Emergence of IoT

Computing for Internet of Things

Dr. Arijit Roy

Overview

Global Trends in IoT

- Each second, the present-day Internet allows massively heterogeneous traffic through it.
- This network traffic consists of images, videos, music, speech, text, numbers, binary codes, machine status, banking messages, data from sensors and actuators, healthcare data, data from vehicles, home automation system status and control messages, military communications, and many more.
- This huge variety of data is generated from a much massive number of connected devices, which may be directly connected to the Internet or through gateway devices.
- The total number of connected devices globally is estimated to be around 25 billion. This figure is projected to be tripled within a short span of 7 years by the year 2025.

IoT Trends

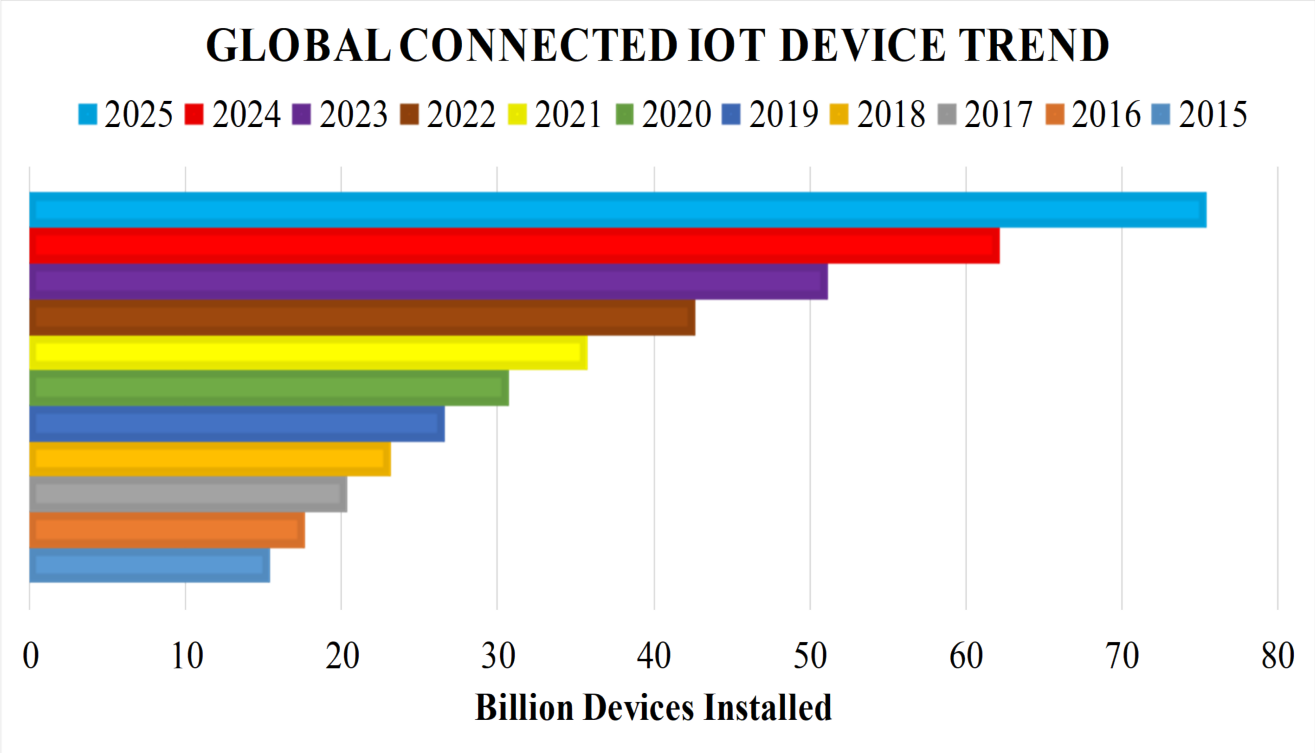


Figure: The 10-year global trend and projection of connected devices

IoT Trends

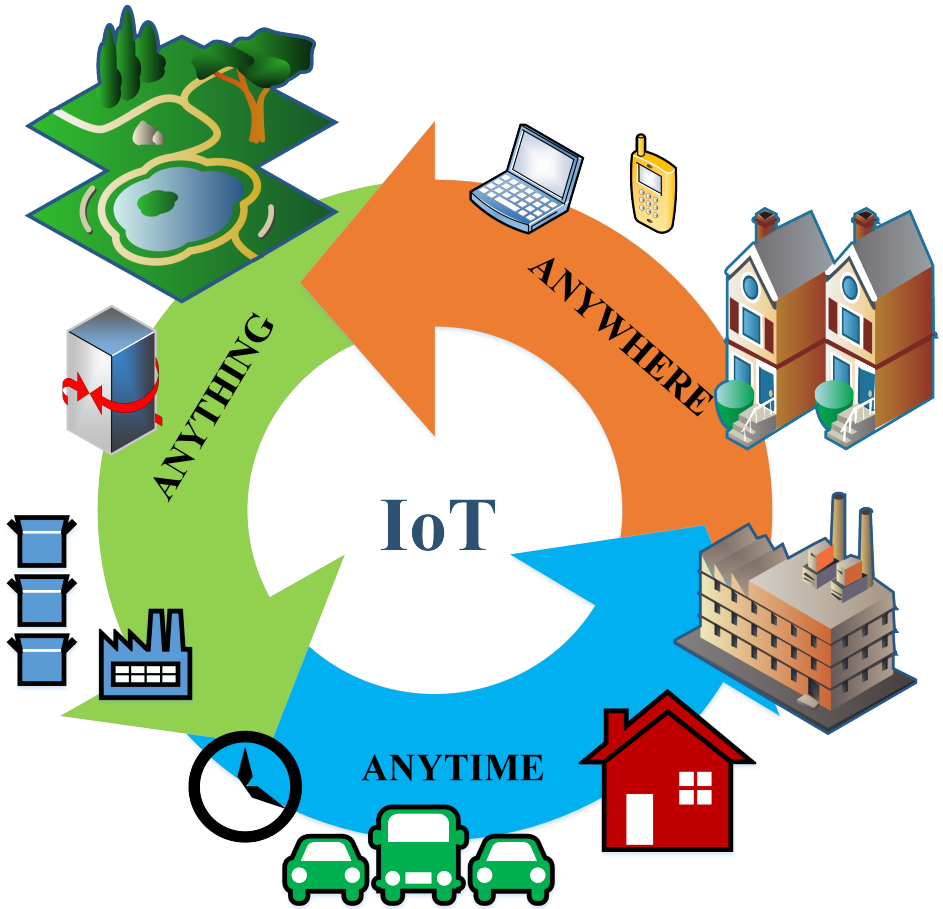


Figure: The three characteristic features – Anytime, Anywhere, and Anything – highlight the robustness and dynamic nature of IoT

