2️⃣

Unit 2 - M2M to IoT - A Market, M2M and IoT Technology Fundamentals

▼ **Syllabus**

- Introduction of M2M: A brief background, M2M communication, A typical M2M solution overview, Key application areas, Trends in information and communications technologies

- M2M to IoT - A Market Perspective, Information marketplaces, Global value chains, IoT value chains

- M2M to IoT - An Architectural Overview, Building an Architecture

- M2M to IoT Technology Fundamentals - Devices and Gateways, Local and Wide Area Networking, Data Management, M2M and IoT Analytics, Knowledge Management

- Architecture Reference Model - IoT Reference Model, Information Model, Functional Model, Communication Model, Safety, Privacy, Trust, Security Model

Introduction to IoT

- IoT is a concept which enables the communication between internetworking devices and applications.

- The physical objects or things communicate through internet.

- The concept of IoT begins with things which can be classified as identity communication devices, e.g., RFID.

> 💡 Internet of Things means a network of physical objects sending, receiving or communication the information using the Internet or other communication technologies.

Hyperconnected Devices

> 💡 Hyper connectivity is the use of multiple systems and devices that are constantly connected to a network with the help of the Internet.

- Example: A network of city lights connected to the main station using sensors and IoT. All the city lights can be controlled through the main station.
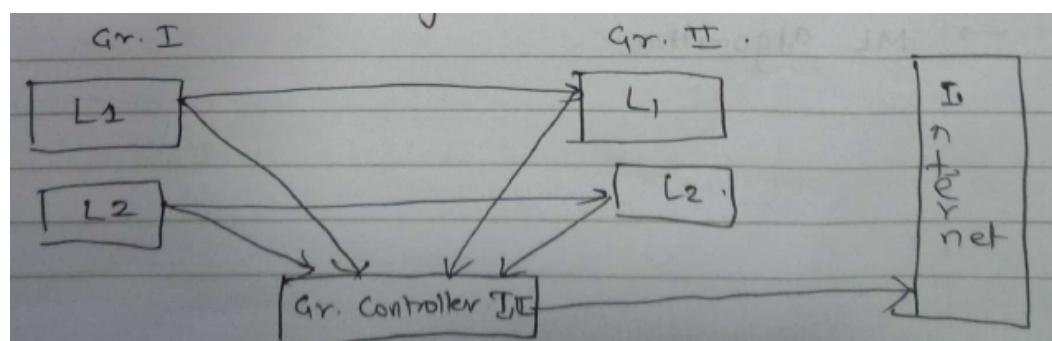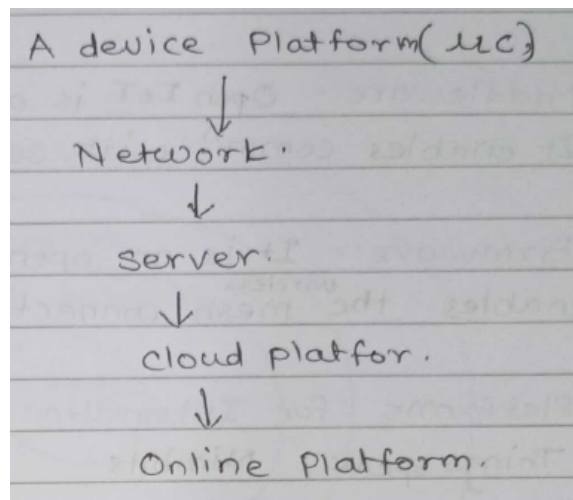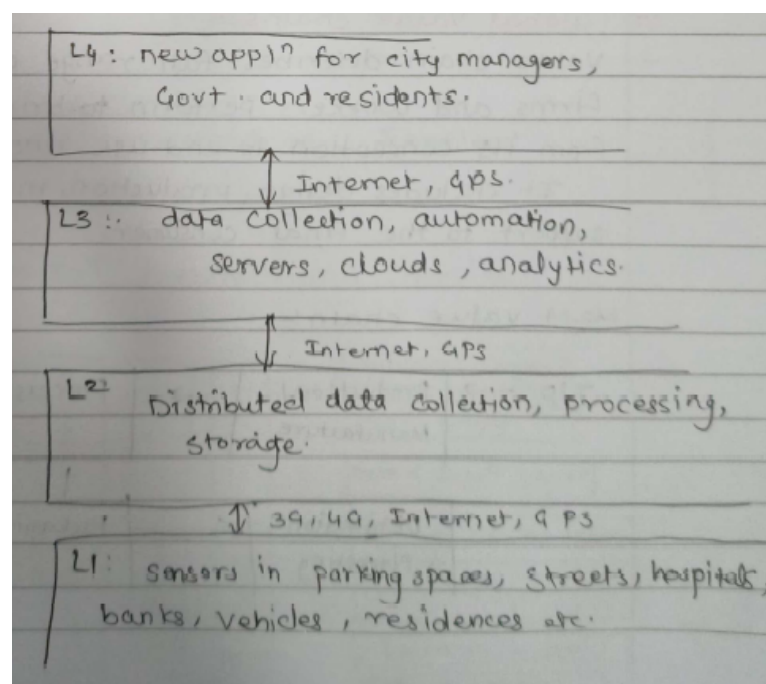

