IOT UNIT1-1 - depth

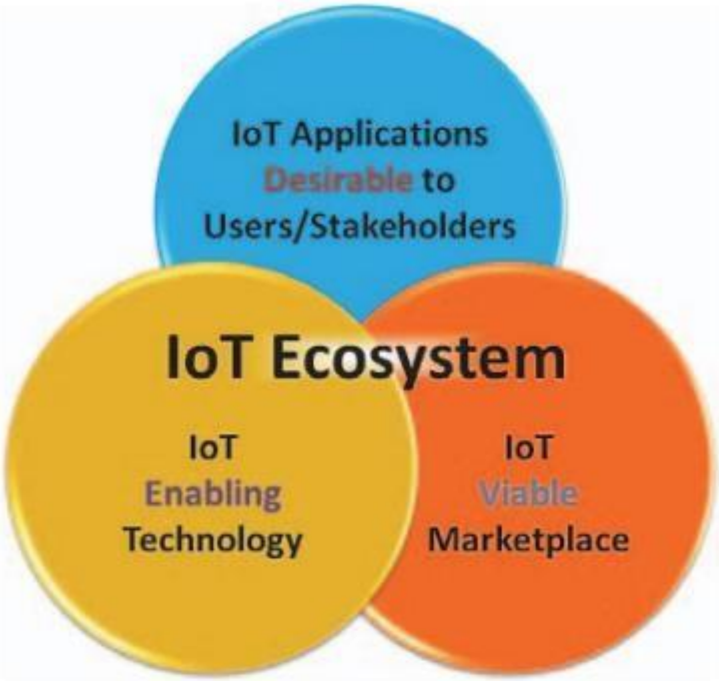
Embedded Systems (Jawaharlal Nehru Technological University, Kakinada)

INTERNET OF THINGS & IT'S APPLICATIONS

UNIT-1

1. INTRODUCTION TO IoT:

- Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways.
- We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web.
- One year after the past edition of the Cluster book 2012 it can be clearly stated that the Internet of Things (IoT) has reached many different players and gained further recognition. Out of the potential Internet of Things application areas, Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem (Figure 1.1) have acquired high attention.



We are entering an era of the "Internet of Things" (abbreviated as IoT). There are 2 definitions:

1. The Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators.
2. Another is the Internet of Things is defined as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object.

- We use these capabilities to query the state of the object and to change its state if possible.
- In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network.
- We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.

- For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers.
- IoT is not a single technology; rather it is an agglomeration of various technologies that work together in tandem.
- Sensors and actuators are devices, which help in interacting with the physical environment.
- The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it.
- Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment).
- An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner.
- The storage and processing of data can be done on the edge of the network itself or in a remote server.
- If any preprocessing of data is possible, then it is typically done at either the sensor or some other proximate device.
- The processed data is then typically sent to a remote server.
- The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to limitations of size, energy, power, and computational capability.
- As a result, the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy.
- Along with the challenges of data collection, and handling, there are challenges in communication as well.
- The communication between IoT devices is mainly wireless because they are generally installed at geographically dispersed locations.
- The wireless channels often have high rates of distortion and are unreliable.
- In this scenario reliably communicating data without too many retransmissions is an important problem and thus communication technologies are integral to the study of IoT devices.
- We can directly modify the physical world through actuators or we may do something virtually. For example, we can send some information to other smart things

