Module 2

Q1. What is M2M communication?

- M2M stands for Machine-to-Machine communication, and it refers to the direct communication between devices or machines without human intervention.
- **Automated Interaction:** M2M communication involves devices communicating autonomously, without requiring human input or control.
- **Data Exchange:** Devices in M2M communication systems exchange data, information, or instructions to coordinate activities, share status updates, or trigger actions.
- **Remote Monitoring and Control:** M2M enables remote monitoring and control of devices and systems. For example, sensors in a smart grid can send real-time data to a central control system, allowing operators to monitor and control energy distribution remotely.
- **Efficiency and Optimization**: M2M communication is often used to improve efficiency and optimize processes. Machines can share information about their status, performance, or environmental conditions, allowing for better decision-making and resource allocation.
- **Applications across Industries:** M2M communication is widely utilized across various industries, including healthcare, agriculture, transportation, manufacturing, and smart cities. Examples include smart meters in utilities, telemetry systems in healthcare, and tracking systems in logistics.
- **Wireless Technologies**: M2M communication often relies on wireless technologies such as cellular networks, Wi-Fi, Zigbee, or other IoT (Internet of Things) protocols.

*** diagram in copy

Q2. List the key application areas of M2M communication.

They are:-

- **Smart Cities:**
  - M2M communication is used in smart city initiatives for intelligent infrastructure management, including smart traffic lights, waste management, public transportation systems, and environmental monitoring.
- **Industrial IoT (IIoT):**

    - M2M communication enables the connection and coordination of machines, sensors, and control systems for optimized production processes, maintenance, and overall operational efficiency.
- **Healthcare and Telemedicine:**
    - M2M communication plays a crucial role in healthcare applications such as remote patient monitoring, wearable health devices, and telemedicine systems, allowing healthcare professionals to monitor patient health remotely.
- **Agriculture:**
    - Agriculture utilizes M2M communication for real-time monitoring of soil conditions, weather patterns, and crop health. This data helps farmers optimize irrigation, fertilization, and other farming practices.
- **Smart Home Automation:**
    - M2M communication is used in smart home systems, allowing devices such as thermostats, security cameras, lighting systems, and appliances to communicate and be controlled remotely.
- **Environmental Monitoring:**
    - M2M communication is employed for environmental monitoring applications, including air quality monitoring, water quality management, and weather forecasting.
- **Banking and Financial Services:**
    - M2M communication is applied in banking and financial services for secure and efficient transactions, ATM monitoring, and fraud detection.

Q3. What are the various trends in information and communication technologies?

1. **5G Technology:**
    - The rollout and adoption of 5G networks enable faster and more reliable wireless communication, supporting higher data speeds, low latency, and increased connectivity for a wide range of devices.
2. **Edge Computing:**
    - Edge computing brings processing capabilities closer to the data source, reducing latency and improving efficiency. This trend is especially crucial for applications requiring real-time data processing, such as IoT devices and smart sensors.
3. **Internet of Things (IoT):**

- IoT involves connecting and integrating various devices, sensors, and everyday objects to the internet. This trend drives the creation of smart homes, cities, industries, and healthcare systems.

4. **Artificial Intelligence (AI) and Machine Learning (ML):**
   - AI and ML technologies are increasingly integrated into various applications, providing capabilities such as natural language processing, image recognition, predictive analytics, and automation across industries.
5. **Augmented Reality (AR) and Virtual Reality (VR):**
   - AR and VR technologies are transforming industries such as gaming, healthcare, education, and manufacturing by providing immersive and interactive experiences.
6. **Blockchain Technology:**
   - Blockchain, known for its role in cryptocurrencies, is finding applications beyond finance. It offers decentralized and secure solutions for various sectors, including supply chain, healthcare, and identity verification.
7. **Quantum Computing:**
   - Quantum computing explores the potential of quantum mechanics to perform complex computations at a much faster rate than classical computers.

Q4. List various market places for IOT.