IoT Trends

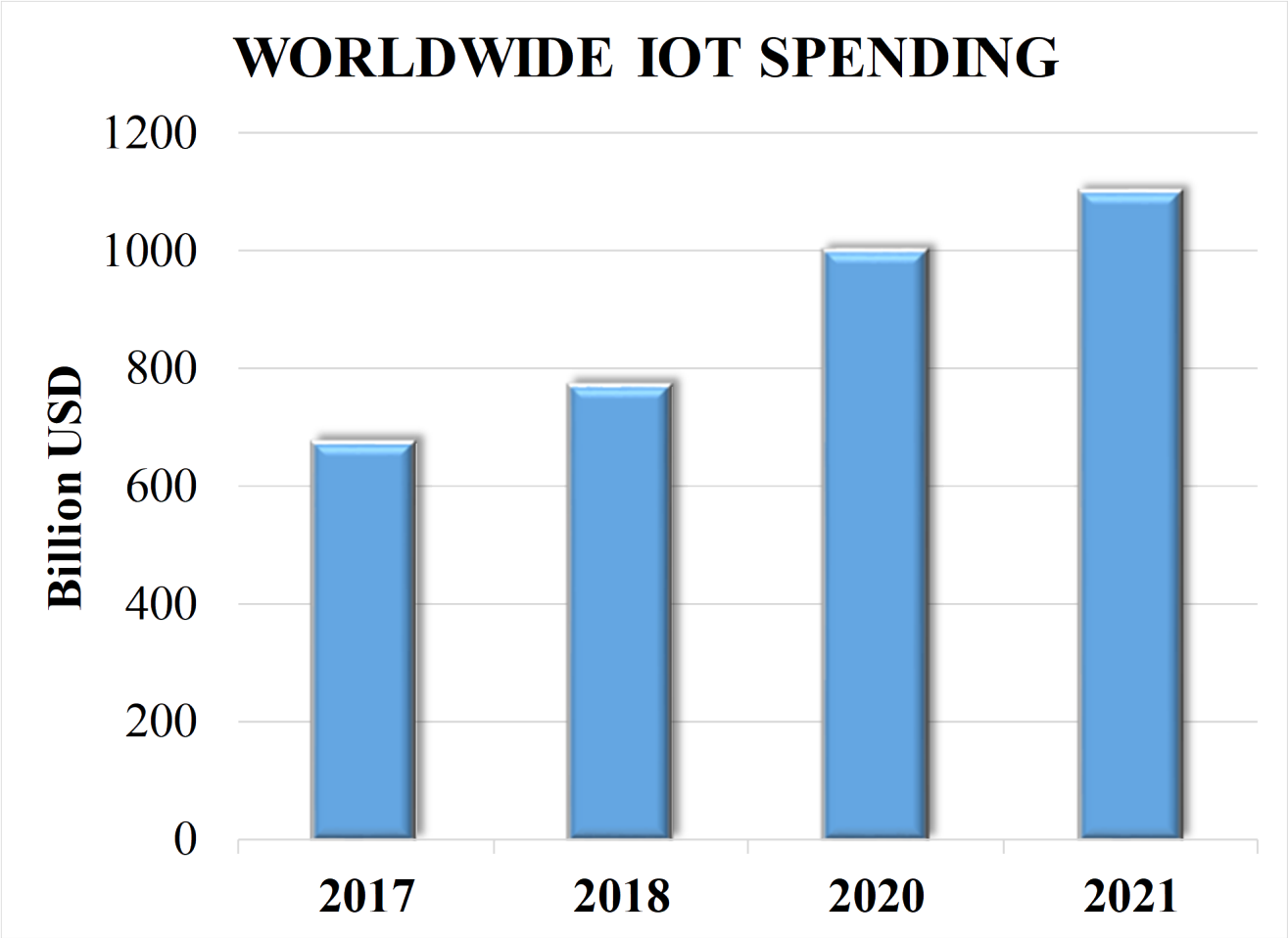