1.2 TECHNOLOGIES INVOLVED IN IOT DEVELOPMENT: INTERNET/WEB AND NETWORKING BASICS OSI MODEL

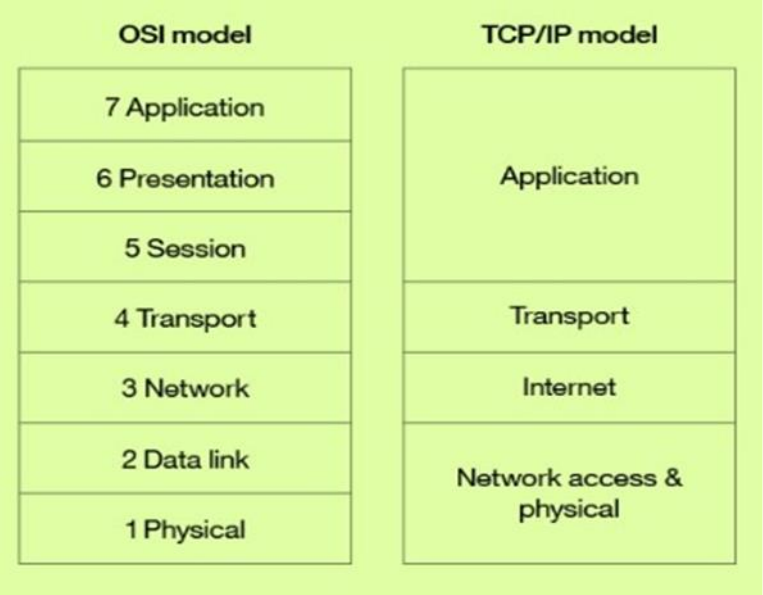
- Networking technologies enable IoT devices to communicate with other devices, applications, and services running in the cloud.
- The internet relies on standardized protocols to ensure communication between heterogeneous devices is secure and reliable.
- Standard protocols specify rules and formats that devices use to establish and manage networks and transmit data across those networks.

- Networks are built as a “stack” of technologies. A technology such as Bluetooth LE is at the bottom of the stack.
- While others such as such as IPv6 technologies (which is responsible for the logical device addressing and routing of network traffic) are further up the stack. Technologies at the top of the stack are used by the applications that are running on top of those layers, such as message queuing technologies.
- This article describes widely adopted technologies and standards for IoT networking. It also provides guidance for choosing one network protocol over another. It then discusses key considerations and challenges related to networking within IoT: range, bandwidth, power usage, intermittent connectivity, interoperability, and security.

NETWORKING STANDARDS AND TECHNOLOGIES:

- The Open Systems Interconnection (OSI) model is an ISO-standard abstract model is a stack of seven protocol layers.

- From the top down, they are: application, presentation, session, transport, network, data link and physical. TCP/IP, or the Internet Protocol suite, underpins the internet, and it provides a simplified concrete implementation of these layers in the OSI model.



OSI model	TCP/IP model
7 Application	Application
6 Presentation	
5 Session	
4 Transport	Transport
3 Network	Internet
2 Data link	Network access & physical
1 Physical	

Figure 1. OSI and TCP/IP networking models

The TCP/IP model includes only four layers, merging some of the OSI model layers:

Network Access & Physical Layer:

This TCP/IP Layer subsumes both OSI layers 1 and 2. The physical (PHY) layer (Layer 1 of OSI) governs how each device is physically connected to the network with hardware, for example with an optic cable, wires, or radio in the case of wireless network like wifi IEEE 802.11 a/b/g/n). At the link layer (Layer 2 of OSI), devices are identified by a MAC address, and protocols at this level are concerned with physical addressing, such as how switches deliver frames to devices on the network.

Internet Layer:

This layer maps to the OSI Layer 3 (network layer). OSI Layer 3 relates to logical addressing. Protocols at this layer define how routers deliver packets of data between source and destination hosts identified by IP addresses. IPv6 is commonly adopted for IoT device addressing.

Transport Layer:

The transport layer (Layer 4 in OSI) focuses on end-to-end communication and provides features such as reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent. UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.

Application Layer:

The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging. HTTP/S is an example of an application layer protocol that is widely adopted across the internet.

IOT NETWORKING CONSIDERATIONS AND CHALLENGES:

When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:

- Range
- Bandwidth
- Power usage
- Intermittent connectivity
- Interoperability
- Security

Range:

Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network:

- PAN(PersonalAreaNetwork) PAN is short-range, where distances can be measured in meters, such as a wearable fitness tracker device that communicates with an app on a cell phone over BLE.

- LAN(LocalAreaNetwork) LAN is short- to medium-range, where distances can be up to hundreds of meters, such as home automation or sensors that are installed within a factory production line that communicate over Wi-Fi with a gateway device that is installed within the same building.

- MAN (Metropolitan Area Network) MAN is long-range (city wide), where distances are measured up to a few kilometres, such as smart parking sensors installed throughout a city that are connected in a mesh network topology.

- WAN (Wide Area Network) WAN is long-range, where distances can be measured in kilometres, such as agricultural sensors that are installed across a large farm or ranch that are used to monitor micro-climate environmental conditions across the property.