1. **AWS IoT Marketplace (Amazon Web Services):**
   - AWS IoT Marketplace offers a wide range of IoT solutions, including software, hardware, and services. It provides a platform for discovering, purchasing, and deploying IoT applications and devices.
2. **Azure IoT Marketplace (Microsoft Azure):**
   - Azure IoT Marketplace is part of Microsoft's Azure platform, offering a variety of pre-built solutions, services, and devices for IoT development. It enables users to find, test, and deploy IoT solutions seamlessly.
3. **IBM Watson IoT Marketplace:**
   - IBM Watson IoT Marketplace provides a collection of IoT applications, services, and assets built on IBM's Watson IoT platform. It facilitates the discovery and integration of IoT solutions into projects.
4. **Google Cloud IoT Marketplace:**
   - Google Cloud IoT Marketplace is part of the Google Cloud ecosystem, offering a selection of IoT solutions, applications, and services. It provides a platform for discovering and deploying IoT technologies.
5. **IoTize Market:**

- IoTize Market is a platform focused on connectivity solutions for the Internet of Things. It includes products and tools for integrating connectivity into existing devices and applications.

6. **IoTSense Marketplace:**
   - IoTSense Marketplace offers a range of IoT solutions, applications, and devices. It is part of the IoTSense IoT platform, providing a marketplace for developers and businesses.
7. **Thingiverse:**
   - Thingiverse is a platform focused on 3D printing, where users can find and share IoT-related designs and models. It's a community-driven marketplace for physical IoT components.

Q5. Describe global value chain in detail.

The global value chain describes the full range of activities that firms and workers perform to bring a product from its conception to end use and beyond.
It includes:

1. **Design:**
   - The design stage involves conceptualizing and developing products or services based on market needs, consumer preferences, and technological advancements.
2. **Production:**
   - The production stage encompasses manufacturing processes and operations for transforming raw materials or components into finished goods or intermediate products.
3. **Marketing:**
   - The marketing stage focuses on promoting and selling products or services to target markets and consumers.
4. **Distribution:**
   - The distribution stage involves the movement and logistics of goods or services from production facilities to distribution channels, retailers, and ultimately to end consumers.
5. **Support to the Consumer:**
   - The support stage focuses on providing after-sales services, customer support, and assistance to ensure customer satisfaction and loyalty. Support activities may include product installation, training, technical support, warranty services, repair and maintenance, and customer feedback management.

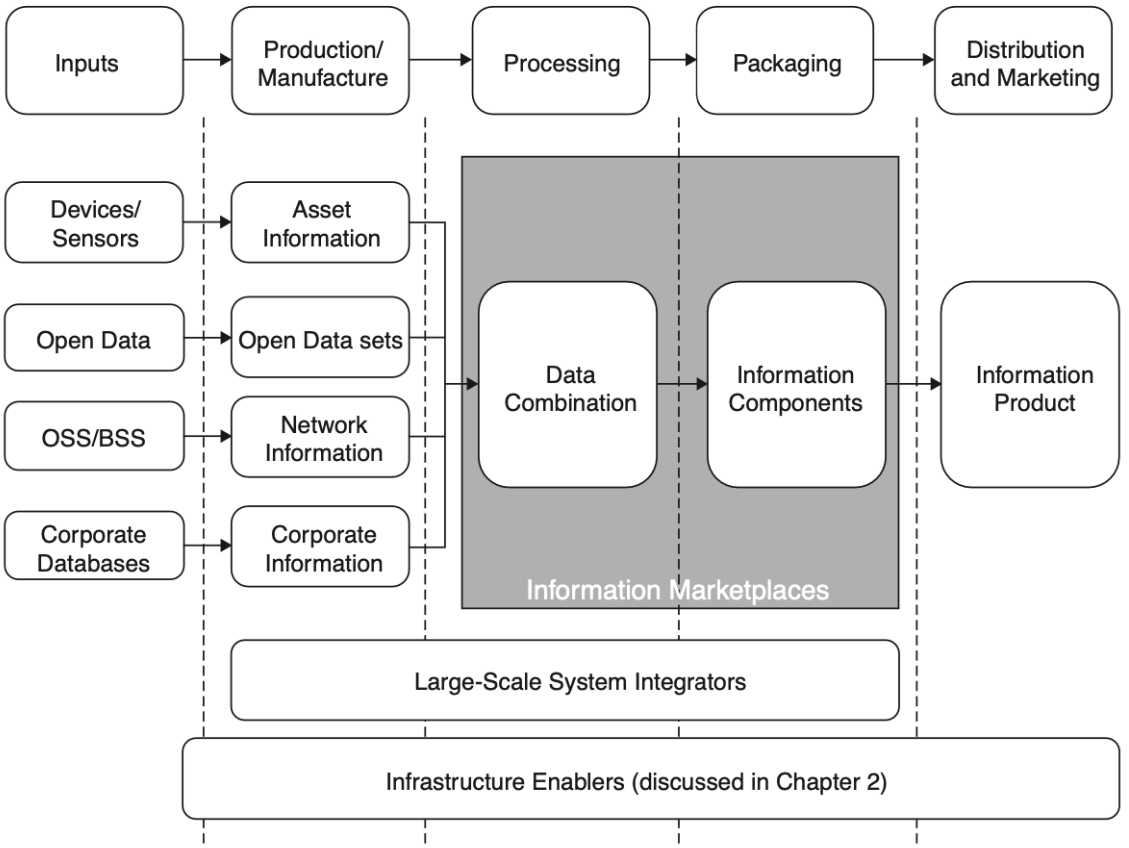
Q6. Explain M2M value chains.