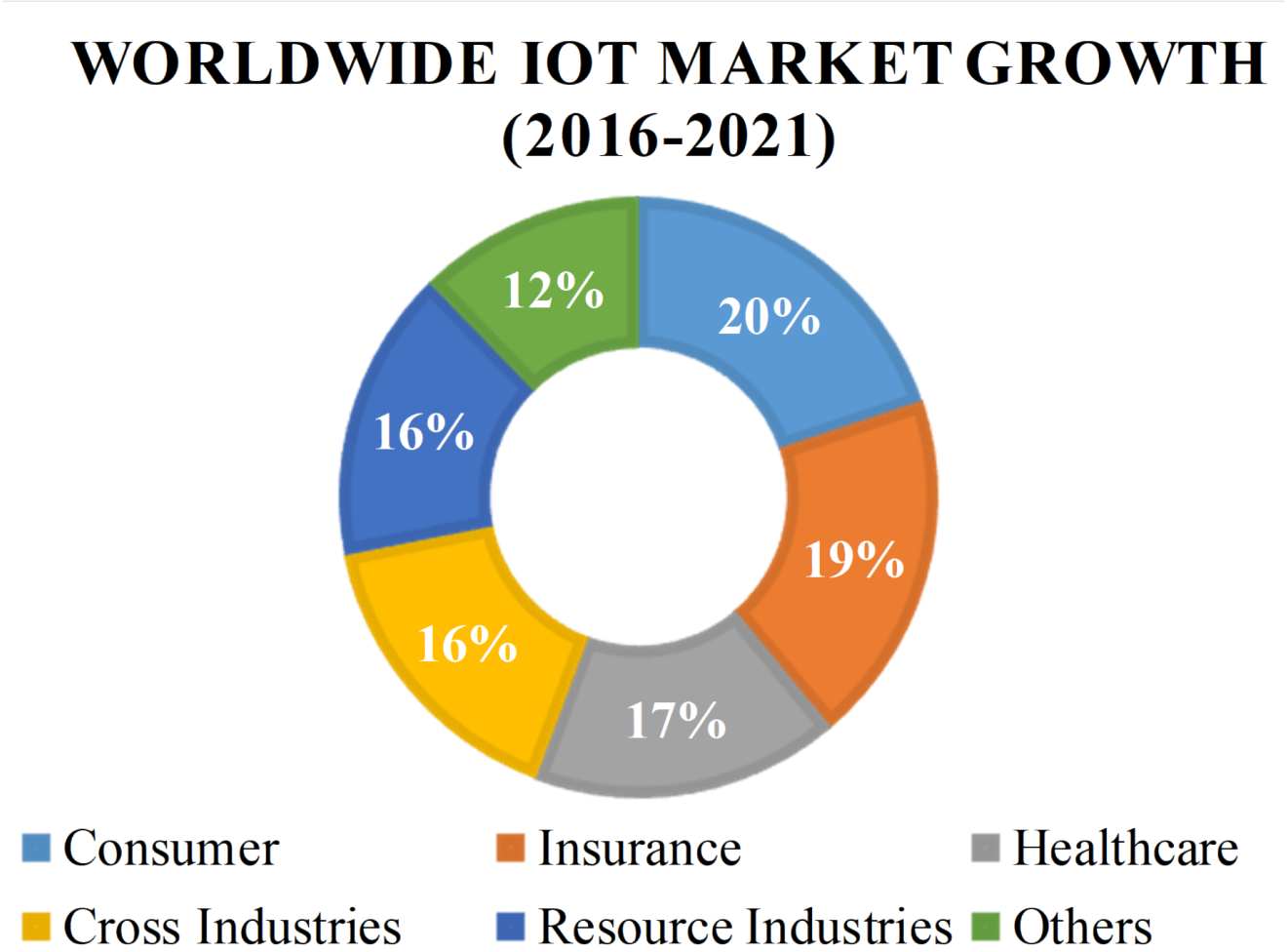