Bandwidth

Bandwidth is the amount of data that can be transmitted per unit of time. It limits the rate at which data can be collected from IoT devices and transmitted upstream. Bandwidth is affected by many factors, which include:

- The volume of data each device gathers and transmits

- The number of devices deployed

Whether data is being sent as a constant stream or in intermittent bursts, and if any peak periods are notable the packet size of the networking protocol should match up with the volume of data typically transmitted. It is inefficient to send packets padded with empty data. In contrast, there are overheads in splitting larger chunks of data up across too many small packets. Data transmission rates are not always symmetrical (that is, upload rates might be slower than download rates). So, if there is two-way communication between devices, data transmission needs to be factored in. Wireless and cellular networks are traditionally low bandwidth, so consider whether a wireless technology is the right choice for high-volume applications.

Power usage:

Transmitting data from a device consumes power. Transmitting data over long ranges requires more power than over a short range. You must consider the power source – such as a battery, solar cell, or capacitor – of a device and its total lifecycle. A long and enduring lifecycle will not only provide greater reliability but reduce operating cost. Steps may be taken to help achieve longer power supply lifecycles. For example, to prolong the battery life, you can put the device into sleep mode whenever it is idle. Another best practice is to model the energy consumption of the device under different loads and different network conditions to ensure that the device's power supply and storage capacity matches with the power that is required to transmit the necessary data by using the networking technologies that you adopted.

Intermittent connectivity:

IoT devices aren't always connected. In some cases, devices are designed to connect periodically. However, sometimes an unreliable network might cause devices to drop off due to connectivity issues. Sometimes quality of service issues, such as dealing with interference or channel contention on a wireless network using a shared spectrum. Designs should incorporate intermittent connectivity and seek any available solutions to provide uninterrupted service, should that be a critical factor for IoT landscape design.

Interoperability:

Devices work with other devices, equipment, systems, and technology; they are interoperable. With so many different devices connecting to the IoT, interoperability can be a challenge. Adopting standard protocols has been a traditional approach for maintaining interoperability on the Internet. Standards are agreed upon by industry participants and avoid multiple different designs and directions. With proper standards, and participants who agree to them, incompatibility issues, hence interoperability issues may be avoided.

Security:

Security is a priority. Selection of networking technologies that implement end-to-end security, including authentication, encryption, and open port protection is crucial. IEEE 802.15.4 includes a security model that provides security features that include access control, message integrity, message confidentiality, and replay protection, which are implemented by technologies based on this standard such as ZigBee.

Consider the following factors in shaping a secure and safe IoT network:

- **Authentication**

Adopt secure protocols to support authentication for devices, gateways, users, services, and applications. Consider using adopting the X.509 standard for device authentication.

- **Encryption**

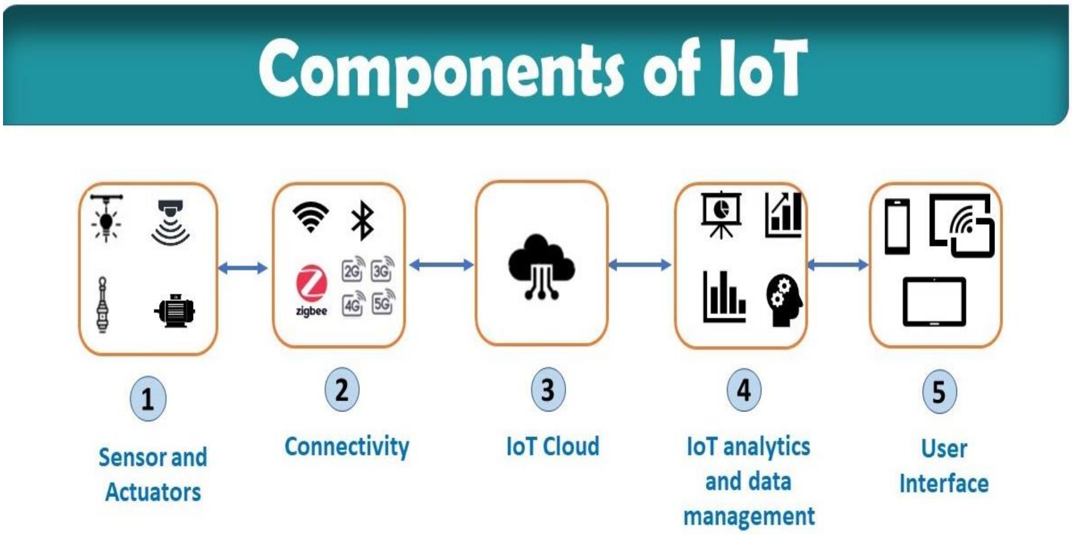
If you are using wifi, use Wireless Protected Access 2 (WPA2) for wireless network encryption. You may also adopt a Private Pre-Shared Key (PPSK) approach. To ensure privacy and data integrity for communication between applications, be sure to adopt TLS or Datagram Transport-Layer Security (DTLS), which is based on TLS, but adapted for unreliable connections that run over UDP. TLS encrypts application data and ensures its integrity

