# IOT Module-18

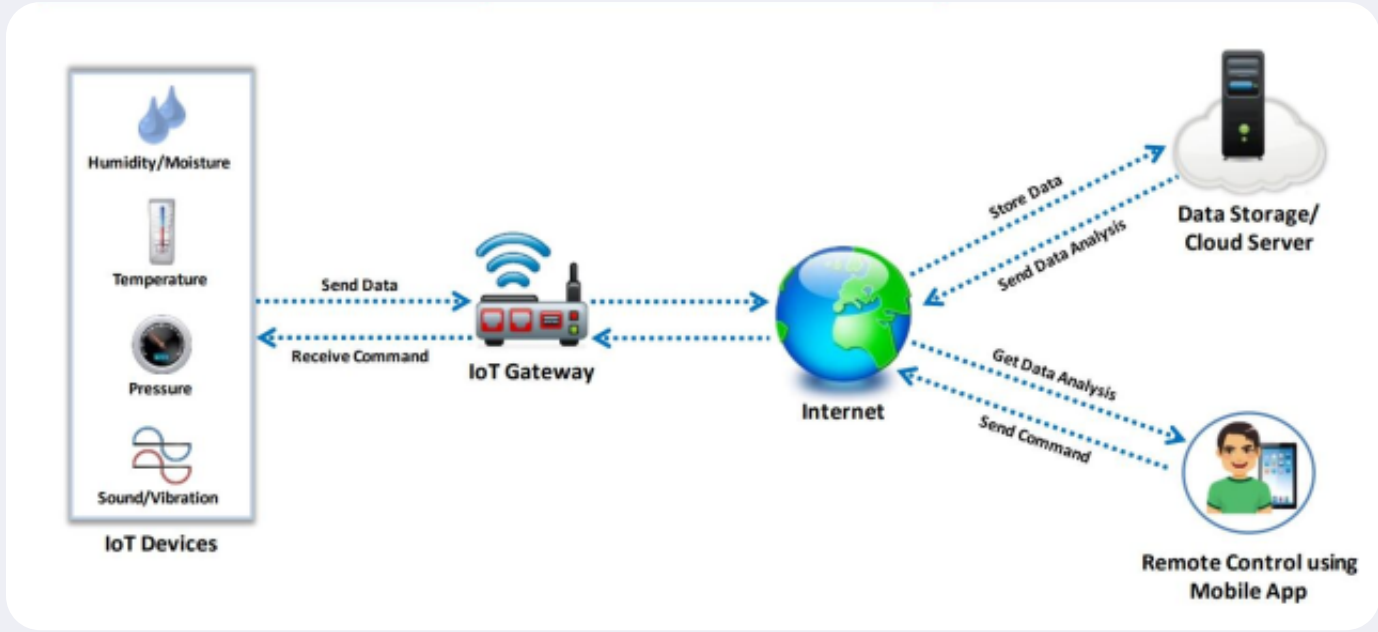
by Durgesh Thakare

Made with Gamma

Internet of Things (IoT), also known as Internet of Everything (IoE), refers to the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors In IoT, the term thing is used to refer to a device that is implanted on natural, human-made, or machine-made objects and has the functionality of communicating over the network

Made with Gamma

# HOW IOT WORKS




The Internet of Things (IoT) is a network of interconnected devices that communicate and share data over the internet. The basic concept involves embedding sensors, processors, and communication hardware into everyday objects, enabling them to send and receive data. Here's a general overview of how IoT works:

1. **Sensors and Actuators:**
   - **Sensors:** IoT devices are equipped with various types of sensors that can gather information from the environment. These sensors could include temperature sensors, motion sensors, light sensors, and more.
   - **Actuators:** In addition to sensors, many IoT devices have actuators that allow them to perform actions based on the data they receive. For example, a smart thermostat might not only sense the temperature but also actuate to adjust the heating or cooling.
2. **Connectivity:**
   - IoT devices need a way to transmit and receive data. They are equipped with communication technologies such as Wi-Fi, Bluetooth, Zigbee, or cellular networks, depending on the application and requirements.
   - The choice of connectivity method depends on factors such as range, power consumption, and data transfer speed.
3. **Data Processing:**
   - The collected data from sensors is processed locally on the device or transmitted to a cloud server for processing, depending on the device's capabilities and the application's requirements.
   - Local processing is often done to reduce latency and make real-time decisions on the device itself. Cloud processing allows for more complex analytics and storage of large datasets.
4. **Data Storage:**
   - Processed data is typically stored in databases or data lakes. Cloud platforms are commonly used for storing and managing IoT data due to their scalability and accessibility.
5. **Communication Protocols:**
   - Various communication protocols facilitate the exchange of data between IoT devices and servers. Examples include MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and HTTP/HTTPS.
6. **User Interface and Control:**
   - Users interact with IoT devices through interfaces such as mobile apps or web applications. These interfaces provide a way to monitor device status, receive alerts, and control device functionalities remotely.
7. **Security:**
   - Security is a critical aspect of IoT. Measures such as encryption, authentication, and secure communication protocols are implemented to protect data and ensure the integrity of the system.
8. **Analytics and Insights:**
   - Data collected from IoT devices can be analyzed to gain insights, identify patterns, and make informed decisions. Machine learning algorithms are often employed for predictive analytics.
9. **Feedback Loop:**
   - Based on the insights and analytics, IoT systems can generate feedback or trigger actions. For example, a smart irrigation system might adjust watering schedules based on weather forecasts and soil moisture data.

Made with Gamma

# Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below:

1. AI – IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.
2. Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.
3. Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
4. Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.
5. Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

Made with Gamma

# The architecture of an Internet of Things (IoT)

The architecture of an Internet of Things (IoT) system is designed to facilitate the seamless integration and communication between devices, sensors, networks, and cloud-based services. IoT architecture typically consists of multiple layers, each serving a specific purpose in the overall functionality of the system. Here is a general overview of the key components and layers in IoT architecture:

1. **Perception Layer (Sensors and Actuators):**
   - This is the bottommost layer of the IoT architecture and includes physical devices such as sensors and actuators.
   - **Sensors:** Gather data from the environment. Examples include temperature sensors, motion sensors, and light sensors.
   - **Actuators:** Perform actions based on the data received. For instance, actuators in smart thermostats adjust temperature settings.
2. **Network Layer:**
   - Responsible for transmitting data from sensors to the next layer in the architecture. It involves various communication protocols and technologies.
   - **Wireless Technologies:** Wi-Fi, Bluetooth, Zigbee, LoRa, and cellular networks are commonly used for device-to-device and device-to-cloud communication.
3. **Middleware Layer:**
   - Acts as a bridge between the network layer and the application layer, providing communication, data translation, and protocol conversion services.
   - **Message Queues:** Middleware often involves message queuing systems like MQTT or AMQP to manage the flow of messages between devices and applications.
4. **Application Layer:**
   - This layer consists of the actual applications and services that process and analyze the data collected from sensors.
   - **Data Processing and Analytics:** Application layer services process the data for insights, perform analytics, and make decisions based on the input.
   - **User Interface:** Provides a user interface for end-users to interact with the IoT system, monitor device status, and control device functionalities.
5. **Business Layer (IoT Platform):**
   - The business layer or IoT platform serves as the backbone of the IoT system. It manages device connectivity, data storage, and application enablement.
   - **Device Management:** Handles device provisioning, authentication, and software updates.
   - **Data Storage:** Manages databases or data lakes to store and retrieve IoT data efficiently.
   - **Security:** Implements security measures to protect data and devices.
6. **Edge Computing Layer:**
   - In some architectures, edge computing is introduced to process data closer to the source (devices) rather than sending all data to the cloud. This reduces latency and bandwidth usage.
   - **Edge Devices:** These are devices that perform processing tasks locally, closer to the sensors.
7. **Cloud Layer:**
   - The cloud layer involves cloud-based services that provide scalable storage, computation, and additional analytics capabilities.
   - **Scalable Storage:** Cloud platforms offer scalable storage solutions to handle large volumes of data generated by IoT devices.
   - **Advanced Analytics:** Cloud services may include machine learning algorithms for advanced analytics and predictive modeling.
8. **Security and Privacy Layer:**
   - Ensures the security and privacy of data throughout the entire IoT system.
   - **Encryption:** Implements encryption techniques to secure data during transmission and storage.
   - **Access Control:** Manages user access and permissions to prevent unauthorized access.
9. **Perception Layer (Sensors and Actuators):**
   - This is the bottommost layer of the IoT architecture and includes physical devices such as sensors and actuators.
   - **Sensors:** Gather data from the environment. Examples include temperature sensors, motion sensors, and light sensors.
   - **Actuators:** Perform actions based on the data received. For instance, actuators in smart thermostats adjust temperature settings.
10. **Network Layer:**
    - Responsible for transmitting data from sensors to the next layer in the architecture. It involves various communication protocols and technologies.
    - **Wireless Technologies:** Wi-Fi, Bluetooth, Zigbee, LoRa, and cellular networks are commonly used for device-to-device and device-to-cloud communication.
11. **Middleware Layer:**
    - Acts as a bridge between the network layer and the application layer, providing communication, data translation, and protocol conversion services.
    - **Message Queues:** Middleware often involves message queuing systems like MQTT or AMQP to manage the flow of messages between devices and applications.
12. **Application Layer:**
    - This layer consists of the actual applications and services that process and analyze the data collected from sensors.
    - **Data Processing and Analytics:** Application layer services process the data for insights, perform analytics, and make decisions based on the input.
    - **User Interface:** Provides a user interface for end-users to interact with the IoT system, monitor device status, and control device functionalities.
13. **Business Layer (IoT Platform):**
    - The business layer or IoT platform serves as the backbone of the IoT system. It manages device connectivity, data storage, and application enablement.
    - **Device Management:** Handles device provisioning, authentication, and software updates.
    - **Data Storage:** Manages databases or data lakes to store and retrieve IoT data efficiently.
    - **Security:** Implements security measures to protect data and devices.
14. **Edge Computing Layer:**
    - In some architectures, edge computing is introduced to process data closer to the source (devices) rather than sending all data to the cloud. This reduces latency and bandwidth usage.
    - **Edge Devices:** These are devices that perform processing tasks locally, closer to the sensors.
15. **Cloud Layer:**
    - The cloud layer involves cloud-based services that provide scalable storage, computation, and additional analytics capabilities.
    - **Scalable Storage:** Cloud platforms offer scalable storage solutions to handle large volumes of data generated by IoT devices.
    - **Advanced Analytics:** Cloud services may include machine learning algorithms for advanced analytics and predictive modeling.
16. **Security and Privacy Layer:**
    - Ensures the security and privacy of data throughout the entire IoT system.
    - **Encryption:** Implements encryption techniques to secure data during transmission and storage.
    - **Access Control:** Manages user access and permissions to prevent unauthorized access.

Made with Gamma

# IOT APPLICATION AREAS and DEVICES

| Service Sectors | Application Groups | Locations | Devices |
|---|---|---|---|
| **Buildings** | Commercial/ Institutional | Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums | Heating, Ventilation, and Air Conditioning (HVAC), Transport, Fire and Safety, Lighting, Security, Access, etc. |
| | Industrial | Process, Clean Room, Campus | |
| **Energy** | Supply/ Demand | Power Generation, Transport, and Distribution, Low Voltage, Power Quality, Energy Management | Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc. |
| | Alternative | Solar Wind, Co-generation, Electrochemical | |
| | Oil/Gas | Rigs, Derricks, Heads, Pumps, Pipelines | |

