy and consistency of data

   D) To check for vulnerabilities and ensure the system is protected against threats

4. **True or False:** Usability testing in IoT systems assesses how user-friendly and intuitive the system is.
5. **True or False:** JMeter is a tool used primarily for security testing in IoT systems.
6. **True or False:** Connectivity tests ensure the system performs consistently under specified conditions.

7. Match the IoT testing type to its primary focus

IoT testing	**Its primary focus**
Usability	A) Ensures the system performs consistently under specified conditions
Reliability	B) Assesses how user-friendly and intuitive the system is
Data Integrity	C) Evaluates the system's responsiveness, throughput, and scalability
Security	D) Verifies the accuracy and consistency of data over its lifecycle
Compatibility	E) Checks for vulnerabilities and ensures the system is protected against threats
Performance	F) Tests the system's ability to function with different devices and environments

Practical assessment

As a testing professional, your responsibility is to ensure the reliability and effectiveness of an Industrial IoT system designed for predictive maintenance in a manufacturing facility. The system incorporates sensors on machinery, data analytics tools, and a central monitoring platform. The primary objective is to identify potential issues in the machinery before they lead to failures, optimizing maintenance efforts, and minimizing downtime. Your tasks include the identification of IoT testing types, the performance of IoT tests, and the elaboration of a comprehensive testing report.

The duration of the work is 3 hours.

Resources

Tools	Software platforms, simulation software, tape measure, multi-meter, screwdrivers, drilling machine, hammer, ladder, pliers,
Equipment	Smart Lighting System, Smart Thermostats, Smart Security Cameras, Home Automation Hub, Mobile Devices (Smartphones, Tablets) and IoT-enabled Sensors
Material/Consumable	Internet bundles, power extension, electricity, sensors

End

References

"Internet of Things: Principles and Paradigms" by Rajkumar Buyya, Amir Vahid Dastjerdi

"Internet of Things: A Hands-On-Approach" by Arshdeep Bahga, Vijay Madisetti

"Sensor Technologies: Healthcare, Wellness and Environmental Applications" by Michael J. McGrath

"Wireless Sensor Networks: Technology, Protocols, and Applications" by Kazem Sohraby, Daniel Minoli, and Taieb Znati

"Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die" by Eric Siegel

"Software Testing: A Craftsman's Approach" by Paul C. Jorgensen

"Foundations of Software Testing: ISTQB Certification" by Rex Black, Erik van Veenendaal, and Dorothy Graham

Indicative contents
5.1 Identification of IoT Maintenance types
5.2 Application of IoT Software upgrade
5.3 Performance of IoT system security maintenance
5.4 Documentation of IoT maintenance report

Key Competencies for Learning Outcome 5: Maintain IoT system

Knowledge	Skills	Attitudes
• Identification of IoT Maintenance types • Application of IoT Software upgrade • Performance of IoT system security maintenance • Documentation of IoT maintenance report	• Applying Of IoT Software Upgrade • Performing IoT Action Repairs • Performing IoT System Protection Checks • Generating Report	• Having a Communication And Collaboration • Having a Problem-Solving • Having a Perseverance Initiative • Having a Time Management

Duration:10 hrs

Learning outcome 2 objectives:

By the end of the learning outcome, the trainees will be able to:

1. Identify correctly IoT testing types as used in IoT system installation
2. Apply correctly IoT Software upgrade as used in IoT system
3. Perform properly IoT system security maintenance based on IoT system installation
4. Document correctly IoT maintenance report based on IoT system installation

Resources

Equipment	Tools	Materials
● Computer ● Multi-meter ● Digital Storage Oscilloscope	● Software platforms ● JTAG ● Software defined radio (SDR) ● Drilling machine ● hammer, ● ladder ● pliers ● screwdrivers	● Internet connectivity

Indicative content 5.1: Identification of IoT Testing Types

Duration: 2 hrs

Theoretical Activity 5.1.1: Identification of IoT Maintenance types

Tasks:

1: In small groups, you are requested to answer the following questions related to the identification of IoT Maintenance types

i. Define IoT maintenance

ii. Differentiate predictive from preventive maintenance in IoT and provide examples?

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 5.1.1.

5: In addition, ask questions where necessary.