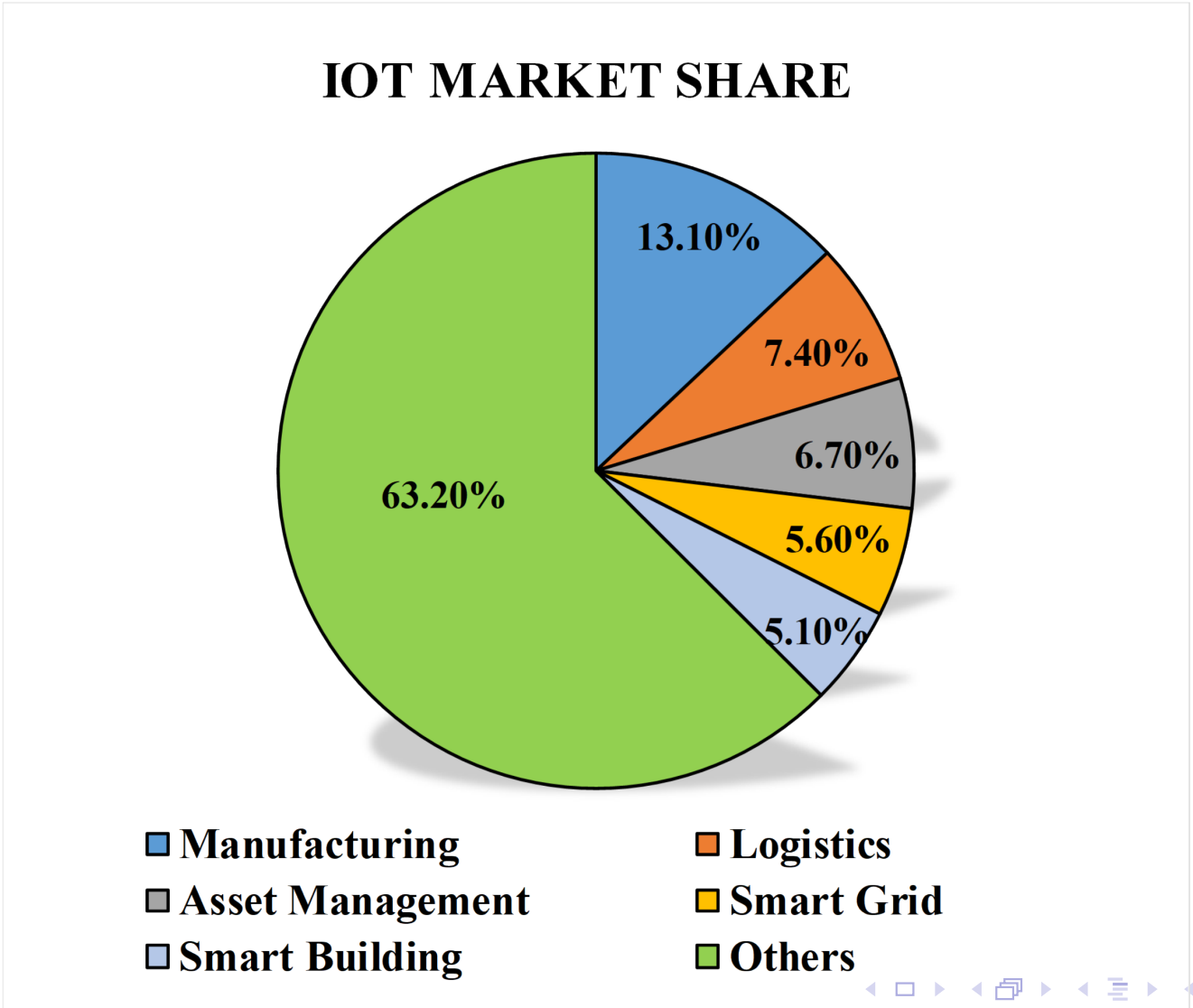