Made with Gamma

| | | | |
|---|---|---|---|
| **Consumer and Home** | Infrastructure | Wiring, Network Access, Energy Management | Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines / Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc. |
| | Awareness and Safety | Security/Alerts, Fire Safety, Elderly, Children, Power Protection | |
| | Convenience and Entertainment | HVAC/Climate, Lighting, Appliances, Entertainment | |
| **Healthcare and Life Science** | Care | Hospital, ER, Mobile, POC, Clinic, Labs, Doctors' Offices | MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc. |
| | In Vivo/Home | Implants, Home, Monitoring Systems | |
| | Research | Drug Discovery, Diagnostics, Labs | |
| **Transportation** | Non-Vehicular | Air, Rail, Marine | Vehicles, Lights, Ships, Planes, Signage, Tolls, etc. |
| | Vehicles | Consumer, Commercial, Construction, Off-Highway | |
| | Transport Systems | Tolls, Traffic Management, Navigation | |

Made with Gamma

| | | | |
|---|---|---|---|
| **Industrial** | Resource Automation | Mining, Irrigation, Agricultural, Woodland | Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc. |
| | Fluid/ Processes | Petrochemicals, Hydro, Carbons, Food, Beverages | |
| | Converting/ Discrete | Metals, Papers, Rubber/Plastic, Metalworking, Electronics, Assembly/Test | |
| | Distribution | Pipelines, Conveyance | |
| **Retail** | Specialty | Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events | POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc. |
| | Hospitality | Hotels Restaurants, Bars, Cafes, Clubs | |
| | Stores | Supermarkets, Shopping Centers, Single Site, Distribution, Centers | |
| **Security / Public Safety** | Surveillance | Radar/Satellite, Environment, Military Security, Unmanned, Fixed | Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc. |
| | Equipment | Weapons, Vehicles, Ships, Aircraft, Gear | |
| | Tracking | Human, Animal, Postal, Food, Health, Baggage | |

Made with Gamma

| | | | |
|---|---|---|---|
| | Public Infrastructure | Water, Treatment, Building, Environment, Equipment and Personnel, Police, Fire, Regulatory | |
| | Emergency Services | Ambulance, Police, Fire, Homeland Security | |
| **IT and Networks** | Public | Services, E-Commerce, Data Centers, Mobile Carriers, ISPs | Servers, Storage, PCs, Routers, Switches, PBXs, etc. |
| | Private Enterprise | IT/Data Center Office, Privacy Nets | |

Made with Gamma

# IOT TECHNOLOGIES AND PROTOCOLS

## Short-range Wireless Communication:

- **Bluetooth Low Energy (BLE):** Designed for short-range communication with low power consumption, commonly used in wearable devices and smart home applications.
- **Near Field Communication (NFC):** Enables short-range communication between devices, often used for contactless payments and data transfer.

## Medium-range Wireless Communication:

- **ZigBee:** A wireless communication standard for short to medium-range applications in home automation and industrial settings.
- **Z-Wave:** A wireless protocol for home automation, especially in smart home devices.

## Long-range Wireless Communication:

- **LoRaWAN:** A low-power, long-range wireless communication protocol suitable for IoT applications like smart agriculture and smart cities.
- **Sigfox:** A low-power, wide-area network (LPWAN) technology for long-range communication with low data rates.

## LPWAN (Low-power Wide Area Networking):

- **NB-IoT:** A cellular communication standard designed for low-power, wide-area IoT applications.

## Wired Communication:

- **Ethernet:** A standard for wired local area networking (LAN) commonly used for connecting devices in a network.

## IoT Operating Systems:

- **Windows 10 IoT:** An edition of the Windows 10 operating system designed for IoT devices.
- **Amazon FreeRTOS:** A real-time operating system (RTOS) for microcontrollers, compatible with AWS IoT services.
- **Contiki:** An open-source operating system designed for the Internet of Things.

## IoT Application Protocols:

- **MQTT (Message Queuing Telemetry Transport):** A lightweight messaging protocol often used for communication between devices in IoT.
- **CoAP (Constrained Application Protocol):** A lightweight protocol for constrained devices and networks.