Technology behind IoT

- These entities provide a large and diverse technological environment:
    - Hardware
    - IDE

- Network connection
- Software
- Machine learning algorithms
- **Various Levels in IoT**

A device Platform(μc)
↓
Network.
↓
Server.
↓
Cloud platfor.
↓
Online Platform.

- **E.g. Smart City**

L4: new appln for city managers, Govt. and residents.

↑ Internet, GPS.

L3: data collection, automation, servers, clouds, analytics.

↑ Internet, GPS

L2: Distributed data collection, processing, storage.

↑ 3G, 4G, Internet, GPS

L1: sensors in parking spaces, streets, hospitals, banks, vehicles, residences etc.

Components of IoT Systems

1. **Sensors and Control Units/Modules**

> 💡 Sensors are electronic components used for sensing physical parameters (like temperature, pressure, sound, etc.).

- Each street light has sensors for measuring light intensity and sends that data over a fixed period of time.
- Most commonly used control units are microcontrollers.
- Sensors can be
  1. **Analog**
     - The output of the sensor is some continuous function of its input parameter.
     - E.g. Thermistor, photoconductor, etc.
  2. **Digital**
     - The output of the sensor is in binary nature.
     - Designed to replace analog.
     - Touch sensors, metal sensors, passive IR sensors, etc.
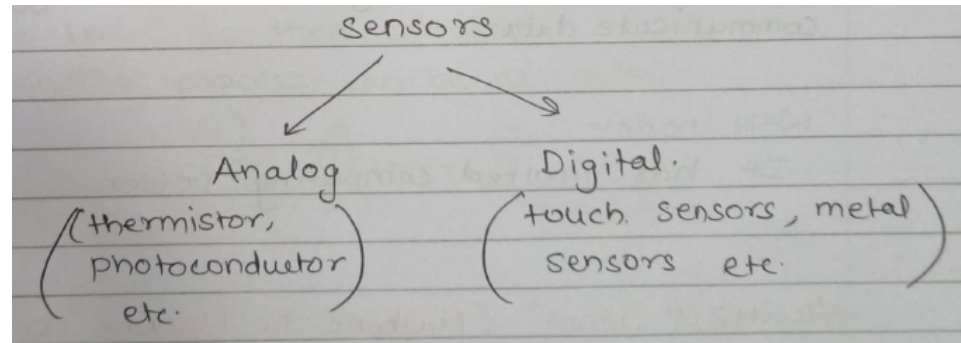
2. **Communication Module**

   - It enables devices to transmit and receive data over some wired/wireless communication network.

   - It consists of protocol handles, message queues, etc.

   - Wired: Ethernet

   - Wireless: Wi-Fi, Bluetooth, ZigBee

3. **Software**

   - **Device Software**

     - Interacts with sensors, communication module and other network components.

     - Collects and processes data before sending it to the backend system.

   - **Server Software**

     - Includes databased, application server, and middleware components.

     - Manages data storage, access control, authentication, and most importantly, data processing tasks.

4. **Middleware**

   - It is responsible for communication between sensor and cloud.

   - It acts as a bridge between IoT devices and backend systems.

   - Handles normalization, protocol translation, device management and security enforcement.

   - Example: OpenIoT, FiWare

5. **Firmware**

   - It is an open source technology.

   - It enables wireless mesh connecvtivity.

Platforms for Integration

   - Thingspeak

   - Nimbits

Sources for IoT

   - Arduino Uno

   - Microduino

   - Intel Galileo

   - Intel Edison

   - Beagle Board

   - Raspberry Pi

Wireless Sensor Network

> 💡 It is a network in which each sensor node connects wirelessly with the ability to compute, aggregate and communicate data over it.

   - WSN node has limited computing power.

M2M Communication

💡 Machine-to-Machine Communication refers to the direct communication between devices or machines without human intervention.

💡 M2M refers to those solutions that allow communication between devices of the same type and a specific application, all via wired/wireless communication networks.