Figure: The global IoT spending across various organizations and industries and its subsequent projection till the year 2021

IoT Trends


WORLDWIDE IOT MARKET GROWTH
(2016-2021)
20%
19%
17%
16%
16%
12%
Consumer
Insurance
Healthcare
Cross Industries
Resource Industries
Others

IoT Trends


IOT MARKET SHARE
13.10%
7.40%
6.70%
5.60%
5.10%
63.20%
Manufacturing
Logistics
Asset Management
Smart Grid
Smart Building
Others

IoT Characteristics

IoT systems can be characterized by the following features:

- Associated architectures, which are also efficient and scalable.
- No ambiguity in naming and addressing.
- Massive number of constrained devices, sleeping nodes, mobile devices, and non-IP devices.
- Intermittent and often unstable connectivity.

Evolution of IoT

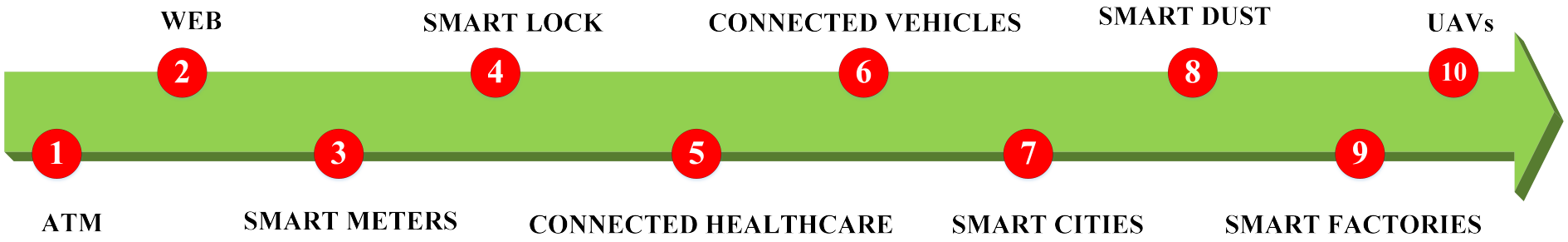


Figure: The sequence of technological developments leading to the shaping of the modern-day IoT

Technological Interdependencies in IoT

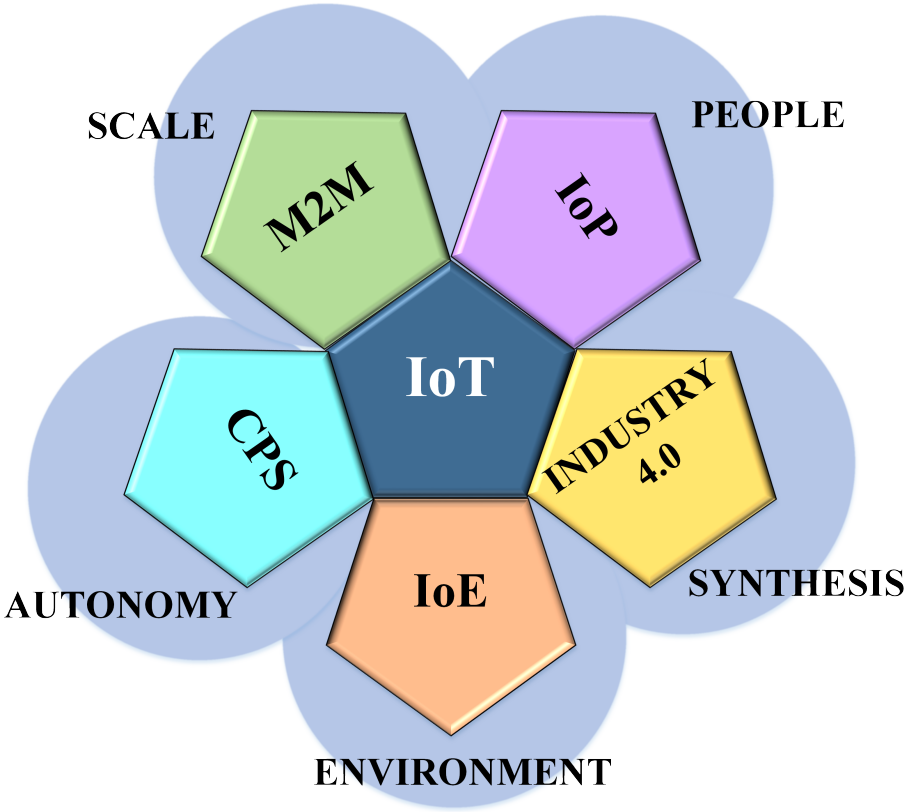


Figure: The interdependence and reach of IoT over various application domains and networking paradigms