Key readings 5.1.1.: Identification of IoT Maintenance types

- **IoT maintenance** refers to the process of ensuring the optimal functionality, security, and efficiency of interconnected devices and systems within the Internet of Things (IoT) ecosystem.
- **Identification of IoT Maintenance types**
  - Preventive Maintenance:
    - ✓ Regular Inspections: Periodic checks and inspections to identify potential issues before they escalate.
    - ✓ Scheduled Maintenance: Planned maintenance activities based on predetermined schedules to ensure device longevity.
    - ✓ Software Updates: Applying firmware and software updates to enhance features, security, and performance.
  - Predictive Maintenance:

✓ Data Analytics: Utilizing real-time data and analytics to predict when equipment failure or maintenance is likely to occur, allowing for proactive interventions.

- ✓ Machine Learning Algorithms: Employing machine learning models to analyse historical data and predict future maintenance needs based on patterns and trends.
- Corrective Maintenance:
- ✓ Fault Detection: Identifying and diagnosing malfunctions or failures in real-time to promptly initiate corrective actions.
- ✓ Repairs and Replacements: Conducting repairs, component replacements, or device replacements to restore functionality.

Points to Remember

- **IoT maintenance** refers to the process of ensuring the optimal functionality, security, and efficiency of interconnected devices and systems within the Internet of Things (IoT) ecosystem.
- The main difference between preventive and predictive maintenance is how maintenance work is triggered and scheduled. Preventive maintenance is scheduled regularly based on triggers like time and usage, while predictive maintenance is scheduled based on machine data that measures the asset's condition

Application of learning 5.1.

An HVAC (heating, ventilation, and air conditioning) system in a smart manufacturing plant is monitored and controlled by means of a temperature sensor that is part of the smart manufacturing plant systems. Describe different types of IoT Maintenance you can apply to ensure the continuous and efficient operation of a smart manufacturing plant using various IoT maintenance strategies.

Indicative content 5.2: Application of IoT Software upgrade

Duration: 3 hrs

Theoretical Activity 5 .2.1: Application of IoT Software upgrade

Tasks:

1: In small groups, you are requested to answer the following questions related to the identification of IoT Maintenance types

i. Define a software upgrade?

ii. What are the types of software upgrade?

iii. How is the software upgrade is done? (list and explain options)

2: Provide the answer for the asked questions and write them on papers.

3: Present the findings/answers to the whole class

4: For more clarification, read the key readings 5.2.1.

5: In addition, ask questions where necessary.

Key readings 5.2.1.: Application of IoT Software upgrade

- **Automatic Software Upgrades**
  - Advantages:

✓ Efficiency: Updates can be deployed across multiple devices simultaneously, saving time and reducing the need for manual intervention.

✓ Consistency: Ensures all devices are running the latest software version, reducing discrepancies and potential compatibility issues.

✓ Security: Automatic updates can quickly address security vulnerabilities, reducing the risk of attacks or exploits.

✓ User Experience: Minimal disruption to users, as updates can be scheduled during off-peak hours or pushed silently in the background.

- Considerations:
  - ✓ Control: Users or administrators may have limited control over when

updates are applied, which could be an issue in critical or sensitive environments.

- ✓ Testing: Updates should be thoroughly tested before deployment to avoid introducing new bugs or issues across all devices.
- ✓ Bandwidth: Large updates can consume significant bandwidth, potentially affecting network performance.

- **Manual Software Upgrades**
  - Advantages:
    - ✓ Control: Administrators can decide when to apply updates, allowing for planned downtime and minimal disruption.
    - ✓ Customization: Allows for selective updating of devices, which can be useful if certain devices need to remain on a specific version for compatibility reasons.
    - ✓ Testing: Updates can be tested on a small subset of devices before being rolled out more widely, reducing the risk of widespread issues.
  - Considerations:
    - ✓ Time-Consuming: Manually updating devices can be labor-intensive, especially in large-scale IoT deployments.
    - ✓ Inconsistency: Higher risk of some devices being missed or not updated promptly, leading to potential security vulnerabilities and compatibility issues.
    - ✓ User Dependency: Relies on the diligence and availability of administrators or users to perform updates, which can lead to delays.
- **Implementation Strategies**
  - Automatic Upgrades:
    - ✓ Over-the-Air (OTA) Updates: Commonly used in IoT devices, where updates are pushed to devices wirelessly.
    - ✓ Scheduled Updates: Automatic updates can be scheduled during off-peak hours to minimize disruption.
    - ✓ Rolling Updates: Gradually updating a subset of devices at a time to monitor for any issues before a full rollout.
  - Manual Upgrades:
    - ✓ Local Updates: Using USB drives or other local media to manually update each device.
    - ✓ Centralized Management Systems: Administrators use centralized systems to manage and deploy updates to specific devices as needed.
    - ✓ User-Initiated Updates: End users are notified and given instructions on how to manually update their devices.

