

Module 09

IoT Device Security



Module Objectives

1. Understanding the IoT and Why Organizations Opt for IoT-enabled Environments
2. Overview of IoT Application Areas and IoT Devices
3. Understanding the IoT Architecture and IoT Communication Models
4. Understanding the Security in IoT-Enabled Environments
5. Understanding the Security Considerations of the IoT Framework
6. Overview of IoT Device Management
7. Understanding the Best Practices and Tools for IoT Security

Module Flow

1

Understand IoT Devices, Application Areas, and Communication Models

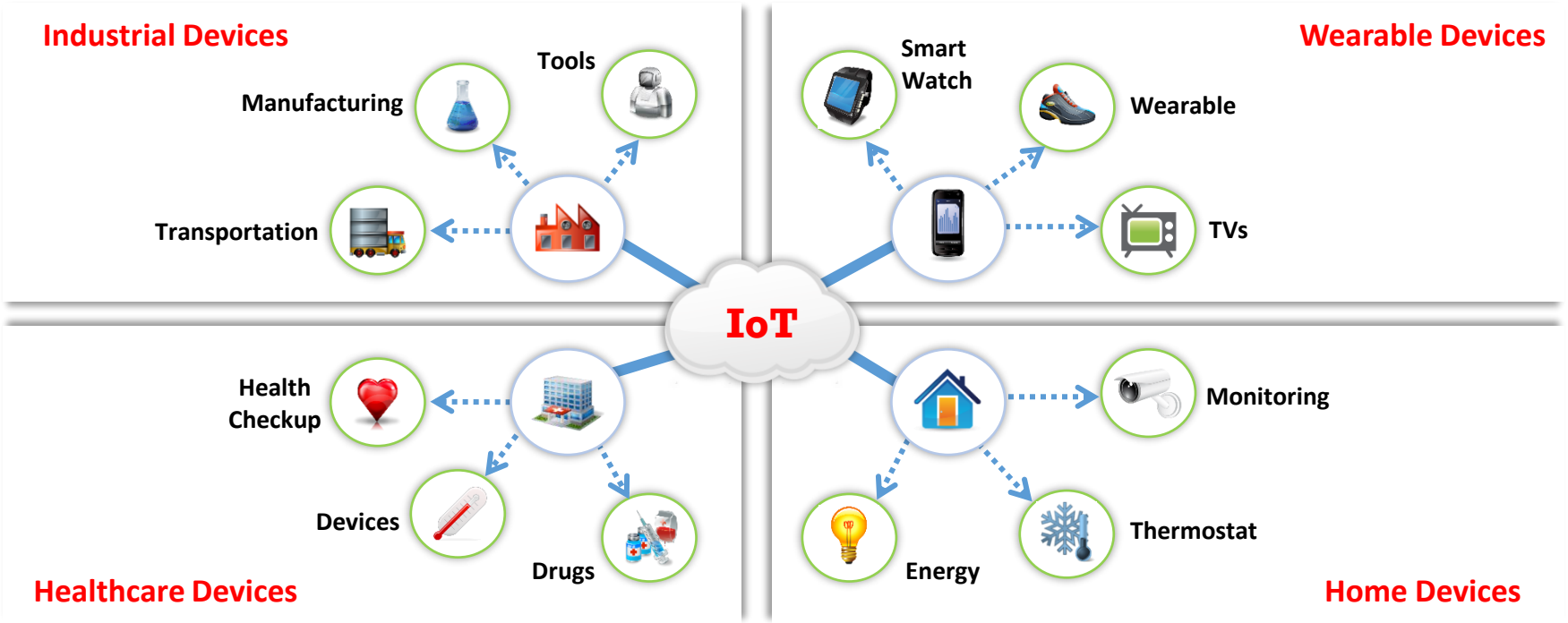


2

Discuss the Security in IoT-enabled Environments

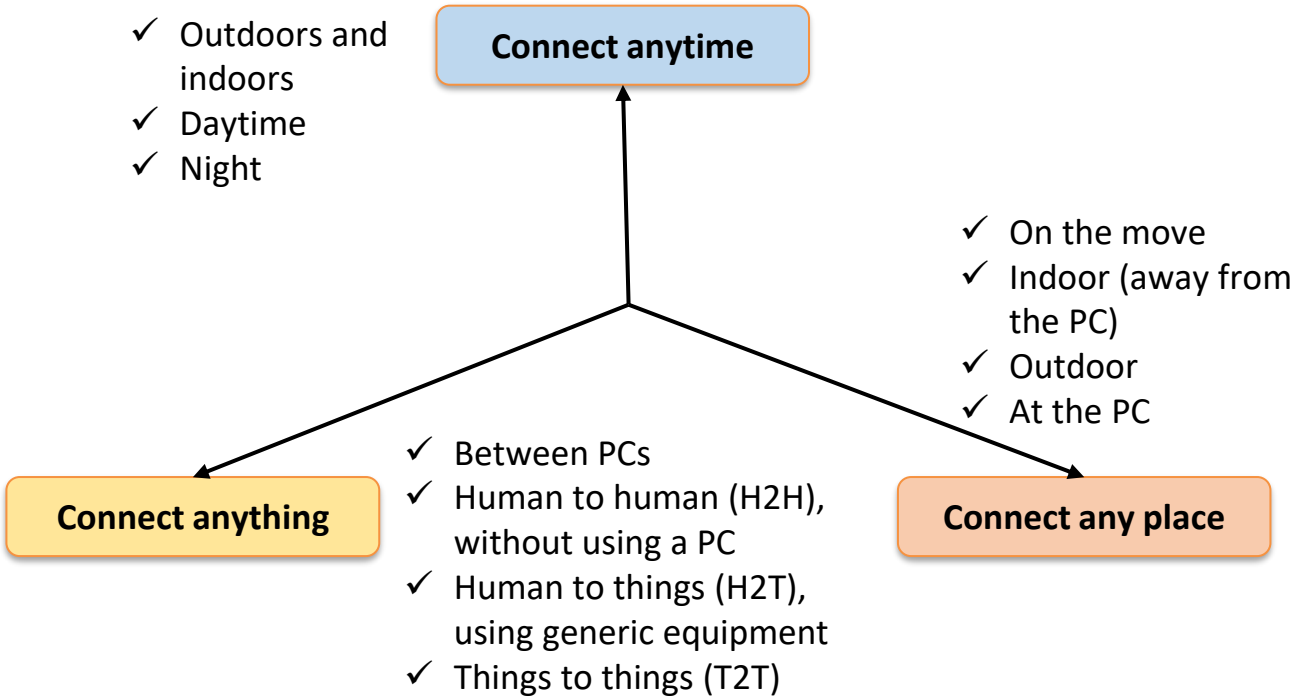
What is IoT?

- 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**



Why Organizations are Opting for IoT-enabled Environments

IoT devices work on a **three-dimensional plane**, offering connectivity for anyone at anytime, for anything, and from any place