- M2M allows end-users to capture data about events from assets (temperature, inventory levels).
- It is an important and basic block in IoT.
- Automated Interaction: Involves devices communicating autonomously.
- Data Exchange: To coordinate activities, share status updates, or trigger actions.
- Remote Monitoring and Control: Allows operators to monitor and control devices remotely.
- Efficiency: Share information about machine status, performance, resource allocation, etc.
- Wireless Technologies: Cellular networks, Wi-FI, Zigbee, etc.
- **Advantages**
  - Contains large number of nodes
  - Low cost
  - Energy efficient
  - Small traffic per machine/device
- **Overview**
  - Sensors collect data from remote areas
  - Networks are responsible for transportation of data
  - The required/necessary information is then extracted from the data
  - Then the process is activated using that information
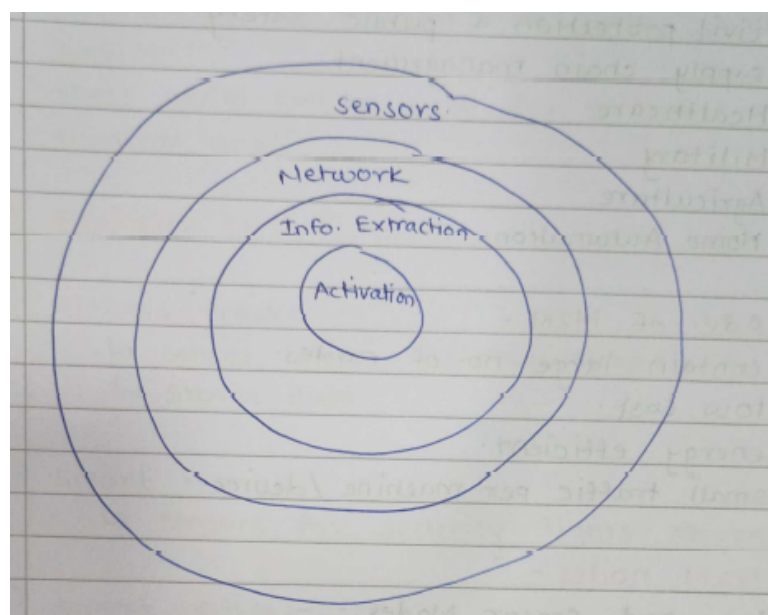
  - Example of M2M communication
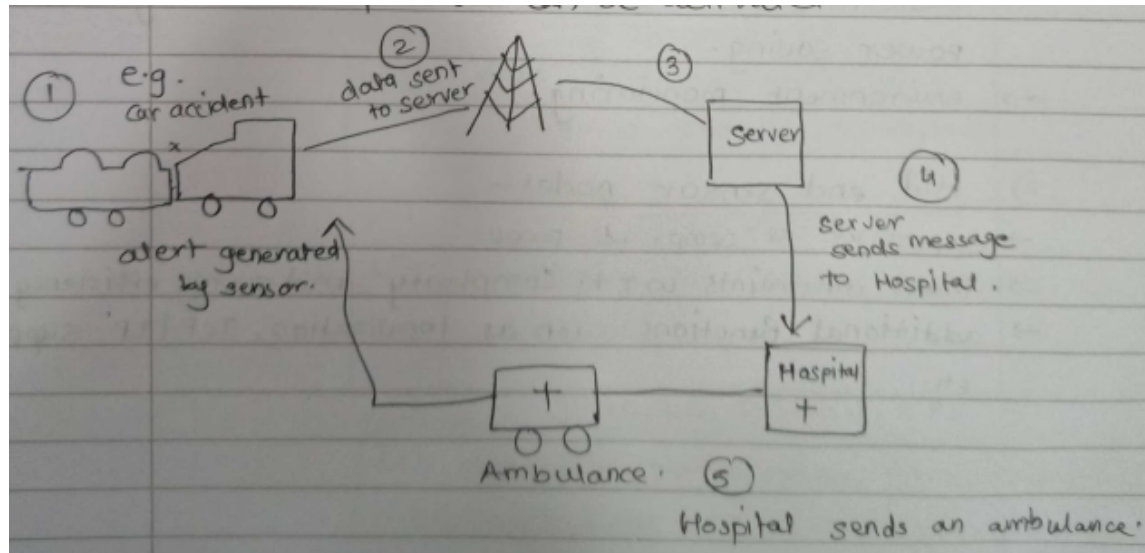
M2M Key Application Areas

- **Smart Cities**

  Used for intelligent infrastructure management, which includes

  - smart traffic lights

  - waste management

  - public transportation systems

  - environmental monitoring

- **Environmental Monitoring**

  - Air quality monitoring (AQI)

  - Water quality management

  - Weather forecasting

- **Healthcare**

  Plays crucial role in healthcare, allows professionals to monitor patient health remotely.