Points to Remember

- Manual updates are the opposite of automatic updates, as they require you to check for updates, download them, and install them yourself. You can usually change your operating system settings to disable automatic updates and enable manual updates, or to be notified before any installations.

Application of learning 5.2.

A smart home system integrates various IoT devices, including smart thermostats, security cameras, lighting controls, door locks, and voice assistants. These devices communicate via a central hub and are controlled through a mobile app or voice commands. The system is widely used by homeowners to enhance comfort, security, and energy efficiency. Implement a software upgrade for a smart home system to enhance security, add new features, and improve system performance without disrupting user experience

Indicative content 5.3: Performance of IoT system security maintenance

Duration: 3 hrs

Practical Activity 5.3.1: Performing IoT action repairs

Task:

1: Read the given task

A security camera on your IoT network is found to be transmitting unusual amounts of data at unexpected times, indicating a potential breach or malfunction. As an IoT Technician you are asked to repair issue.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 5.3.1and ask clarification where necessary Perform the task provided in application of learning 5.3

Key readings 5.3.1: Performing IoT action repairs

Steps to Repair:

- Setup and Baseline Monitoring:
  - ✓ Install Wireshark on your computer.
  - ✓ Capture normal traffic from the security camera and document its usual behavior.
- Simulate an Issue:
  - ✓ Manually install an outdated firmware version on the camera that is known to have a vulnerability.
- Incident Response:
  - ✓ Use Wireshark to detect the unusual data transmission.
  - ✓ Isolate the camera from the network by disconnecting it or blocking its IP address on the router.
- Patching and Repair:
  - ✓ Download the latest firmware for the camera from the manufacturer's website.
  - ✓ Follow the manufacturer's instructions to update the camera's firmware.

- Post-Repair Testing:
  - ✓ Verify that the camera is functioning correctly and no longer transmitting unusual data.
  - ✓ Compare its performance to the baseline metrics.
- Documentation: Log the entire process, including the issue detected, isolation steps, firmware update, and verification results.
- Review and Improve:
  - ✓ Review logs periodically to ensure no similar issues arise.
  - ✓ Update your maintenance procedures based on this repair experience.

Practical Activity 5.3.2: Performing IoT system protection checks

Task:

1: Read the given task

Your organization has deployed several IoT devices, including smart cameras and environmental sensors, in an office environment. You need to perform regular protection checks to ensure these devices are secure.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 5.3.2and ask clarification where necessary Perform the task provided in application of learning 5.3

Key readings 5.3.2: Performing IoT system protection checks

Steps to Perform Protection Checks:

- Regular Security Audits:
  - Vulnerability Scanning:
    - ✓ Use Nessus to scan the network and identify vulnerabilities.
    - ✓ Prioritize high-risk vulnerabilities and plan remediation steps.
  - Penetration Testing:
    - ✓ Use Kali Linux to perform penetration testing on the IoT network.
    - ✓ Document the vulnerabilities and how they were exploited, and create a remediation plan.

- Access Control Review:
  - Permission Audit:
    - ✓ Review and update access permissions for all IoT devices.
    - ✓ Remove access for former employees or roles that no longer need it.
  - Implement MFA:
    - ✓ Enable MFA for accessing the IoT management console and critical devices.
- Network Security:
  - Firewall Configuration:
    - ✓ Ensure the firewall is configured to block unnecessary ports and protocols.
    - ✓ Restrict incoming and outgoing traffic to what is necessary for IoT device operation.
  - Network Segmentation:
    - ✓ Create VLANs to separate IoT devices from the main office network.
- Data Protection:
  - Encryption Setup:
    - ✓ Ensure that all communication between IoT devices and the server is encrypted using TLS.
    - ✓ Encrypt sensitive data stored on IoT devices.
  - Integrity Checks:
    - ✓ Implement checks to verify data integrity using hash functions.
- Compliance and Policies:
  - Policy Review:
    - ✓ Review and update security policies to include IoT device management and security.
    - ✓ Ensure policies address current best practices and regulatory requirements.
  - Compliance Check:
    - ✓ Conduct a compliance check to ensure all IoT devices and processes adhere to GDPR requirements.
- User Education:
  - Training Session:
    - ✓ Conduct training on recognizing phishing attempts and maintaining secure passwords.
    - ✓ Emphasize the importance of following security protocols for IoT devices.
  - Awareness Campaign:

✓ Distribute newsletters and posters highlighting recent IoT security threats and tips for safe usage.