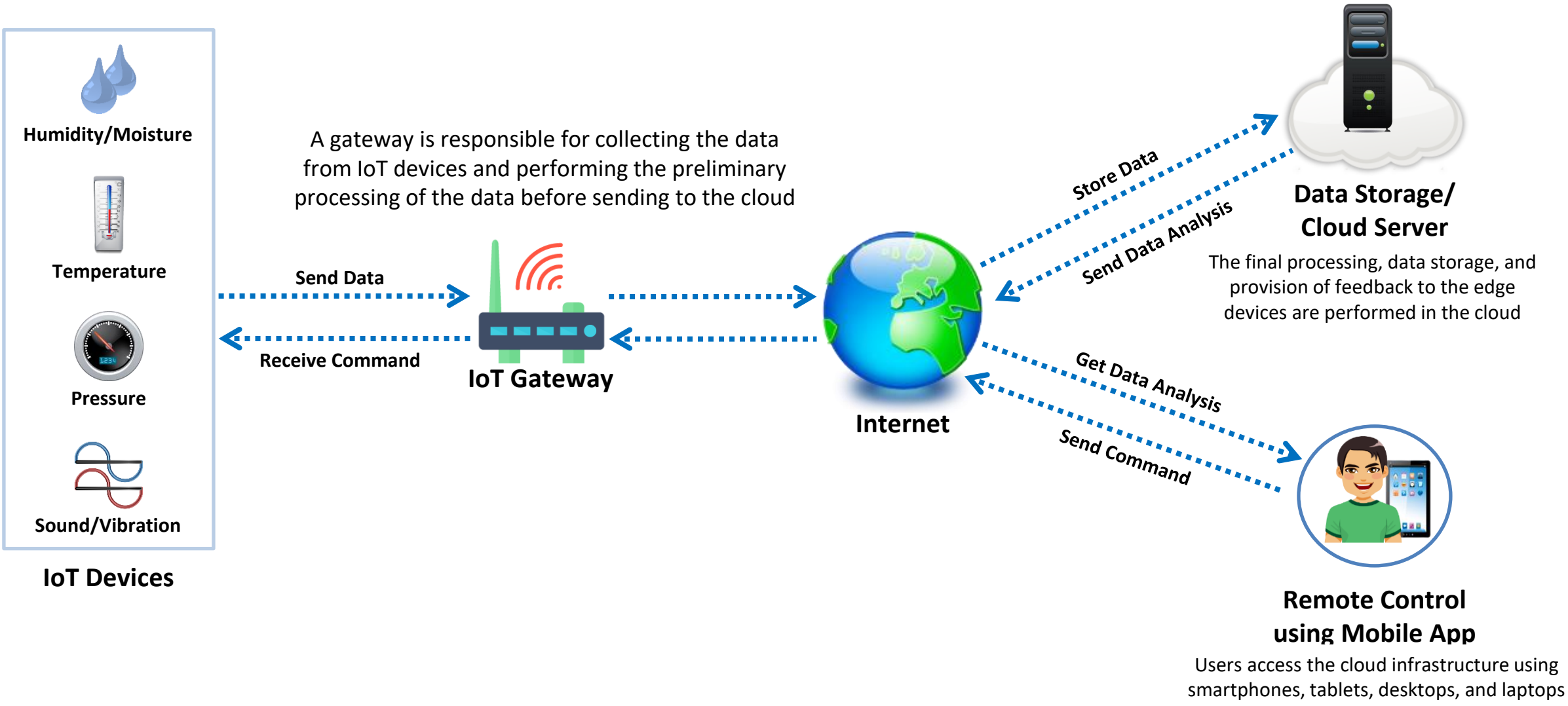
IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, 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	
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 & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	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	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

IoT Application Areas and Devices (Cont'd)

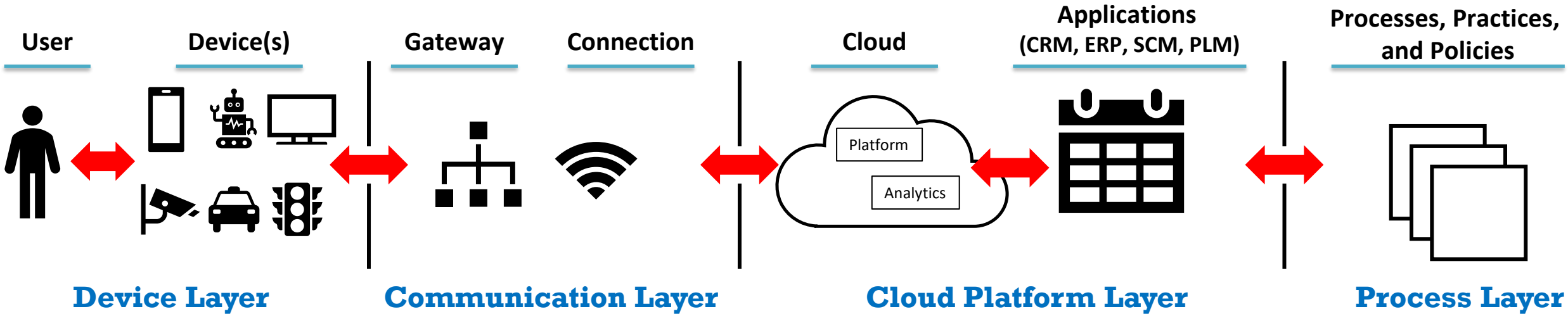
Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, 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, Environ., 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	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & 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	