  - Remote patient monitoring

  - Wearable health devices

  - Telemedicine systems

- **Agriculture**

  - This data helps farmers optimize irrigation, fertilization, and other farming practices.

  - Real time-monitoring of soil conditions, weather patterns, crop health.

- **Home Automation**

  Allows smart-home devices to communication and be controlled remotely.

  - Thermostats

  - Security cameras

  - Lighting systems

  - Automated appliances

- **Supply chain management**

  - Connection and coordination of machines, sensors, and control systems.

  - Optimizes production processes, maintenance, and overall operational efficiency.

- Civil protection and public safety

- Military

Trends in ICTs

1. **5G**
   - Enables faster and more reliable wireless communication
   - Supports higher data speeds, low latency, and increased connectivity for a wide range of devices.

2. **Edge Computing**
   - Brings processing capabilities closer to the data source, reducing latency and improving efficiency.
   - Crucial for applications requiring real-time data processing (IoT devices, smart sensors).

3. **IoT**
   - Involves connecting and integrating various devices, sensors, and everyday objects to the internet.
   - Drives the creation of smart homes, cities, industries, and healthcare systems.

4. **AI/ML**
   - Provide capabilities such as NLP, image recognition, predictive analysis and automation across industries.

5. **AR/VR**
   - Provide immersive and interactive experiences.
   - Transforming industries such as gaming, healthcare, education and manufacturing.

6. **Blockchain**
   - Known for its role in cryptocurrencies
   - Offers decentralized and secure solutions
   - Supply chain, healthcare, identity verification

7. **Quantum Computing**
   - Explores potential of quantum mechanics
   - Perform complex computations at a much faster rate than classical computers

M2M Nodes

- **Low End Sensor Nodes**
  - Cheaper
  - Low-range data-transfer capabilities
  - Basic functions like data collection, auto configuration, power saving
  - e.g. Environment monitoring

- **Mid End Sensor Nodes**
  - More expensive than low-end sensor nodes
  - Fewer constraints with respect to complexity and energy efficiency
  - Additional functions such as localization, TCP/IP support.
  - e.g. Energy meters

- **High End Sensor Nodes**
  - Can handle multimedia with quality of service
  - Highest cost
  - Can be used for military and biomedical applications

Information Marketplaces

- Data can be shared between companies and value chains in internal information marketplaces.
- Alternatively, data could be publicly exchanged on a public information marketplace.
- These marketplaces are based on the exchange of data in order to create information products.
- **AWS IoT Marketplace**: Provides a platform for discovering, purchasing, and deploying IoT applications and devices.
- **Azure IoT Marketplace**: Offers a variety of pre-built solutions, services, and devices for IoT development.
- **IBM Watson IoT Marketplace**: Facilitates the discovery and integration of IoT solutions into projects.
- **Google Cloud IoT Marketplace**: Provides a platform for discovering and deploying IoT technologies.
- **Cisco IoT Marketplace**: Platform for Cisco IoT solutions and services, accelerating IoT deployments with software, hardware, and consulting.
- **IoTize Market**: Focused on connectivity solutions for IoT
- **IoTSense Marketplace**: Provides a marketplace for developers and businesses.
- **Thingiverse**: Platform focused on 3D printing, where users can find and share IoT-related designs and models.

Global Value Chains

> 💡 Value chain describes full range of activities that industries (or firms and workers) perform to bring a product from its conception to end-use and beyond.

1. **Design**
   - Involves conceptualizing and developing products or services
   - Based on market needs, consumer preferences, and technological advancements
2. **Production**
   - Encompasses manufacturing processes and operations for transforming raw materials or components into finished goods or intermediate products.
3. **Marketing**
   - Focuses on promoting and selling products or services to target markets and consumers.
4. **Distribution**
   - Involves the movement and logistics of goods or services from production facilities to distribution channels, retailers, and the end user.
5. **Support to the Consumer**
   - Focuses on providing after-sales services, customer support, and assistance to ensure customer satisfaction and loyalty.
   - Product installation and training
   - Tech support
   - Repair and maintenance

M2M Value Chains

> 💡 M2M Value Chains are specific type of value chain within the broader concept of GVCs.

- Internal to one company and cover one solution.

Input → Production → Processing → Packaging → Distribution/Marketing

1. **Inputs**

- Base raw ingredients that are turned into a product.
- Example: cocoa beans for the manufacture of chocolate or data from an M2M device that will be turned into a piece of information.

2. **Production/Manufacture**

- The process that the raw inputs are put through to become part of a value chain.
- Example: cocoa beans may be dried and separated before being transported to overseas markets, or Data from an M2M solution needs to be verified and tagged.