M2M

- The M2M or the Machine-to-Machine paradigm signifies a system of connected machines and devices, which can talk amongst themselves without human intervention.
- The communication between the machines can be for
  1. updates on machine status (stocks, health, power status, and others)
  2. collaborative task completion
  3. overall knowledge of the systems and the environment

CPS

- The CPS or the Cyber-Physical System paradigm insinuates a closed control loop – from sensing, processing, and finally to actuation – using a feedback mechanism.
- CPS helps in maintaining the state of an environment through the feedback control loop, which ensures that till the desired state is attained, the system keeps on actuating and sensing.
- Humans have a simple supervisory role in CPS-based systems, and most of the ground-level operations are automated.

IoE

- The IoE paradigm is mainly concerned with minimizing and even reversing the ill-effects of permeation of Internet-based technologies on the environment.
- The major focus areas of this paradigm include smart and sustainable farming, sustainable and energy-efficient habitats, enhancing the energy efficiency of systems and processes, and others.
- Summarily, we can safely assume that any aspect of IoT that concerns and affects the environment, falls under the purview of IoE.

Industry 4.0

- Commonly referred to as the fourth industrial revolution pertaining to digitization in the manufacturing industry.
- The previous revolutions chronologically dealt with mechanization, mass production, and the industrial revolution, respectively.
- This paradigm strongly puts forward the concept of smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT.
- The digitization and connectedness in Industry 4.0 translate to better resource and workforce management, optimization of production time and resources, and better upkeep and life-times of the industrial systems.

IoP

- IoP is a new technological movement on the Internet, which aims to decentralize online social interactions, payments, transactions, and other tasks while maintaining confidentiality and privacy of its user's data.
- A famous site for IoP states that as the introduction of the Bitcoin has severely limited the power of banks and governments, the acceptance of IoP will limit the power of corporations, governments, and their spy agencies

IoT versus M2M

1. M2M or the Machine-to-Machine paradigm refers to communications and interactions between various Machines and Devices.
2. M2M collects data from machinery and sensors, while also enabling device management and device interaction. Telecommunication services providers introduced the term M2M, and technically emphasized on machine interactions via one or more communication networks (e.g., 3G, 4G, 5G, satellite, public networks).
3. The scope of IoT is vaster than M2M and comprises a broader range of interactions such as the interactions between devices/things, things, and people, things and applications, and people with applications, M2M enables the amalgamation of workflows comprising of such interactions within IoT.
4. Internet connectivity is central to the IoT theme but is not necessarily focused on the use of telecom networks.