IoT Architecture



Layers of the IoT Architecture



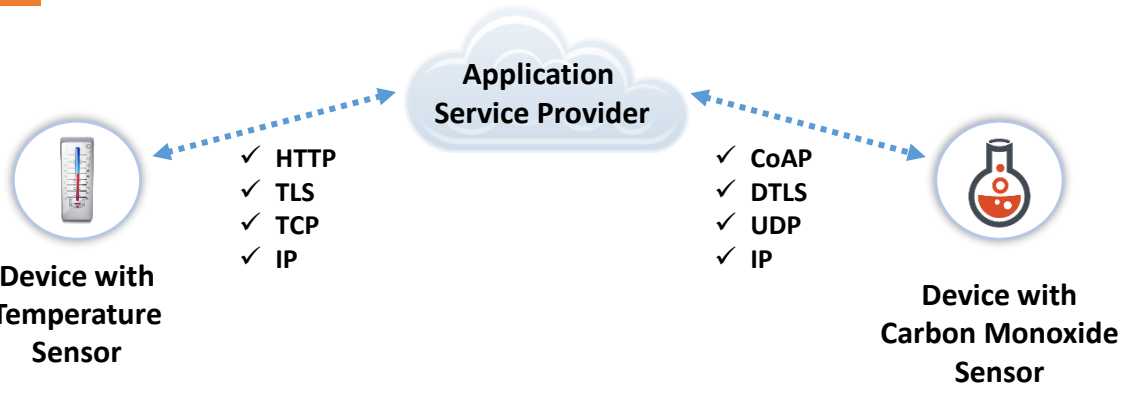


IoT Communication Models

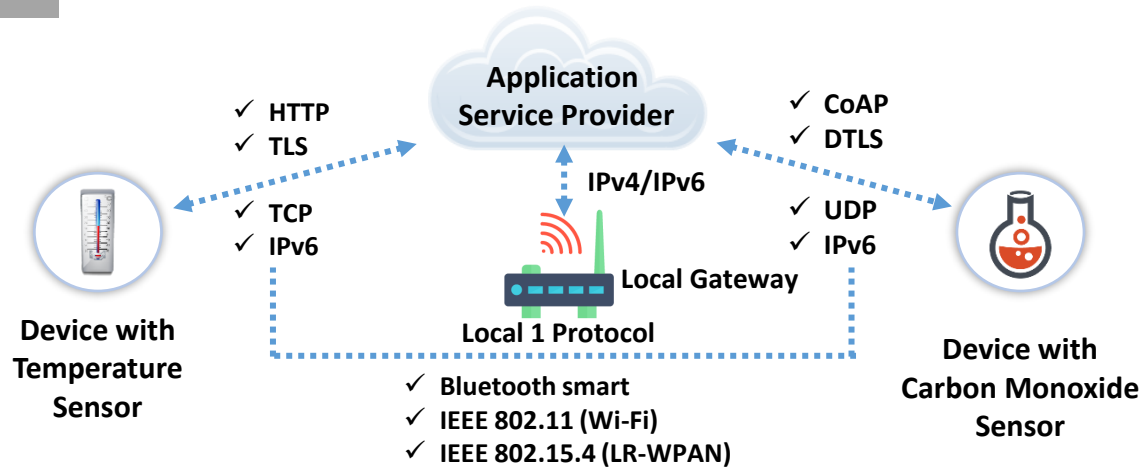
01 Device-To-Device Model



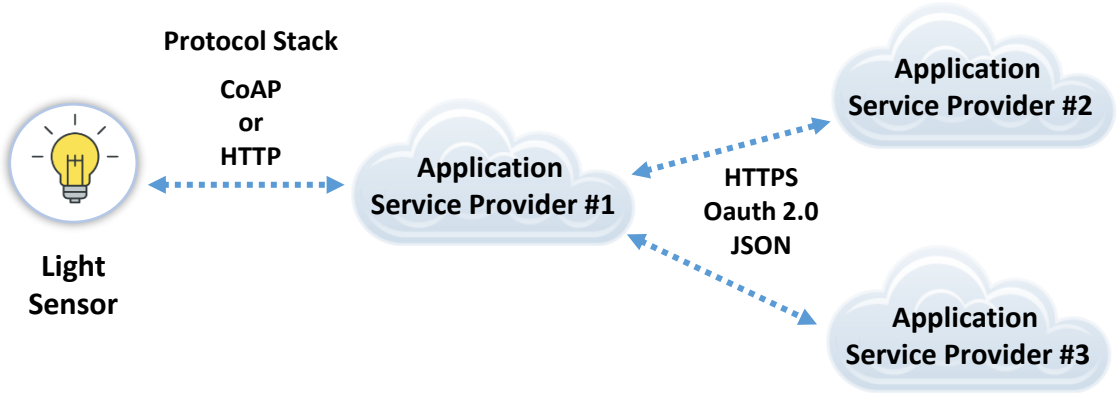
02 Device-To-Cloud Model



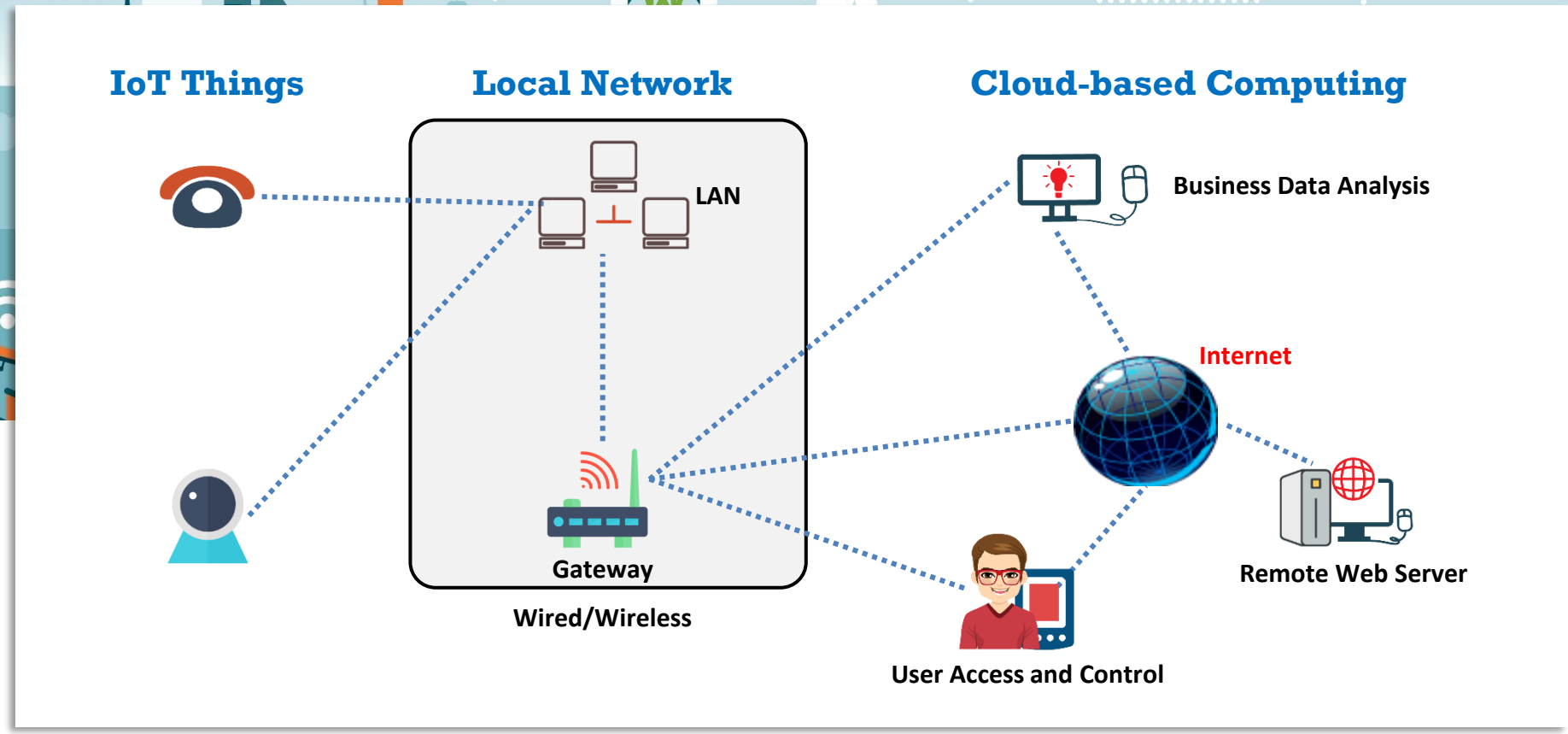
03 Device-to-Gateway Model



04 Cloud-to-Cloud (Back-End Data-Sharing Model)



IoT-Enabled IT Environment



IoT-Enabled IT Environment (Cont'd)

Features of an IoT-Enabled IT Environment

- **Real-time monitoring** involves monitoring IoT assets, processing products, maintaining a flow, helping detect issues, and taking actions immediately
- **Real-time analytics** involves analyzing IoT things and taking steps accordingly
- **Multi-layer security** involves preventing unauthorized access to IoT things by using multi-factor authentication (MFA), Transport Layer Security (TLS), device identity management, etc.
- **Data collection** involves the exchange of data between IoT-enabled organizations using different communication protocols
- **Communication** among multiple devices involves configuring multiple devices to access IoT things even remotely at any time and from anywhere