- **Port protection**

Port protection ensures that only the ports required for communication with the gateway or upstream applications or services remain open to external connections. All other ports should be disabled or protected by firewalls. Device ports might be exposed when exploiting Universal Plug and Play (UPnP) vulnerabilities. Thus, UPnP should be disabled on the router.

COMPONENTS OF IOT:

In the Internet of Things (IoT) ecosystem, various components work together to enable the connection, communication, and data exchange between devices and systems. These components can be broadly categorized as follows:



Devices/Things:
These are physical objects or sensors embedded with computing power and communication capabilities. They are at the heart of IoT and can include a wide range of items, such as sensors, actuators, wearables, industrial machines, and even household appliances.

Connectivity:
This layer involves the communication protocols and technologies that enable devices to connect to the internet or to other devices. Common IoT connectivity options include Wi-Fi, Bluetooth, Zigbee, cellular networks (3G, 4G, 5G), Lora WAN, and satellite communications.

Data Processing:
Once data is generated by IoT devices, it needs to be processed and analysed. Data processing can occur at various levels, including at the device itself (edge computing), in a local gateway, or in the cloud. Edge computing is becoming increasingly important for real-time or low-latency applications.

Cloud Services:
Cloud computing platforms play a crucial role in IoT by providing storage, data analytics, and scalable computing resources. IoT data is often sent to the cloud for storage and further analysis. Cloud services also facilitate remote device management and software updates.

Analytics and Insights: IoT data can provide valuable insights when analysed. Data analytics tools and machine learning algorithms are used to extract meaningful information from the vast amount of data generated by IoT devices. These insights can be used for decision-making and process optimization.

Power and Energy Management: Many IoT devices are battery-powered or have limited power sources. Effective power management and energy-efficient designs are essential to extend the operational life of these devices.

Management and Monitoring: IoT systems often involve a large number of devices distributed across various locations. Device management platforms help monitor the health and status of devices, perform remote updates, and ensure they operate efficiently.

Applications and User Interfaces:

This layer involves the software applications and user interfaces that allow users to interact with IoT devices and access the data they generate. It includes mobile apps, web dashboards, and other interfaces that provide insights and control over IoT devices.

SOME OF IOT APPLICATIONS:

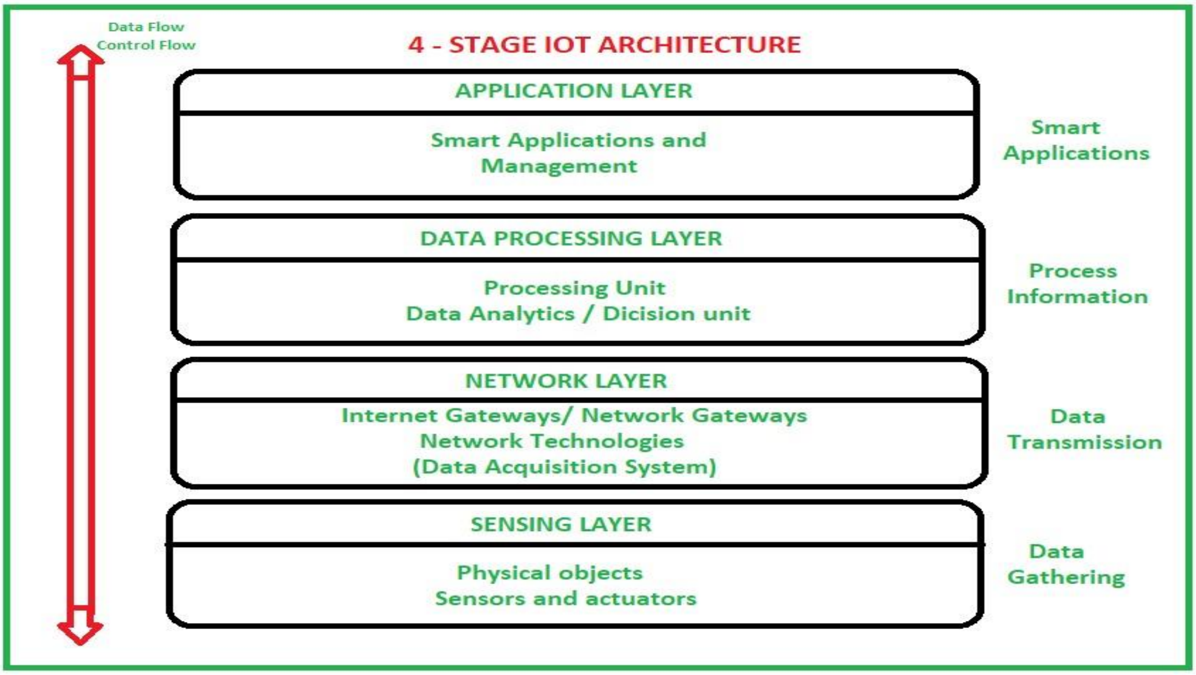
1. **Retail:** IoT is used for inventory management, customer tracking, and personalized shopping experiences.
2. **Transportation:** IoT is applied to vehicle tracking, fleet management, and traffic management systems for safer and more efficient transportation.
3. **Wearable Technology:** Smartwatches, fitness trackers, and other wearables collect and transmit health and activity data.
4. **Smart Grids:** IoT helps utilities improve grid management, monitor power distribution, and enable demand response systems.
5. **Connected Cars:** IoT is used for in-car entertainment, navigation, remote diagnostics, and vehicle-to-vehicle communication.
6. **Security and Surveillance:** IoT cameras and sensors enhance security systems by providing real-time monitoring and alerts.
7. **Smart Building Management:** IoT systems control lighting, HVAC, security, and access control to optimize building operations.
8. **Manufacturing:** IoT facilitates smart manufacturing processes with real-time data analytics, quality control, and supply chain integration.
9. **Oil and Gas:** IoT is used for remote monitoring and predictive maintenance of equipment in the oil and gas industry.
10. **Water Management:** IoT helps in monitoring and managing water resources, leak detection, and water quality control.
11. **Maritime and Shipping:** IoT devices are employed for ship tracking, navigation, cargo monitoring, and maritime safety.
12. **Education:** IoT enhances the learning experience with smart classrooms, campus security, and student engagement.
13. **Sports and Fitness:** IoT devices and wearables track sports performance, provide coaching insights, and encourage physical fitness.

14. **Hospitality:** IoT improves guest experiences in hotels and restaurants through smart room controls and personalized services.
15. **Aerospace:** IoT is used for aircraft maintenance, engine health monitoring, and flight data analysis.
16. **Smart Agriculture:** IoT enables precision farming techniques like automated irrigation, pest control, and crop monitoring.
17. **Renewable Energy:** IoT helps manage and optimize renewable energy sources like solar and wind power.

ARCHITECTURE OF IOT:

Internet of Things (IoT) technology has a wide variety of applications and use of Internet of Things is growing so faster. Depending upon different application areas of Internet of Things, it works accordingly as per it has been designed/developed. But it has not a standard defined architecture of working which is strictly followed universally. The architecture of IoT depends upon its functionality and implementation in different sectors. Still, there is a basic process flow based on which IoT is built.

Here in this article, we will discuss basic fundamental architecture of IoT i.e., 4 Stage IoT architecture.



BASIC IOT ARCHITECTURE

SENSING LAYER:

The sensing layer is the first layer of the IoT architecture and is responsible for collecting data from the physical world using sensors. This data can be anything from temperature and humidity to motion and sound.