Points to Remember

- **Perform IoT Action Repairs:** To address and fix specific issues or malfunctions in the IoT system that have been identified through monitoring, user reports, or routine checks.
- **Perform IoT System Protection Checks:** To ensure the ongoing security, reliability, and resilience of the IoT system by regularly checking protective measures, identifying potential vulnerabilities, and implementing preventive actions.

Application of learning 5.3

The smart city utilizes a vast network of IoT devices, including traffic management systems, environmental sensors, public safety cameras, and connected infrastructure. These systems are critical to the city's operations and must be protected against cyber threats that could disrupt services or compromise data integrity. Due to the growing sophistication of cyber threats, regular security maintenance is crucial to protect the IoT network. As a technician you are asked to perform protection checks ensuring that all devices and communication channels are secure.

Indicative content 5.4: Documentation of IoT maintenance report

Duration: 2 hrs

Practical Activity 5.4.1: Data analysing and facts recording

Task:

1: Read the given task

A motion sensor on your IoT network is found to be transmitting unusual amounts of data at unexpected times, indicating a potential breach or malfunction. As an IoT Technician you are asked to make Data analysing and facts recording.

2: Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 5.4.1and ask clarification where necessary Perform the task provided in application of learning 5.4

Key readings 5.4.1: Data analysing and facts recording

- **Data analysis** in IoT involves extracting meaningful insights from the vast amount of data generated by connected devices. This process is crucial for optimizing operations, improving decision-making, and identifying potential issues.

  - **Steps in IoT data analysis:**

    - ✓ Data Collection: Gathering data from various IoT sensors and devices.
    - ✓ Data Cleaning: Ensuring data accuracy, consistency, and completeness by removing errors and inconsistencies.
    - ✓ Data Transformation: Converting raw data into a suitable format for analysis.
    - ✓ Data Exploration: Discovering patterns, trends, and anomalies within the data.
    - ✓ Data Modeling: Creating statistical models to predict future outcomes

or understand relationships between variables.

- ✓ Data Visualization: Representing data graphically to facilitate understanding and communication of insights.

Common IoT data analysis techniques:

- ✓ Descriptive statistics: Summarizing data using measures like mean, median, mode, and standard deviation.
- ✓ Exploratory data analysis (EDA): Discovering patterns and relationships within data through visualization and summary statistics.
- ✓ Predictive analytics: Forecasting future trends or outcomes based on historical data.
- ✓ Prescriptive analytics: Recommending actions based on data-driven insights.

- **Facts recording** in IoT refers to the systematic collection and storage of data generated by IoT devices. This data serves as the foundation for subsequent analysis and decision-making.

Considerations for facts recording:

- ✓ Data storage: Choosing appropriate storage solutions (databases, data warehouses, cloud platforms) based on data volume and structure.
- ✓ Data format: Selecting suitable data formats (CSV, JSON, XML) for efficient storage and retrieval.
- ✓ Data retention: Determining the necessary data retention period based on legal and business requirements.
- ✓ Data security: Implementing robust security measures to protect sensitive data.
- ✓ Data governance: Establishing policies and procedures for data management and access control.

Practical Activity 5.4.2: Report generation

Task:

1: Read the given task

A security camera on your IoT network is found to be transmitting unusual amounts of data at unexpected times, indicating a potential breach or malfunction. As an IoT Technician you are asked to generate a report after performing the maintenance.

2**:** Follow the demonstration of the trainer in trainee manual

3: Referring to the demonstration provided on task 2, Perform the given tasks.

4: Present your work to the trainer and whole class

5: Read key reading 5.4.2 and ask clarification where necessary Perform the task provided in application of learning 5.4

Key readings 5.4.2: Report generation

- **Report Structure:** A well-structured IoT maintenance report should provide a clear overview of the maintenance activities and their impact. Consider the following structure:
  - ✓ **Executive Summary:** A concise overview of the report, highlighting key findings and recommendations.
  - ✓ **Maintenance Overview:** General information about the IoT system, including the number of devices, their criticality, and maintenance schedules.
  - ✓ **Performance Metrics:** Analysis of KPIs such as MTBF, MTTR, and equipment uptime.
  - ✓ **Issue Analysis:** Detailed breakdown of reported issues, including frequency, severity, and resolution time.
  - ✓ **Preventive Maintenance:** Summary of preventive maintenance activities performed, including their effectiveness.
  - ✓ **Corrective Maintenance:** Analysis of corrective maintenance actions, including costs and time taken.
  - ✓ **Spare Parts Management:** Evaluation of spare parts inventory, usage, and replenishment strategies.