M2M Value chain are specific type of value chain within the broader concept of global value chains(GVCs).
M2M value chains are internal to one company and cover one solution.
The inputs and outputs of an M2M value chain:

1. **Inputs:** Inputs are the base raw ingredients that are turned into a product. Examples could be 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:** Refers to the process that the raw inputs are put through to become part of a value chain. For example, cocoa beans may be dried and separated before being transported to overseas markets. Data from an M2M solution, meanwhile, needs to be verified and tagged for provenance.
3. **Processing:** Processing refers to the process whereby a product is prepared for sale. For example, cocoa beans may now be made into cocoa powder, ready for use in chocolate bars. For an M2M solution, this refers to the aggregation of multiple data sources to create an information component that is ready to be combined with other data sets to make it useful for corporate decision-making.
4. **Packaging**: Packaging refers to the process whereby a product can be branded as would be recognizable to end-user consumers. For example, a chocolate bar would now be ready to eat and wrapped in a brand name. For M2M solutions, the data will have to be combined with other information from internal corporate databases.
5. **Distribution/Marketing:** This process refers to the channels to market for products. For example, a 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.

Q7. Explain IoT value chains.

IoT Value Chains, meanwhile, are about the use and reuse of data across value chains and across solutions.



- **Inputs:**
  1. **Device/Sensors:** comprises of the sensors, actuators, microcontrollers, gateways that collect data
  2. **Open Data:** data provided by government and city organizations such as city maps
  3. **OSS/BSS:** The Operational Support Systems and Business Support Systems of mobile operator networks
  4. **Corporate databases:** As the use of devices and sensors increases, these databases will be connected to data to create new information sources and new knowledge.
- **Production/Manufacture:** the raw inputs described above will undergo initial development into information components and products.
  1. **Asset Information:** includes data such as temperature over time of container during transit or air quality during a particular month.
  2. **Open Data Sets:** may include maps, rail timetables, or demographics about a certain area in a country or city.
  3. **Network Information:** relates to information such as GPS data, services accessed via the mobile network, etc
  4. **Corporate Information:** for example, the current state of demand for a particular product in the supply chain at a particular moment in time.

- **Processing:** During this stage, the data from the various inputs from the production and manufacture stage are combined together to create information.
- **Packaging:** The packaging section of the information value chain creates information components. These components could be produced as charts or other traditional methods of communicating information to end-users
- **Distribution/Marketing:** This process refers to the channels to market for products.

Q8. What are the parameters considered in building M2M to IoT architechture?

1. Scalability:
    - M2M: M2M solutions are often designed for specific applications with a limited number of devices.
    - IoT: IoT architectures need to accommodate a massive number of devices and scale seamlessly as the network grows.
2. Interoperability:
    - M2M: M2M systems may use proprietary protocols and interfaces, limiting interoperability.
    - IoT: IoT emphasizes standardization and interoperability across devices and platforms.
3. Data Variety and Complexity:
    - M2M: M2M often involves simple, predefined data exchanges between devices.
    - IoT: IoT deals with diverse data types, including structured and unstructured data. The architecture must support complex data analytics, machine learning, and data fusion for valuable insights.
4. Communication Protocols:
    - M2M: M2M systems may use specific communication protocols tailored to their applications.
    - IoT: IoT architectures leverage standardized and widely accepted protocols such as MQTT, CoAP, and HTTP to ensure interoperability and efficient communication.
5. Security:
    - M2M: Security in M2M may focus on securing point-to-point communication.