3. **Processing**

- The process whereby a product is prepared for sale.
- Example: cocoa beans may now be made into cocoa powder, ready for use in chocolate bars Or for an M2M solution, the aggregation of multiple data sources to create an information component.

4. **Packaging**

- The process whereby a product can be branded as would be recognizable to end-user consumers.
- Example: the chocolate bar would now be ready to eat and have a red wrapper with the words "KitKat" on it. For M2M solutions, the data will have to be combined with other information from internal corporate databases.

5. **Distribution/Marketing**

- The channels to market for products.
- Example: the chocolate bar may be sold at a supermarket, a kiosk, or even online. An M2M solution, however, will have produced an Information Product that can be used to create new knowledge within a corporate environment.

IoT Value Chains
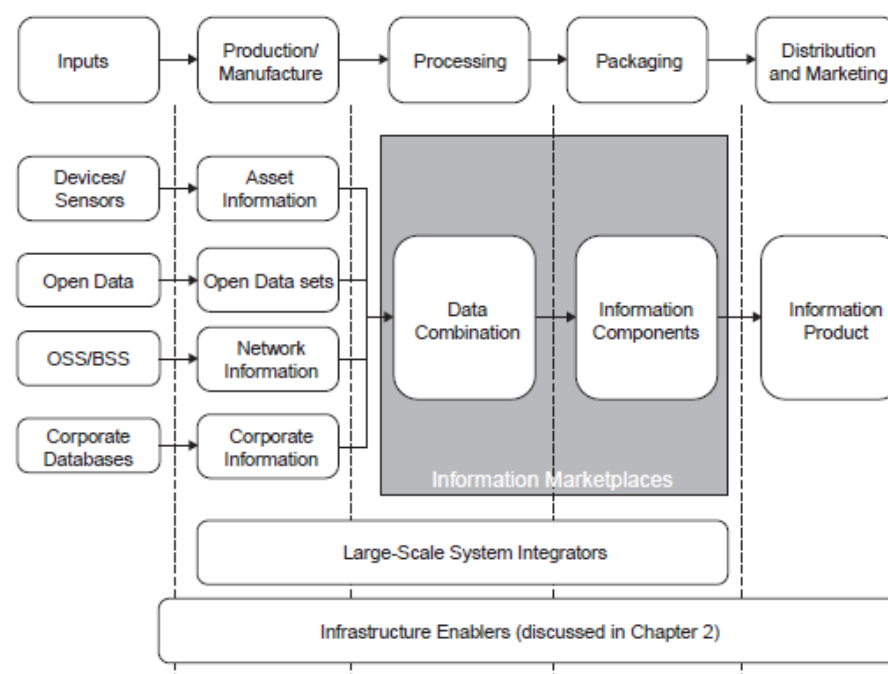
1. **Inputs**

- Significantly more inputs than for an M2M solution.
- Devices/Sensors: Data from these devices and sensors is used provides a different and much broader marketplace than M2M does.
- Open Data: Data provided by government and city organizations, like city maps.
- OSS/BSS (Operational and Business Support Systems): OSS/BSS of mobile operator networks are being used in information marketplaces
- Corporate Databases: Companies of a certain size generally have multiple corporate databases covering various functions.

2. **Production/Manufacture**

- The raw inputs described above will undergo initial development into information components and products.

- Asset Information: This data relates to whatever the sensor/device has been developed to monitor.

- Open Data Sets: May include maps, rail timetables, or demographics (about a certain area)

- Network Information: Information such as GPS data, services accessed via mobile network.

- Corporate Information: Information like the current state of demand for a particular product.

3. **Processing**

- The data from the various inputs from the production and manufacture stage are combined together to create information.

- Extensive use of data analytics.

4. **Packaging**

- Creates information components, which could be produced as charts or other traditional methods of communicating information to end-users.

5. **Distribution and Marketing**

- Final stage in creation of an Information Product.

- Two categories of Information Products

  1. For improving internal decision-making

  2. For resale to other economic actors

M2M to IoT - Architectural Overview
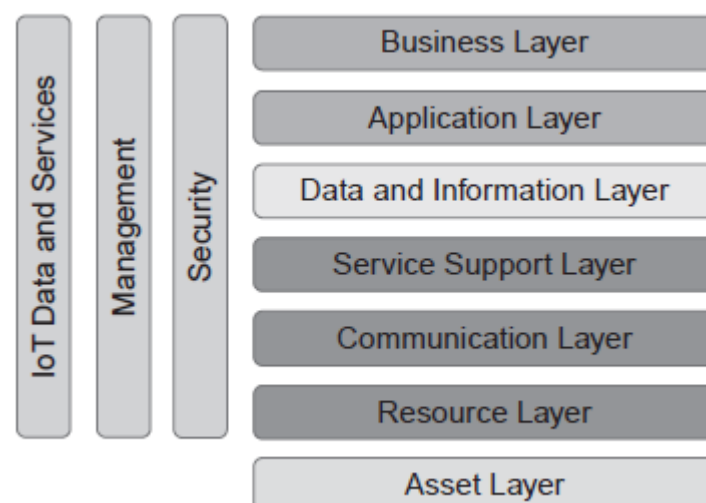
1. **Asset Layer**

- At the lowest level is the Asset Layer.