Module Flow

1

Understand IoT Devices, Application Areas, and Communication Models



2

Discuss the Security in IoT-enabled Environments

Security in IoT-enabled Environments



With no or inadequate focus on IoT device security by manufacturers, security measures used to **harden** the IoT device are often insufficient

Therefore, organizations should focus on countering attack scenarios in IoT-enabled environments. Organizations should focus on securing network devices and routers in an IoT-enabled environment. This helps restrict the attacker from accessing other parts of the network and performing targeted attacks

The organization should use **multilayered** management. An overarching multilayered security plan and constant maintenance are necessary to effectively secure all these disparate IoT devices

Company-wide **collaboration** and **synchronization** are required to secure an IoT-enabled environment

IoT System Management



Device Management

- Ensure **secure data transmission** to facilitate fine interaction between devices and to guarantee the proper functioning of devices in an IoT system



User Management

- Provide control over the users who have access to an IoT system. User management includes **identifying users**, **setting user roles** and **access levels**, **controlling access**, etc.

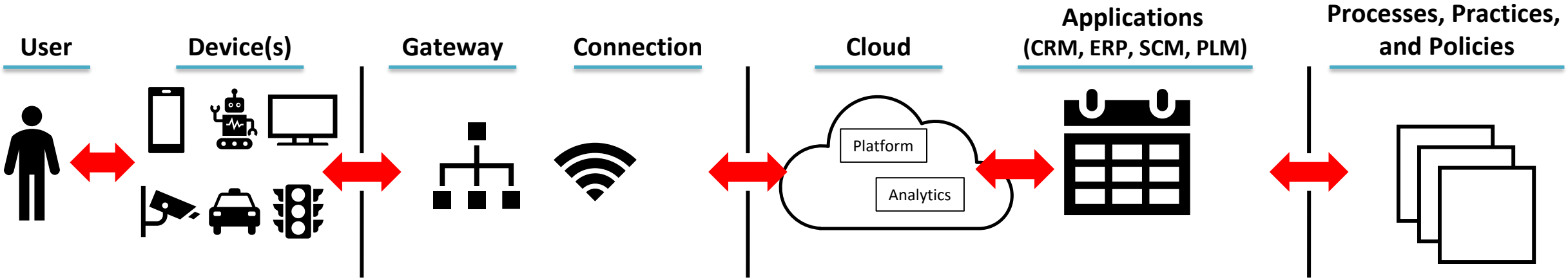


Security Monitoring

- To address security breaches at early stages and to prevent malicious attacks on an IoT system, perform the activities such as **log and analyze commands** sent by control applications to things, **monitor** and **store all the actions** of users, **identify the patterns** of malicious behavior, etc.

Stack-wise IoT Security Principles







IoT Framework Security Considerations

EDGE

- Communications encryption
- Storage encryption
- Update components
- No default passwords

GATEWAY

- Multi-directional encrypted communications
- Strong authentication of all the components
- Automatic updates

CLOUD PLATFORM

- Encrypted communications
- Secure web interface
- Authentication
- Encrypted storage
- Automatic updates

MOBILE

- Local storage security
- Encrypted communications channels
- Multi-factor authentication
- Account lockout mechanism