Sensors are devices that can detect and measure physical changes in their environment. They are typically small and inexpensive, and can be embedded in a wide variety of objects. For example, sensors can be found in smartphones, fitness trackers, and even thermostats.

The type of sensor used depends on the specific IoT application. For example, a smart home system might use temperature and humidity sensors to monitor the indoor environment. A smart city system might use traffic sensors to monitor traffic flow. And a smart agriculture system might use soil moisture sensors to monitor crop health.

Once the sensors have collected data, they transmit it to the network layer. The network layer is responsible for transmitting the data to the data processing layer, where it can be analysed and interpreted.

The sensing layer is the most important layer of the IoT architecture, as it is the layer that interacts with the physical world. Without the sensing layer, IoT systems would not be able to collect the data that they need to function.

Here are some examples of sensors that are commonly used in IoT applications:

- Temperature sensors
- Humidity sensors
- Motion sensors
- Sound sensors
- Light sensors
- Pressure sensors
- Gas sensors
- Chemical sensors
- Vibration sensors
- Image sensors
- RFID sensors

IoT sensors can be used to collect data about a wide variety of environmental factors, including:

- Temperature

- Humidity
- Light levels
- Air quality
- Noise levels
- Motion
- Vibration
- Chemical levels
- Presence
- Location

NETWORK LAYER:

The network layer is an essential part of the IoT architecture, as it allows devices to communicate with each other and with the data processing layer. Without the network layer, IoT systems would not be able to function.

Here are some of the key challenges that the network layer in IoT architecture faces:

- **Scalability:** IoT systems can generate a large volume of data, so the network layer must be able to scale to handle this increased traffic load.
- **Reliability:** IoT systems are often used in critical applications, so the network layer must be highly reliable and able to withstand disruptions.
- **Security:** IoT systems are often vulnerable to cyberattacks, so the network layer must implement robust security measures to protect data from unauthorized access and modification.

Despite these challenges, the network layer is a critical component of the IoT architecture, and the development of new and innovative networking technologies is essential for the continued growth of IoT.Here are some examples of network technologies that are commonly used in IoT applications:

- Wi-Fi
- Bluetooth
- Cellular networks (LTE, 5G)
- LPWAN technologies (LoRaWAN, NB-IoT)
- Satellite networks

DATA PROCESSING LAYER

The data processing layer in IoT architecture is responsible for analyzing and interpreting the data received from the network layer. This can be done using a variety of software and hardware components, such as edge computing devices and cloud computing platforms.

The data processing layer is where the magic of IoT happens. This is where the data collected from the sensors is turned into meaningful insights that can be used to make decisions.

For example, a smart home system might use the data processing layer to analyze temperature and humidity data from sensors to determine whether the thermostat needs to be adjusted. A smart city system might use the data processing layer to analyze traffic data from sensors to identify traffic congestion and optimize traffic flow. And a smart agriculture system might use the data processing layer to analyze soil moisture data from sensors to determine whether the crops need to be watered.

The data processing layer is a critical component of the IoT architecture, as it allows us to extract meaningful insights from the data collected from sensors. Without the data processing layer, IoT systems would not be able to function.

Here are some examples of data processing tasks that are commonly performed in IoT applications:

- Data filtering and cleaning
- Data aggregation and summarization
- Real-time data analytics
- Machine learning and artificial intelligence
- Data visualization and reporting

APPLICATION LAYER

The application layer in IoT architecture is the topmost layer and is responsible for providing the end user with access to the data and insights generated by the data processing layer. This can be done through a variety of user interfaces, such as mobile apps, web dashboards, and desktop applications.

The application layer is the layer that the end user interacts with most directly. It is the layer that provides the user with the ability to control IoT devices, monitor data, and receive insights.

The application layer is a critical component of the IoT architecture, as it provides the end user with the ability to interact with IoT systems and derive value from the data that they generate. Without the application layer, IoT systems would not be able to provide the benefits that they do.