- Consists of real world objects and entities that are subject to being monitored and controlled, as well as having digital representation and identities.

- Assets are instrumented with embedded technologies that bridge the digital realm with the physical world.

- e.g. Homes, vehicles, machinery, buildings, etc.

2. **Resource Layer**

- Provides the main functional capabilities of sensing, actuation, and embedded identities.

- Gateways of different types are placed that can provide aggregation or other capabilities.

3. **Communication Layer**

- Provides means for connectivity between the resources on one end and different computing infrastructures on the other.

- These computing infrastructures host and execute service support and application logic.

Network	Description
LAN (Local Area Network)	Connects devices in close proximity

Network	Description
WAN (Wide Area Network)	Wired and Wireless technologies (public or private), cellular mobile technologies
WPAN (Wireless Personal Area Network)	Fitness and healthcare applications
HAN and BAN (Home and Building Area Network)	Automation and control applications
NAN (Neighborhood Area Network)	Distribution grid of a smart electricity grid
V2V (Vehicle to Vehicle)	Collision avoidance or car platooning
ZigBee	Protocol stack for home automation

4. **Service Support Layer**

- Provides support services

- These support services

    - execute in data centers (or server farm) in a cloud environment.

    - provide uniform handling of underlying devices and networks

- Example: remote device management for remote software updates, diagnostics or recovery

5. **Data and Information Layer**

- Provides a more abstract set of functions

- Main purposes are to capture knowledge and provide control logic support.

- Main focus is on the organization of information.

6. **The Application Layer**

- Provides the specific IoT applications.

- Open ended array of different applications

- Examples: smart meter in Smart Grid, vehicle tracking

7. **Business Layer**

- Focuses on supporting core business operations of any organization

- Where integration of IoT applications into business process and enterprise systems take place.

- Provides exposure to APIs for third parties to get access to data and information

- Support for business process workflow

Parameters for Building M2M to IoT Architecture

Parameter	M2M	IoT
Scalability	Designed for applications with a limited number of devices	Need to accommodate a massive number of devices and scale seamlessly with network growth
Interoperability	Limited: May use proprietary protocols and interface	Emphasizes interoperability across devices and platforms
Data Variety and Complexity	Involves simple, predefined data exchanges between devices	Deals with diverse data types (structured and unstructured)
Communication Protocols	May use specific communication protocols tailored to their application	Leverage standardized protocols such as MQTT, CoAP, HTTP
Security	May focus on securing point-to-point communication	Introduces a broader attack surface, requiring comprehensive security measures
Device Management	Typically simpler, focusing on basic functionalities	More complex tasks, including firmware updates, configuration and lifecycle

Parameter	M2M	IoT
		management
Standardization	May lack standardized approaches	Crucial in IoT to ensure compatibility and collaboration between different ecosystems

Devices in IoT Systems

1. **Basic Devices**

   - Microcontroller class devices, which can perform simple operations

   - Cannot communicate without using gateways

   - Good for simple processes like alarms, metering, etc.

   - Components used are cheap, usually using SoC, at least two microprocessors and wireless connectivity stack.

   - E.g. landline phones, 2-way radio

2. **Advanced Devices**

   - General purpose class devices, which perform application level logic and support communication protocols.

   - Designed for more complex processes like automated units, processing multiple actions at the same time.

   - May also function as a gateway for devices on the same LAN.

   - E.g. wireless router

M2M vs IoT

Parameter for Difference	IoT	M2M
	Internet of Things	Machine-to-Machine
Intelligence	Devices have objects responsible for decision making	Limited intelligence observed
Connection	Via network	Point-to-point
Communication Protocol	Internet protocols (HTTP, FTP, Telnet)	Traditional protocol and communication technologies
Internet	Required for communication	Not dependent on Internet
Business Model	B2B and B2C	B2B
Approach	Horizontal enabler approach	Vertical system solution approach
Components	Devices/Sensors Connectivity Data Processing UI	Device Area Networks Gateway Application Server
Deployment	Cloud	In-house
Examples	Smart wearables, home automation	Telemetry, environmental monitoring

IoT Gateways

💡 IoT Gateways act as a bridge between different communication technologies.

- Acts as a medium to establish connection between the cloud and controller in IoT.