IoT Device Management

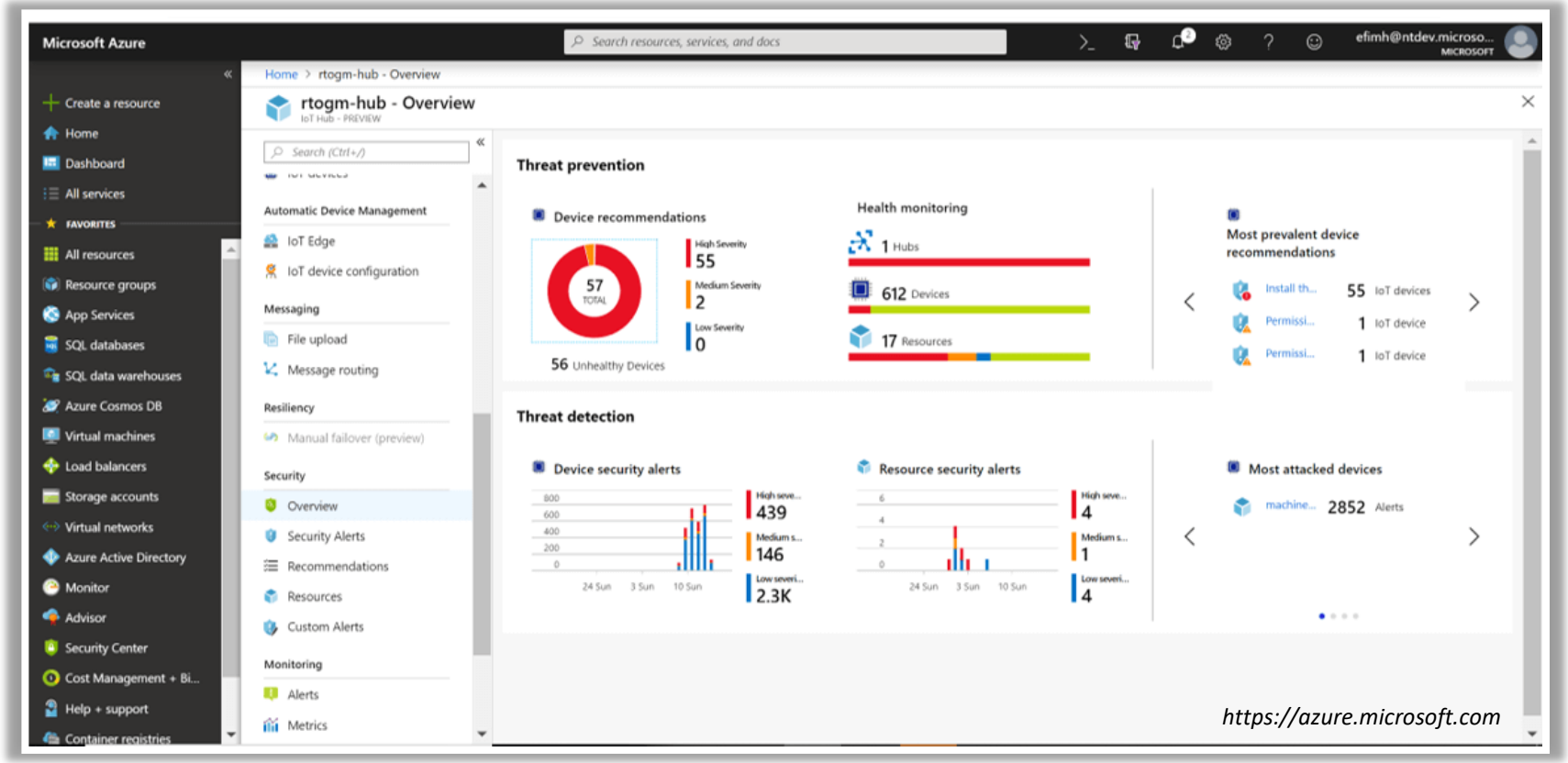
- IoT device management helps in supporting IoT solutions by using any software tools and processes and helps in **onboarding latest devices** securely and promptly



IoT Device Management Solutions

- **Oracle IoT Asset Monitoring Cloud**
  https://www.oracle.com
- **Predix**
  https://www.ge.com
- **Cloud IoT Core**
  https://cloud.google.com
- **IBM Watson IoT Platform**
  https://www.ibm.com
- **AT&T IoT Connectivity Management**
  https://www.business.att.com

Azure IoT Central



IoT Security Best Practices

1

Disable the “**guest**” and “**demo**” user accounts if enabled

2

Use the “**Lock Out**” feature to lock out accounts for excessive invalid login attempts

3

Implement **strong authentication** mechanisms

4

Locate control system networks and devices behind firewalls and isolate them from the business network

5

Implement **IPS** and **IDS** in the network

6

Implement **end-to-end encryption** and use Public Key Infrastructure (PKI)