## Wireless Communication:

- **Wi-Fi:** Standard for local wireless networking, commonly used for high-bandwidth applications.
- **Bluetooth:** A short-range wireless communication technology for connecting devices.

## Others:

- **QR Codes and Barcodes:** Used for encoding information and can be scanned by devices with cameras.
- **Radio Frequency Identification (RFID):** Technology for wireless data transfer and identification.

## IoT Operating Systems (Continued):

- **Ubuntu Core:** A version of Ubuntu designed for IoT and embedded systems.
- **ARM Mbed OS:** An operating system for IoT devices.
- **Zephyr:** An open-source RTOS for embedded systems.

## Communication Protocols (Continued):

- **Edge:** Microsoft's framework for IoT edge computing.

## IoT Protocols and Technologies (Continued):

- **LWM2M (Lightweight M2M):** A protocol for device management and service enablement in IoT.

## Communication Protocols (Continued):

- **Physical Web:** A project by Google that enables interaction with smart devices using web technologies.

## Networking Technologies (Continued):

- **VSAT (Very Small Aperture Terminal):** A satellite communication technology.

## IoT Protocols (Continued):

- **XMPP (Extensible Messaging and Presence Protocol):** A communication protocol for real-time communication.

## IoT Operating Systems (Continued):

- **RIOT:** An open-source operating system designed for the Internet of Things.

## Communication Protocols (Continued):

- **QUIC (Quick UDP Internet Connections):** A transport layer protocol designed for low-latency communication.

## Networking Technologies (Continued):

- **MQTT:** A messaging protocol for lightweight communication between devices.

## IoT Protocols (Continued):

- **Thread:** A low-power, wireless IoT protocol.

Made with Gamma

# OWASP iot atttack surface

1. **Insecure Web Interface:**
    - Default or weak credentials for web interfaces can provide unauthorized access to IoT devices.
    - Lack of secure communication (HTTPS) can expose sensitive data during transmission.
2. **Insecure Network Services:**
    - Unprotected network services and protocols may be vulnerable to attacks, including information disclosure and remote code execution.
3. **Insecure Ecosystem Interfaces:**
    - Insecure communication between IoT devices and other components in the ecosystem can lead to unauthorized access or data manipulation.
4. **Lack of Secure Update Mechanism:**
    - Absence of secure methods for updating firmware or software may expose devices to exploitation of known vulnerabilities.
5. **Insufficient Authentication/Authorization:**
    - Weak authentication mechanisms or insufficient authorization controls can lead to unauthorized access and privilege escalation.
6. **Insecure Cloud Interface:**
    - Vulnerabilities in the communication between IoT devices and cloud services can result in data breaches and unauthorized access.
7. **Insecure Mobile Interface:**
    - Weak security controls in mobile apps used to interact with IoT devices may lead to unauthorized access or data exposure.
8. **Insufficient Security Configurability:**
    - Devices lacking security configuration options may be more susceptible to attacks or may not be able to adapt to changing threat landscapes.
9. **Insecure Software/Firmware:**
    - Vulnerabilities in the software or firmware of IoT devices can be exploited for various malicious purposes.
10. **Poor Physical Security:**
    - Lack of physical security controls on IoT devices may result in unauthorized physical access, leading to tampering or theft.
11. **Privacy Concerns:**
    - Improper handling of user data or inadequate privacy controls may lead to privacy breaches.
12. **Insecure Data Transfer and Storage:**
    - Weak encryption or improper data storage mechanisms can result in the exposure of sensitive information.
13. **Lack of Device Management:**
    - Inadequate management controls for monitoring, updating, and retiring IoT devices can lead to security gaps.
14. **Insecure Default Settings:**
    - Devices with insecure default settings may be more susceptible to attacks if users do not change or update these settings.
15. **Lack of Physical Hardening:**
    - Devices that lack physical hardening measures may be susceptible to physical attacks.
16. **Social Engineering:**
    - Human factors, such as social engineering attacks, can manipulate users into taking actions that compromise the security of IoT systems.