- Developer-to-developer, or developer-to-cloud communication can be established using gateways.
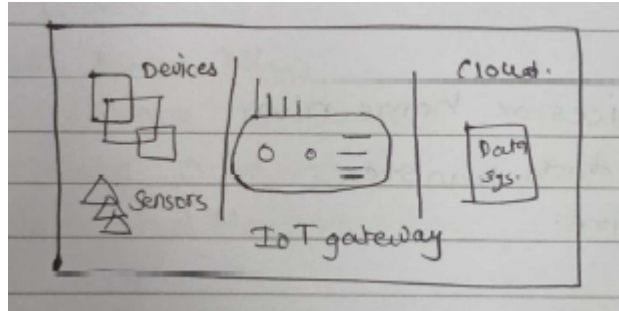
- **Functions**

  1. Protocol Translation: Translate data between different communication protocols.

  2. Data Aggregation: Collect and aggregate data, preparing them for further processing or transmission.

  3. Local Processing: To extract insights, or execute predefined algorithms.

  4. Data Filtering: Based on predefined criteria, rules, or thresholds to discard redundant data.

  5. Local Data Storage: Temporarily cache or buffer incoming data before transmission.

  6. Autonomous Development Control: Execute predefined scripts, rules, or workflows (server-independent)

  7. Device Security: Implement security controls like encryption and authentication to ensure CIA.

- **Working**

  1. Receive data from sensor network

  2. Perform preprocessing, filtering, and cleaning on unfiltered data

  3. Transports it into standard protocol for communication

  4. Send data to cloud

- **Advantages**

  - Reliable (fault tolerance and remote management)

  - Scalable (modular architecture and distributed processing)

  - Cost-effective

LAN and WAN in IoT

LAN

- Group of network devices that allow communication between those connected devices.

- Advantages

  - Reliable and secure

  - No need for Internet communication

- Wired LAN

  - Used in offices or home networks

  - High speed data transfer

  - Fast and secure

- Wi-Fi

  - Uses radio waves to connect devices

  - Used in homes, shops, public spaces

  - Convenient and easy to use

  - Flexible, suitable for mobile phones

- ZigBee

  - Low-power, low-data rate

- Used in home automation and sensor networks

  - Reliable

WAN

- Connected collection of telecommunication networks.

- Switched WAN

  - Multiple components of LANs connected via shared network infrastructure

  - Best suited for distributed environments

- Point-to-Point WAN

  - Two LAN nodes are connected via a leased line

LAN vs WAN

LAN	WAN
Local Area Network	Wide Area Network
Ownership is private	Ownership is private/public
Higher speed than WAN	Lower speed than LAN
Propagation delay is short	Propagation delay is long
Easy design and maintenance	Difficult design and maintenance
Covers small area	Covers large geographical area
Principle of broadcasting	Principle of Point-to-Point
High data transfer rate	Low data transfer rate
Ethernet, Token Ring	Frame Relay, X.25
Low setup cost	High setup cost
e.g. computer lab	e.g. pager/beeper

M2M to IoT Analytics

> 💡 The process of analyzing data generated by connected devices to derive meaningful insights and drive informed decision-making.

1. Data Collection

2. Data Integration

3. Data Preprocessing

4. Data Analysis

5. Visualization and Reporting

6. Real-time Analytics

7. Predictive Analysis

8. Continuous Improvement

Data Management (Page 107)

- Effective data management is crucial for handling the vast amount of data generated by connected devices efficiently and securely.

- Needed for data governance, as massive volumes of data are generated.

- **Need of Data Management**

- Product Development: Error detection, performance analysis, offer product insights

- Prediction of Wear and Tear: Equipment lifecycles, make maintenance plans

- Facilitate Resource and System Efficiency

- **Methods**

    1. **Data Generation:** First stage within which data is generated actively or passively from the device, system, or as a result of its interactions.

    2. **Data Acquisition:** Deals with the collection of data (actively or passively) from the device, system, or as a result of its interactions.

    3. **Data Validation:** Data acquired must be checked for correctness and meaningfulness within the specific operating context.

    4. **Data Storage:** Specialized technologies such as massively parallel processing DBs, distributed file systems, cloud computing platforms, etc. are needed.

    5. **Data Processing:** Main goal is to operate on the data at a low level and enhance it for future needs.

    6. **Data Remanence:** Prevention of data remanence using overwriting, degaussing, encryption, and physical destruction.

    7. **Data Analysis:** The data is subjected to analysis with the aim to obtain the information they encapsulate and use it for supporting decision-making processes.

Knowledge Management

> 💡 Involves the systematic process of capturing, organizing, sharing, and leveraging knowledge and insights derived from connected devices and systems.