- ✓ **Cost Analysis:** Breakdown of maintenance costs, including labor, parts, and equipment.
- ✓ **Recommendations:** Suggestions for improving maintenance efficiency and reducing downtime.
- ✓ **Appendices:** Supporting data, such as maintenance logs, repair reports, and performance graphs.

- **Report Visualization:** Effective use of visuals can enhance the report's clarity and impact. Consider incorporating:
  - ✓ Graphs and charts: To represent performance metrics, issue trends, and cost analysis.
  - ✓ Tables: To summarize maintenance activities, spare parts inventory, and labor hours.
  - ✓ Maps: To visualize device locations and maintenance coverage.

Points to Remember

Report generation is the process of creating a structured document that presents information, findings, or results in a clear and organized manner. This process involves several key steps and objectives, particularly in contexts like testing, project management, business analysis, and research.

Application of learning 5.4

A smart factory utilizes an IoT system to monitor and control various manufacturing processes, including machinery performance, energy consumption, and production line efficiency. The IoT system comprises sensors, actuators, connected machines, and a central control system. Regular maintenance is essential to ensure that the IoT system operates optimally and to prevent unplanned downtime. Documenting an IoT Maintenance Report for a Smart Factory.

Learning outcome 5 end assessment

Written assessment

Choose the letter corresponding to the correct answer:

1. **Which IoT network technology is best suited for long-range, low-power communication?**

   A) Zigbee
   B) Wi-Fi6
   C) LoRa
   D) Bluetooth/LE

2. **What is the purpose of predictive maintenance in IoT systems**

   A) To perform regular maintenance at fixed intervals
   B) To predict when maintenance should be performed based on real-time data
   C) To replace all components periodically
   D) To monitor the physical environment of IoT devices

3. **Which IoT deployment level typically involves basic device installation and initial configuration?**

   A) Level-1

   B) Level-2

   C) Level-4

   D) Level-6

4. **Which of the following is NOT a common IoT testing type?**

   A) Usability

   B) Data Integrity

   C) Environmental Impact

   D) Security

5. **True or False:** Zigbee is a network technology suitable for long-range communication with high power consumption.

6. **True or False:** Preventive maintenance involves fixing problems only when they occur.

7. **True or False:** Functional testing of IoT systems involves verifying the speed, latency, and jitter of the device**.**
8. **True or False:** Calibration of tools and equipment ensures that they operate with increased precision and accuracy.
9. Match the following IoT network technologies with their respective range and power characteristics:

IoT network technologies	**range and power characteristics**
1. Zigbee	A) Long Range, Low Power
2. LoRa	B) Short Range, Low Power
3. Wi-Fi6	C) Long Range, High Power
4. LPWAN	D) Short Range, High Power

Practical assessment

You have been hired as an IoT maintenance technician by a manufacturing company that is managing a sophisticated IoT-based monitoring and control system within its facility. The system is designed to integrate various sensors, actuators, and controllers to monitor equipment performance, environmental conditions, and production processes in real-time. Your primary role is to ensure the system operates seamlessly and securely, focusing on software upgrades and security maintenance.

The duration of the work is 3 hours.

Resources

Tools	Software platforms, simulation software, tape measure, multi-meter, screwdrivers, drilling machine, hammer, ladder, pliers,
Equipment	Smart Lighting System, HVAC Automation, Security Cameras and Access Control, Occupancy Monitoring Sensors and Centralized IoT Platform
Material/Consumable	Internet bundles, power extension, electricity, sensors

References

"Internet of Things: Principles and Paradigms" Edited by Rajkumar Buyya, Amir Vahid Dastjerdi
"Internet of Things: A Hands-On-Approach" By Arshdeep Bahga, Vijay Madisetti
"IoT Systems: Architecture and Applications" By R. C. Joshi, S. S. Srivastava
"Embedded Systems: Design and Applications" By Steve Heath
"Security and Privacy in Internet of Things (IoT): Models, Algorithms, and Implementations"
Edited by Hongyu Wu, Dongxu Li
"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things"
By David Hanes, Gonzalo Salgueiro, Patrick Grossetete, and others
"The Internet of Things: A Guide to IoT Systems and Applications" *By Michael Miller*

RTB | RWANDA TVET BOARD

October 2024