Made with Gamma

# IOT VULNURBULITY

Internet of Things (IoT) vulnerabilities refer to weaknesses, flaws, or gaps in the security of IoT devices, networks, and systems that could be exploited by malicious actors. These vulnerabilities pose significant risks to the confidentiality, integrity, and availability of data and services within IoT ecosystems. Here are some common IoT vulnerabilities:

1. **Insecure Authentication and Authorization:**
    - Weak or default passwords, lack of multifactor authentication, or inadequate authorization mechanisms can lead to unauthorized access.
2. **Insufficient Encryption:**
    - Inadequate or absent encryption for data in transit and at rest can expose sensitive information to interception or tampering.
3. **Lack of Device Patching and Updates:**
    - Devices without mechanisms for regular updates and patches are vulnerable to exploitation of known security vulnerabilities.
4. **Insecure Network Services:**
    - Vulnerabilities in network protocols and services may allow attackers to compromise communication channels and gain unauthorized access.
5. **Weak Physical Security:**
    - Physical tampering or theft of devices can occur if there is insufficient protection against unauthorized physical access.
6. **Insecure Device Configuration:**
    - Devices with insecure default settings or lacking proper configuration options can be exploited by attackers.
7. **Inadequate Device Management:**
    - Poorly managed devices may lack monitoring, logging, and reporting capabilities, making it challenging to detect and respond to security incidents.
8. **Insufficient Input Validation:**
    - Lack of proper input validation in IoT applications can lead to injection attacks, such as command injection or SQL injection.
9. **Privacy Concerns:**
    - Improper handling of user data, lack of privacy controls, or excessive data collection may lead to privacy breaches.
10. **Insecure Cloud Interfaces:**
    - Vulnerabilities in the communication between IoT devices and cloud services may result in unauthorized access to cloud-stored data.
11. **Denial of Service (DoS) Attacks:**
    - Devices or networks may be susceptible to DoS attacks, disrupting service availability.
12. **Insecure Firmware and Software:**
    - Vulnerabilities in the firmware or software of IoT devices can be exploited for malicious purposes, including remote code execution.
13. **Man-in-the-Middle Attacks:**
    - Lack of proper authentication and encryption can expose IoT communication to interception by attackers.
14. **Vendor-specific Vulnerabilities:**
    - Security flaws in devices may stem from poor security practices during the manufacturing process or inadequate testing.
15. **Social Engineering Attacks:**
    - Human factors, such as phishing or impersonation, can be exploited to gain unauthorized access or manipulate users.
16. **Supply Chain Attacks:**
    - Compromises in the supply chain, such as tampering with components during manufacturing or distribution, can introduce vulnerabilities.
17. **Insecure Wireless Communication:**
    - Weak encryption or inadequate security measures in wireless communication protocols can expose data to interception.
18. **Interoperability Issues:**
    - Lack of standardized security measures may result in vulnerabilities when IoT devices from different manufacturers interact.