    - IoT: IoT introduces a broader attack surface, requiring comprehensive security measures for devices, networks, and data. This includes device authentication, encryption, secure APIs, and continuous monitoring.
6. Device Management:
    - M2M: Device management in M2M is typically simpler, with a focus on basic functionalities.
    - IoT: IoT device management involves more complex tasks, including firmware updates, configuration management, and lifecycle management.
7. Standardization:
    - M2M: M2M solutions may lack standardized approaches.
    - IoT: Standardization is crucial in IoT to ensure compatibility and collaboration between different vendors and ecosystems.

Q9. What are the various communication devices?

Communication devices are categorized into basic and advanced devices:

Basic Devices:

- *Basic devices*, *microcontroller-class devices* are those which can perform simple operations
- They usually cannot communicate with each other without gateways.
- Good for performing simple processes like alarms, metering, standalone smart thermostats and others.
- Basic IoT devises usually serve a single operation – measure temperature, wind force or others. The hardware requirements are relatively low for this type of devices.
- The components used for this type of devices are inexpensive, usually using an SoC inside, containing at least two microprocessors, and several wireless connectivity stacks.
- Eg: Two-Way Radios , landline phones etc.

Advanced Devices:

- *Advanced devices or general purpose-class devices* are performing application level logic and support communication protocols.
- Advanced IoT devices are designed for more complex processes, representing automated units, and processing multiple different actions at the same time.
- It’s not unusual for the advanced device to also function as a gateway for local devices on the same LAN.
- Eg : wireless routers, laptops etc.

Q10. Explain communication gateways.

- provides a bridge between different communication technologies
- acts as a medium to establish connection between the cloud and controller in IoT
- using IoT gateway, developer-to-developer or developer-to-cloud communication can be established.

Functions of Gateway:

1. Protocol Translation:
    - A communication gateway translates data between different communication protocols used by IoT devices and backend systems.
2. Data Aggregation:
    - The gateway collects and aggregates data from multiple IoT devices within its local network and prepares them for further processing, analysis, or transmission to the cloud or centralized servers.
3. Local Processing:
    - Communication gateways may perform local processing of data to extract insights, derive actionable information, or execute predefined logic and algorithms.
4. Data Filtering:
    - Gateways filter incoming data streams based on predefined criteria, rules, or thresholds to discard irrelevant or redundant data and prioritize critical information.
5. Local Data Storage:
    - Communication gateways may include local storage capabilities to temporarily cache or buffer incoming data before transmitting it to the cloud or remote servers.
6. Autonomous Development Control:
    - Some communication gateways support autonomous development control capabilities, allowing them to execute predefined scripts, rules, or workflows locally without constant reliance on external servers or cloud services.
7. Provide Device Security:
    - Communication gateways implement security measures to protect IoT devices, data, and communication channels from unauthorized access, tampering, or malicious attacks.

Working:

- Receive data from sensor network

- Perform pre-processing, filtering and cleaning on unfiltered data
- Transports into standard protocols for communication
- send data to cloud

Advantages:

- **Reliable :** due to redundancy, fault tolerance, stable hardware/software, and remote management.
- **Scalable :** They scale through modular architecture, distributed processing, and interoperability.
- **Cost effective**

Q11. Describe local and wide area network.

LAN:

- Local Area Network
- group of network devices that allow communication between connected devices
- they generally have private ownership
- used for enabling communication between devices and other components

Advantages:

- reliable and secure
- no need for internet connection

Types:

1. Ethernet :
    - wired lan
    - used in offices and home network
    - high speed data transfer
    - fast and secure
2. Wi-Fi
    - uses radiowaves to connect devices
    - home, shops, public spaces
    - convenient, easy to use
    - flexible, mobile
3. Zigbee:
    - low-power, low-data rate
    - home automation, sensor network
    - reliable, low power consumption

    - long battery life

WAN:

- Wide Area Network
- connected collection of telecommunicating network
- large geographic area coverage

Types:

1. Switched WAN:
    - multiple components of LAN connected via shared network infrastructure
    - best suited to distributed environments
2. Point to Point WAN:
    - two WAN nodes are connected through a leased line

Q12. Differentiate between local and wide area network.