7

Use **VPN architecture** for secure communication

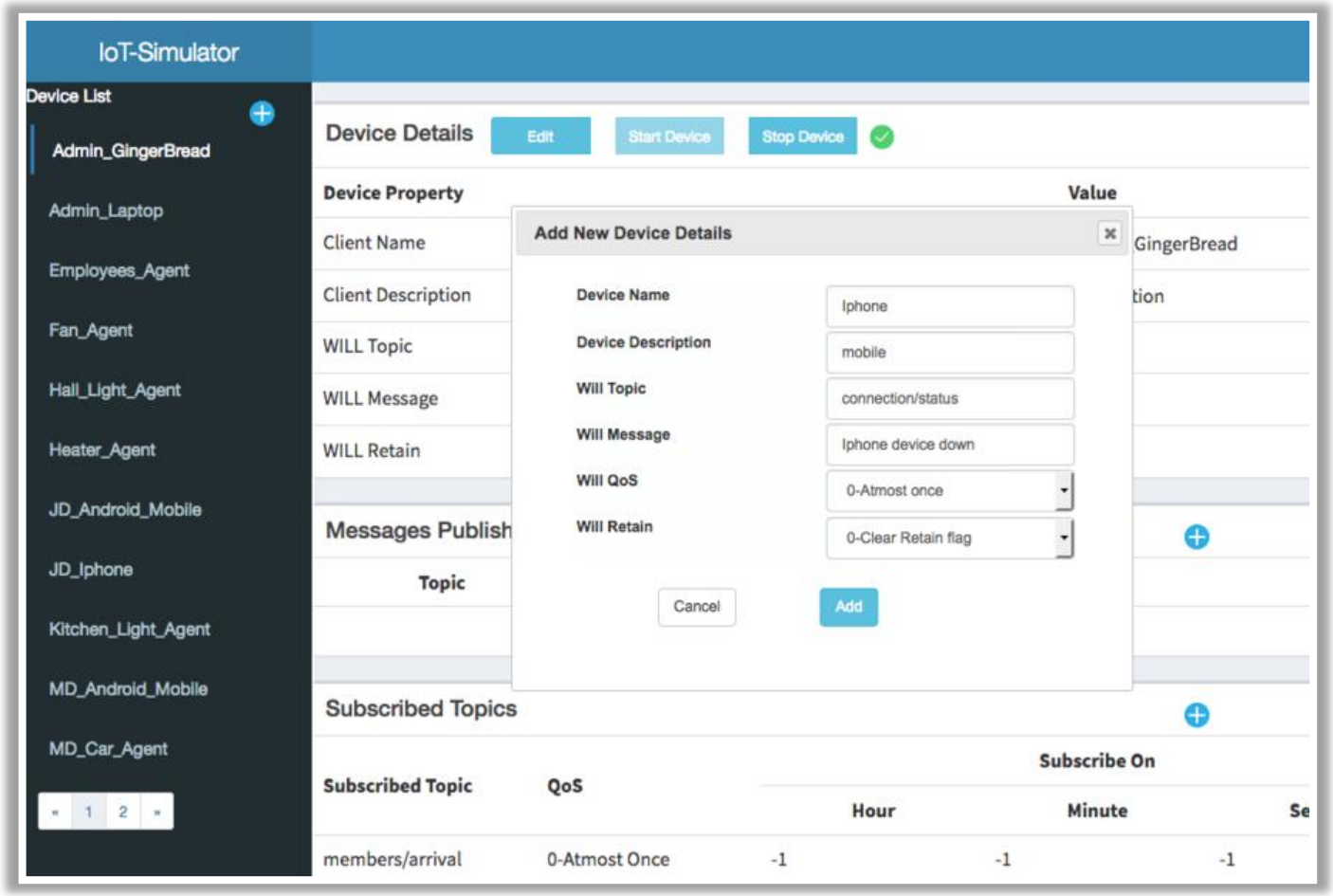
8

Deploy security as a **unified**, **integrated system**

IoT Security Tools

Bevywise IoT Simulator

Bevywise IoT Simulator is an intelligible simulation tool to simulate tens of thousands of **MQTT clients** in a single box



https://www.bevywise.com

SeaCat.io
https://teskalabs.com

DigiCert IoT Security Solutions
https://www.digicert.com

FortiNAC
https://www.fortinet.com

Darktrace
https://www.darktrace.com

Cisco IoT Threat Defense
https://www.cisco.com

Module Summary

1. This module has discussed the IoT concepts and why organizations opt for IoT-enabled environments
2. It has discussed the IoT application areas and IoT devices
3. It has also discussed the IoT architecture and IoT communication models
4. This module also discussed the security in IoT-enabled environments and stack-wise IoT security principles
5. It has briefly discussed the security considerations of the IoT framework and IoT device management
6. Finally, this module ended with a detailed discussion on the best practices and tools for IoT security
7. In the next module, we will discuss on cryptography and PKI concepts in detail