1. **Data Capture**: Sensor readings, device statuses, environmental conditions, user interactions.

2. **Data Organization**: Categorizing data based on attributes such as type, source, time, location.

3. **Data Sharing and Collaboration**: Establishing platforms, tools, and processes for sharing data, analyses, best practices, and lessons learned.

4. **Knowledge Discovery and Analysis**: Data mining, AI/ML are employed to uncover patterns, trends, correlations within the data.

5. **Knowledge Repositories**: House structured and unstructured data, analyses, reports, documentation

6. **Continuous Learning and Improvement**: Capture feedback, lessons learned, and insights from past experiences.

7. **Security and Governance**: Implementing robust security measures, access controls, encryption, and compliance with data privacy regulations.

IoT Reference Model

- Application Layer

    - Interacts with end-user, access and control, IoT development

- Data Processing Layer

    - Software/hardware components responsible for collecting, analyzing and interpreting data.

- Network Layer

    - Responsible for providing communication and connectivity

    - Wi-Fi, Bluetooth, Zigbee, 4G, 5G

- Sensing Layer

    - Collect data from different sources

- ○ Sensors/actuators
- ○ Connected to network layer through wired/wireless communication protocols
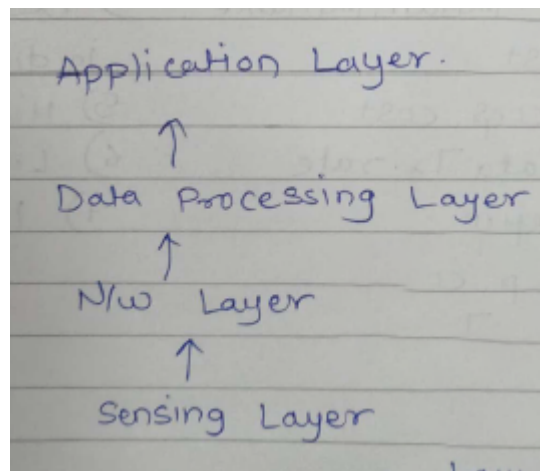
IoT Information Model

- On a high-level, the IoT Information Model maintains the necessary information about Virtual Entities and their properties or attributes.

- The IoT Information Model describes Virtual Entities and their attributes, including metadata.

- Associations between Virtual Entities and their Services are explicitly captured in the Information Model.

- Attributes can be associated with sensor services or actuation services, depending on whether they involve reading sensors or controlling actuators.
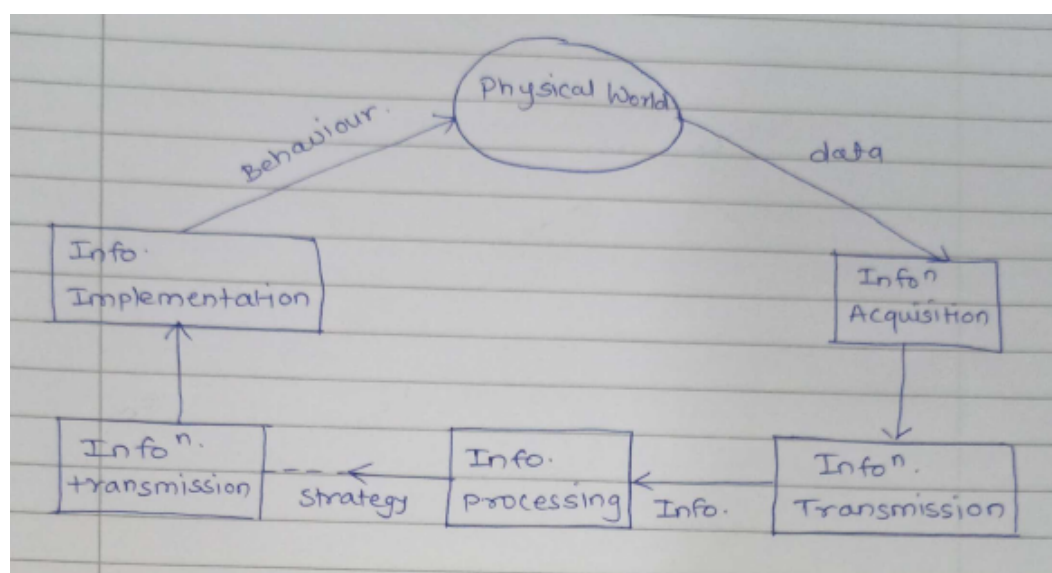
IoT Communication Model

- The communication model involves identifying interaction endpoints, traffic patterns, and underlying technology properties.

- Potential endpoints include Users, Resources, and Devices.

- Gateways bridge different communication technologies for interactions involving constrained Devices.