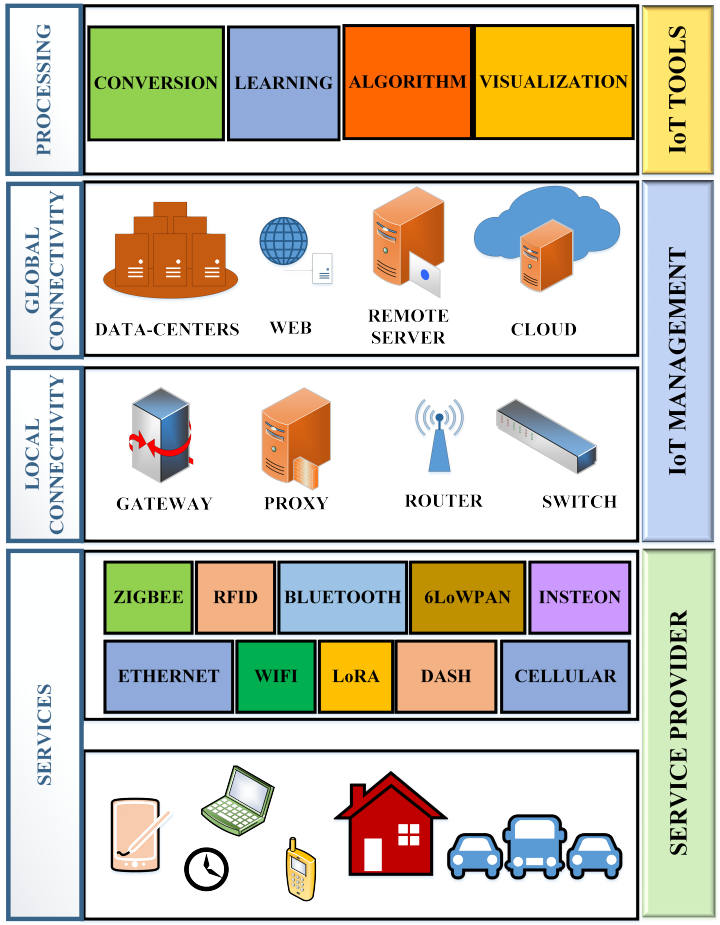
IoT versus CPS

1. Cyber-Physical Systems (CPS) encompasses the sensing, control, actuation, and feedback as a complete package. In other words, a digital twin is attached to a CPS-based system.
2. A digital twin is a virtual system-model relation, in which the system signifies a physical system or equipment or a piece of machinery, the model represents the mathematical model or representation of the physical system's behavior or operation.
3. In contrast, the IoT paradigm does not compulsorily need feedback or a digital twin system. IoT is more focused on networking than controls.
4. Some of the constituent sub-systems in an IoT environment (such as those formed by CPS-based instruments and networks) may include feedback and controls too.

IoT versus WoT

1. From a developer's perspective, the Web of Things (WoT) paradigm enables access and control over IoT resources and applications.
2. These resources and applications are generally built using technologies such as HTML 5.0, JavaScript, Ajax, PHP, and others. REST is one of the key enables or WoT.
3. The use of RESTful principles and RESTful APIs enables both developers and deployers to benefit from the recognition, acceptance, and maturity of existing web technologies, without having to redesign and redeploy solutions from scratch.
4. Technically, WoT can be thought of as an application layer-based hat added over the network layer.
5. However, the scope of IoT applications is much broader, which includes non-IP-based systems that are not accessible through the web.

Enabling IoT - IoT Planes



Enabling IoT - IoT Planes

We divide the IoT paradigm into four planes:

1. services
2. local connectivity
3. global connectivity
4. processing.

If we consider a bottom-up view, the services offered fall under the control and purview of service providers. The service plane is composed of two parts

1. Things or Devices
2. Low-power connectivity.

IoT Networking Components

- An IoT implementation is composed of several components, which may vary with their application domains.
- We outline the broad components, which come into play during the establishment of any IoT network into six types:
  1. IoT Node
  2. IoT Router
  3. IoT LAN
  4. IoT WAN
  5. IoT Gateway
  6. IoT Proxy.

IoT Networking Components

- **IoT Node**: These are the networking devices within an IoT LAN. Each of these devices is typically made up of a sensor, a processor, and a radio, which communicates to the network infrastructure (either within the LAN or outside it). These may be connected to other nodes inside a LAN directly or by means of a common gateway for that LAN. Connections outside the LAN are through gateways and proxies.
- **IoT Router**: An IoT router is a piece of networking equipment, which is primarily tasked with the routing of packets between various entities in the IoT network, and keep the traffic flowing correctly within the network. A router can be repurposed as a gateway by enhancing its functionalities.