UPnP- LAN & CoAP- WAN

S.NO	LAN	WAN
1.	LAN stands for Local Area Network.	Whereas WAN stands for Wide Area Network.
2.	LAN's **ownership** is private.	But WAN's ownership can be private or public.
3.	The **speed** of LAN is high(more than WAN).	While the speed of WAN is slower than LAN.
4.	The **propagation delay** is short in LAN.	Whereas the propagation delay in WAN is long(longer than LAN).
7.	LAN's design and maintenance is easy.	While it's design and maintenance is difficult than WAN.
8.	LAN covers small **area** i.e. within the building.	While WAN covers large geographical area.
9.	LAN operates on the **principle** of broadcasting.	While WAN works on the principle of point to point.
10.	LAN has a higher **data transfer rate.**	WAN has a lower data transfer rate as compared to LAN.
11.	LANs technologies used like ethernet and token.	WANs technologies used like Frame Relay and X.25 for connectivity for longer distances.
12.	low **setup cost**	high setup cost
13.	For eg: A computer lab in a college.	For eg: pager

Q13. Discuss the methods of data management

Data management refers to the process of organizing, storing, retrieving, and analyzing data in a systematic and efficient manner to support decision-making, business operations, and strategic initiatives.

Need for data management:

1. Product development:
    - Error detection and performance analysis

Q14. Explain M2M to IoT analytics

Q15. Discuss knowledge management in M2M to IoT technology.

Q16. Describe IoT reference model

notes

Q17. Explain IoT information model

notes

Q18. Explain IoT communication model

notes

Q19. Describe how safety, privacy and security is ensured while modelling IoT

Safety:

1. **Risk Mitigation** : Prevent IoT devices from causing unacceptable risks of injury or physical damage.
2. **Ethical Use :** Consider social behaviour and ethical use of IoT technologies.

Privacy:

1. **Data Minimization :** Collect necessary data only
2. **Anonymization:** Remove personally identifiable information (PII) from data
3. **Consent Management:** Obtain user consent for data collection
4. **Privacy Policies:** Clearly communicate data handling policies
5. **End-to-End Encryption:** Protect data during transmission
6. **User Control:** Allow users to manage their data preferences

Security:

1. **Security by design:** Integrate security measures from the outset. consider secure communication protocols, encryption and authentication.

2. **Device authentication:** Ensure devices authenticate themselves before accessing the network
3. **Access Control:** Limit access to authorized users and roles.

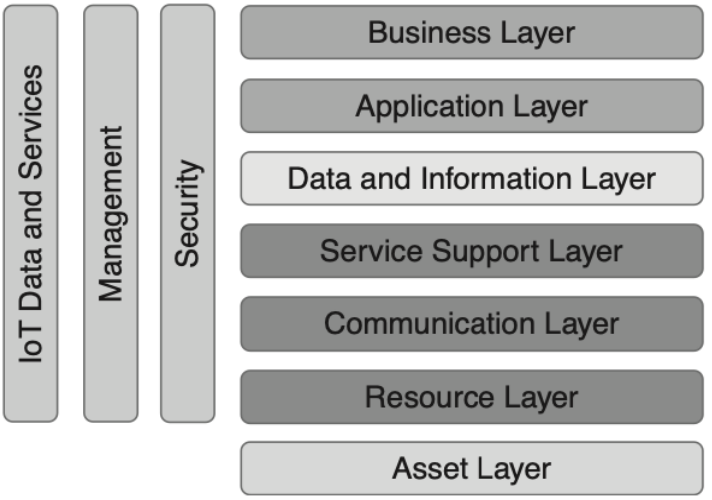
Difference between IoT and M2M

Basis of IoT M2M		
Abbreviation	Internet of Things	Machine to Machine
Intelligence	Devices have objects that are responsible for decision making	In M2M there is limited intelligence observed.
Connection type used	The connection is via Network	The connection is a point to point
Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.	Traditional protocols and communication technology techniques are used
Internet	Internet connection is required for communication	Devices are not dependent on the Internet.
Business Type used	Business 2 Business(B2B) and Business 2 Consumer(B2C)	Only Business 2 Business (B2B)
Approach used	Horizontal enabler approach	Vertical system solution approach .
Components	Devices/sensors, connectivity, data processing, user interface	Device, area networks, gateway, Application server.
Examples	Smart wearables, Big Data and Cloud, etc.	Sensors, Data and Information, etc.