Made with Gamma

# IOT Threats

1. **DDoS (Distributed Denial of Service):**
    a. DDoS attacks involve overwhelming a target system, network, or service with a flood of internet traffic to make it unavailable to its intended users.
2. **HVAC System (Heating, Ventilation, and Air Conditioning):**
    a. HVAC systems can be vulnerable to cyber threats if they are connected to the internet. Attackers might exploit vulnerabilities to gain unauthorized control, disrupt operations, or manipulate temperature settings.
3. **BlueBorne:**
    a. BlueBorne is a set of vulnerabilities affecting Bluetooth-enabled devices. Exploiting these vulnerabilities can allow attackers to take control of devices, spread malware, or perform other malicious activities.
4. **Jamming:**
    a. Jamming refers to the interference with wireless communication signals, disrupting normal communication between devices. This can be done intentionally to cause denial of service.
5. **Remote Access:**
    a. Remote access refers to the ability to access a computer or network from a location other than the physical location of the system. It can be exploited by attackers if not properly secured, leading to unauthorized access.
6. **Sybil Attack:**
    a. A Sybil attack involves creating multiple fake identities to gain a disproportionately large influence over a network. In the context of IoT, this could lead to manipulation of data or control.
7. **Man-in-the-Middle (MitM) Attack:**
    a. In a MitM attack, an attacker intercepts and potentially alters the communication between two parties without their knowledge. This can lead to data theft, manipulation, or unauthorized access.
8. **Forged Malicious:**
    a. It's possible you're referring to the concept of forging malicious data or activities. "Forging" generally means creating something false or imitating. In a cybersecurity context, this could involve creating malicious files, emails, or other digital entities with deceptive intent.
9. **SQL Injection:**
    a. SQL injection is a type of cyber attack where an attacker injects malicious SQL code into input fields of a web application's database query. If the application doesn't properly validate or sanitize inputs, it can lead to unauthorized access, data manipulation, or even data deletion.
10. **DNS Rebinding:**
    a. DNS rebinding is an attack technique that manipulates the Domain Name System (DNS) to bypass the same-origin policy in web browsers. This allows an attacker to make a victim's web browser interact with resources on a different domain, potentially leading to unauthorized access or data theft.
11. **Network Porting:**
    a. It seems there might be a slight confusion in the term. "Network porting" could refer to the process of configuring network ports, but it's not a commonly used term in cybersecurity. If you meant something else or have a specific term in mind, please provide more details.

Made with Gamma

# IOT hacking methodology

1. **Reconnaissance:**
    - Gather information about the target IoT system. This includes identifying devices, network architecture, communication protocols, and potential entry points.
2. **Scanning:**
    - Use scanning tools to discover active devices, open ports, and services in the target network. Identify potential vulnerabilities that could be exploited.
3. **Enumeration:**
    - Gather additional details about the devices and services identified in the scanning phase. This may involve extracting information about the device's configuration, software versions, and potential weaknesses.
4. **Vulnerability Analysis:**
    - Analyze the collected information to identify potential vulnerabilities in the IoT devices, applications, or network components.
5. **Exploitation:**
    - Attempt to exploit the identified vulnerabilities to gain unauthorized access, manipulate data, or control the IoT devices. This phase may involve using known exploits or developing custom exploits.
6. **Post-Exploitation:**
    - Assess the impact of successful exploits and determine the extent of compromise. Identify potential further actions an attacker could take after gaining initial access.
7. **Documentation:**
    - Document the entire testing process, including the vulnerabilities discovered, the methods used for exploitation, and the impact of successful attacks.
8. **Reporting:**
    - Prepare a comprehensive report outlining the findings, risks, and recommendations for mitigating the identified vulnerabilities. This report is typically shared with the organization that owns the IoT devices to help them improve security.
9. **Remediation:**
    - Work collaboratively with the organization to address and fix the identified vulnerabilities. This may involve applying patches, configuring security settings, or implementing additional security controls.
10. **Verification:**
    - Verify that the remediation measures are effective in mitigating the identified vulnerabilities. Conduct additional testing to ensure that the security posture of the IoT system has improved.

Made with Gamma

# The advantages of IoT

The advantages of IoT span across every area of lifestyle and business. Here is a list of some of the advantages that IoT has to offer:

1. Improved Customer Engagement – Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive. IoT completely transforms this to achieve richer and more effective engagement with audiences.
2. Technology Optimization – The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.
3. Reduced Waste – IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
4. Enhanced Data Collection – Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyze our world. It allows an accurate picture of everything.

Made with Gamma

# Disadvantages

Though IoT delivers an impressive set of benefits, it also presents a significant set of challenges. Here is a list of some its major issues:

1. Security – IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
2. Privacy – The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
3. Complexity – Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.
4. Flexibility – Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
5. Compliance – IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle.

Made with Gamma