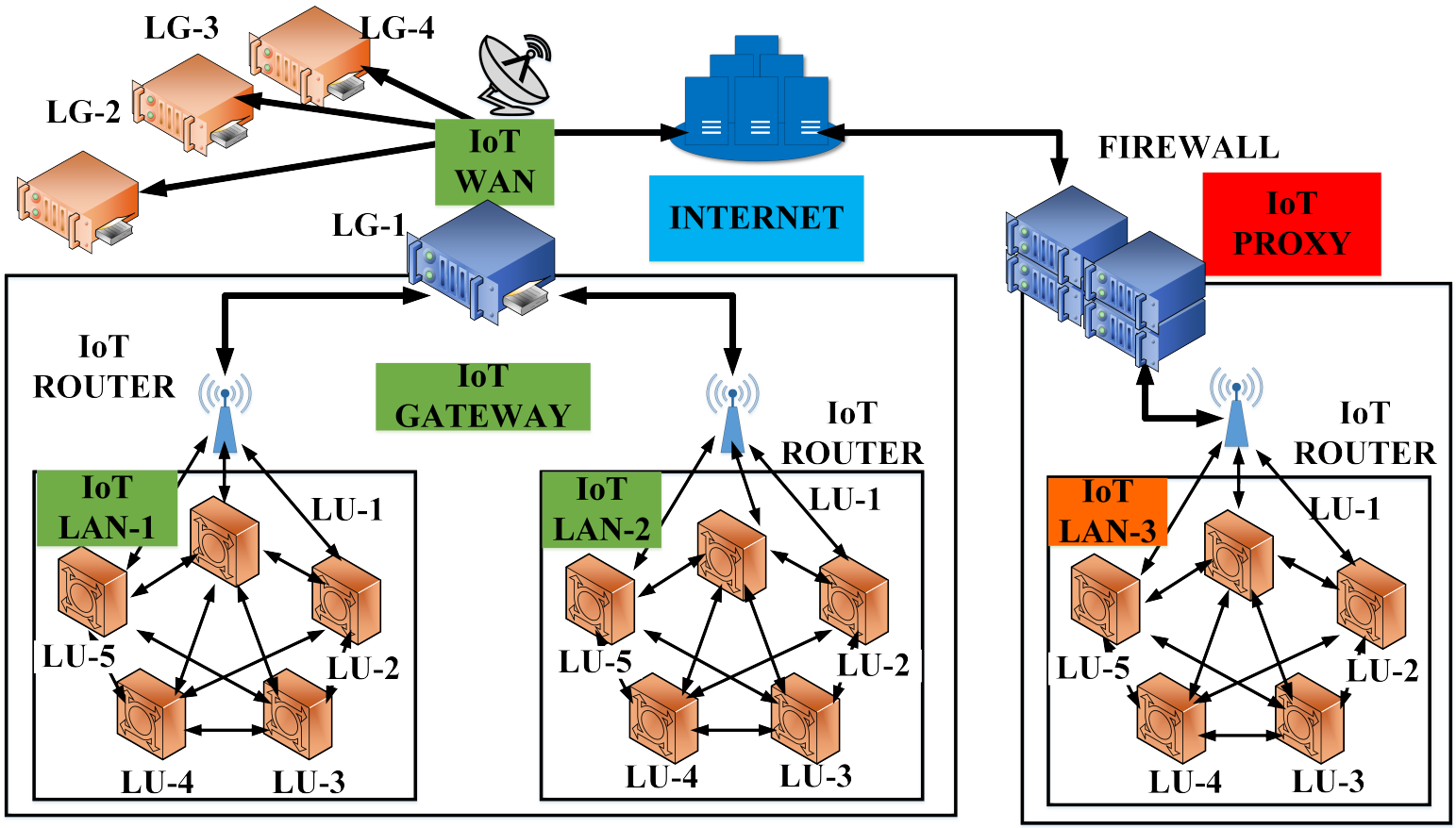
IoT Networking Components

- **IoT LAN**: The Local Area Network (LAN) enables local connectivity within the purview of a single gateway. Typically, they consist of short-range connectivity technologies, and they may or may not be connected to the Internet. Generally, IoT LANs are localized within a building or an organization.
- **IoT WAN**: The Wide Area Network (WAN) connects various network segments such as LANs. These are typically organizationally and geographically wide, with their operational range lying between a few kilometers to hundreds of kilometers. IoT WANs connect to the Internet and enable Internet access to the segments they are connecting.

IoT Networking Components

- **IoT Gateway**: An IoT gateway is simply a router connecting the IoT LAN to a WAN or the Internet. Gateways can implement several LANs and WANs. Their primary task is to forward packets between LANs and WANs, and the IP layer using layer-3 only.
- **IoT Proxy**: Proxies actively lie on the application layer and performs application layer functions between IoT nodes and other entities. Typically application layer proxies are a means of providing security to the network entities under it and enable the extension of the addressing range of its network.

IoT Network Ecosystem



Networking among the Components

- Various IoT nodes within an IoT LAN are configured to talk to one another as well as talk to the IoT router, whenever they are in the range of it.
- The devices have locally unique (LU-x) device identifiers. These identifiers are unique within a LAN only. There is a high chance that these identifiers may be repeated in a new LAN. Each IoT LAN has its own unique identifier.
- A router acts as a connecting link between various LANs by forwarding messages from the LANs to the IoT gateway or the IoT proxy.
- As the proxy is an application layer device, it is additionally possible to include features such as firewalls, packet filters, and other security measures besides the regular routing operations.

Networking among the Components

- Various gateways connect to an IoT WAN, which loften inks these devices to the Internet.
- There may be cases where the gateway or the proxy may directly connect to the Internet.
- An IoT network may be wired or wireless, however, IoT deployments heavily relies on wireless solutions. This is mainly attributed to a large number of devices, which are integrated into the network, and wireless is the only feasible and neat-enough solution to avoid the hassles of laying wires and dealing with restricted mobility rising out of wired connections.

The End