Components of IoT:

1. **Sensors and Control Units:**
    - Sensors are electronic components used for sensing physical parameters such as temp., pressure, audio etc.
    - Eg: Each street light has sensors for measuring light itnensity and sending that data over a fixed period.
    - 2 types:-
        1. Analog: The response or output of the sensor is some continuous function of its input parameter. Ex- Temperature sensor, LDR, analog pressure sensor and analog hall effect.
        2. Digital: Response is in binary nature. Design to overcome the disadvantages of analog sensors. Along with the analog sensor, it also comprises extra electronics for bit conversion. Example – Passive infrared (PIR) sensor and digital temperature sensor(DS1620).
    - Most commonly used control unit is microController
2. **Communication Module:**
    - enables devices to transmit and receive data over various communication netwroks.
    - It may support wired(Eg: Ethernet) or wireless(Eg:Wi-Fi, Bluetooth, Zigbee) connectivity protocols.
3. **Software:**
    - Device Software: interacts with the sensors, communication module and other network components to collect and process data before transmitting it to the backend system.
    - Server Software: includes databases, application servers and middleware components that manage data storage, access control, authentication and data processing tasks.
4. **Middleware:**
    - serves as a bridge between IoT devices and backend systems.
    - handles normalization, protocol translation, device management and security enforcement.
5. **Firmware:**
    - it is an open source technology
    - it enables the wireless mesh technology.

M2M to IoT : an architectural Overview:



1. **Asset Layer:**
    - Consists of real world object and entities that are subject to being monitored and controlled as well as having digital representation and identities.
    - Eg: vehicles, homes, machinery

2. **Resource Layer:**
    - Provides the main functional capabilities of sensing, actuation, and embedded identities.
    - This is also where gateways of different types are placed that can provide aggregation or other capabilities.

3. **Communication Layer:**
    - handles connectivity between the resources on one end and different computing infrastructures on the other.
    -

Network	Descrption
LAN	• Local Area Network • connects devices in close proximity
WAN	• Wide Area Network • wired and wireless technology • public or private
WPAN	• Wireless Personal Area Network • handles fitness and healthcare
HAN & BAN	• Home and Building area network • automation and control applications
NAN	• Neighbourhood Area Network • used in the Distribution Grid of a Smart Electricity Grid
V2V	• Vehicle to Vehicle • collision avoidance
Zigbee	• Protocol stack for home automation

4. **Service Support Layer:**
    - These support services can provide uniform handling of the underlying devices and networks, thus hiding complexities in the communications and resource layers.

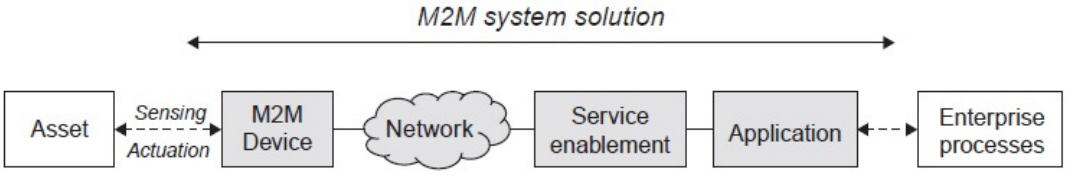
5. **Data and Information Layer:**
    - main purposes are to capture knowledge and provide advanced control logic support.
    - Key concepts here include data and information models and knowledge representation in general, and the focus is on the organization of information.

6. **Application Layer:**
    - provides the specific IoT applications.
    - There is an open-ended array of different applications, and typical examples include smart metering in the Smart Grid, vehicle tracking, building automation, etc.

7. **Business Layer:**
    - focuses on supporting the core business or operations of any enterprise, organization, or individual that is interested in IoT applications
    - integration of the IoT applications into business processes and enterprise systems takes place.

A typical M2M Solution Overview

A typical M2M system solution consists of M2M devices, communication networks that provide remote connectivity for the devices, service enablement and application logic, and integration of the M2M application into the business



1. **M2M Device:** This is the M2M device attached to the asset of interest, and provides sensing and actuation capabilities.

2. **Network:** The purpose of the network is to provide remote connectivity between the M2M device and the application-side servers. Many different network types can be used, and include both Wide Area Networks (WANs) and Local Area Networks (LANs)

3. **M2M Service Enablement:** This component provides a generic functionality that is common among different applications. It's main purpose is to reduce cost for implementation and ease application development.

4. **Application:** The application is integrated into the overall business process system of the enterprise.