Here are some examples of application layer services that are commonly used in IoT applications:

- Device management and control
- Data visualization and reporting
- Real-time alerts and notifications
- Business process automation
- Decision support systems

DESIGN PRINCIPLES:

When designing an IoT system, there are a number of principles that should be kept in mind in order to ensure that the system is reliable, secure, and efficient. Some of the most important design principles for IoT systems include:

- **Security:** Security is one of the most important design principles for IoT systems. This is because IoT systems are often vulnerable to cyberattacks, as they often involve a large number of interconnected devices and systems. It is important to implement robust security measures at all layers of the IoT architecture, from the sensors to the data processing layer to the application layer.
- **Scalability:** IoT systems can generate a large volume of data, so it is important to design the system to be scalable enough to handle this increased traffic load. The system should also be able to accommodate a large number of devices and users.
- **Reliability:** IoT systems are often used in critical applications, so it is important to design the system to be highly reliable and able to withstand disruptions. This can be achieved by implementing redundancy and failover mechanisms.
- **Efficiency:** IoT systems can consume a lot of power, so it is important to design the system to be as efficient as possible. This can be achieved by using low-power devices and by optimizing the data processing and transmission algorithms.

In addition to these general design principles, there are a number of other factors that should be considered when designing an IoT system, such as the specific application requirements, the cost budget, and the regulatory environment.

Here are some additional design principles that can be considered for IoT systems:

- **Modularity:** Designing an IoT system in a modular way can make it easier to scale and maintain the system over time. Modularity can also make it easier to add new features and functionality to the system in the future.

- **Openness:** Using open standards and protocols when designing an IoT system can make it easier to integrate the system with other systems and devices. This can also make it easier to find developers and support for the system.
- **Privacy**: It is important to design IoT systems with privacy in mind. This means collecting and using only the data that is necessary for the system to function properly. It also means taking steps to protect the data from unauthorized access and modification.

DESIGN CAPABILITIES;

The needed capabilities in IoT vary depending on the specific application, but there are a few key capabilities that are essential for all IoT systems:

- **Connectivity:** IoT devices need to be able to connect to the network in order to send and receive data. This can be done using a variety of communication protocols, such as Wi-Fi, Bluetooth, cellular networks, and LPWAN technologies.
- **Security:** IoT systems are often vulnerable to cyberattacks, so it is important to implement robust security measures at all layers of the system, from the sensors to the data processing layer to the application layer.
- Scalability**: IoT systems can generate a large volume of data, so it is important to design the system** to be scalable enough to handle this increased traffic load. The system should also be able to accommodate a large number of devices and users.
- **Reliability:** IoT systems are often used in critical applications, so it is important to design the system to be highly reliable and able to withstand disruptions. This can be achieved by implementing redundancy and failover mechanisms.
- **Power efficiency**: IoT devices are often powered by batteries, so it is important to design them to be as power-efficient as possible. This can be achieved by using low-power components and by optimizing the data processing and transmission algorithms.

In addition to these essential capabilities, there are a number of other capabilities that may be needed for specific IoT applications, such as:

- **Real-time processing:** Some IoT applications require real-time processing of data, such as traffic monitoring and industrial automation systems.
- **Artificial intelligence and machine learning:** Some IoT applications use artificial intelligence and machine learning to analyze data and make predictions.
- **Edge computing:** Edge computing allows IoT devices to process data locally, which can reduce latency and improve performance.
- **Cloud computing**: Cloud computing can be used to store and process large amounts of data from IoT devices.

The specific capabilities that are needed for an IoT system will depend on the specific application requirements. However, the essential capabilities listed above are essential for all IoT systems.

Here are some examples of how these needed capabilities are being used in IoT applications:

- **Smart homes:** Smart homes use a variety of IoT devices, such as thermostats, lights, and security systems, to collect data and control the home environment. These devices need to be able to connect to the network and communicate with each other securely. They also need to be power-efficient so that they can run on batteries for extended periods of time.
- **Smart cities:** Smart cities use IoT devices to monitor and manage urban infrastructure, such as traffic, air quality, and energy consumption. These devices need to be able to collect data in real time and transmit it to a central processing system. They also need to be able to withstand harsh environmental conditions.
- **Smart manufacturing**: Smart manufacturing uses IoT devices to monitor and control production lines. These devices need to be able to connect to the network securely and communicate with each other in real time. They also need to be able to operate in harsh industrial environments.

M2M Communication

Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction. This includes serial connection, powerline connection (PLC), or wireless communications in the industrial Internet of Things (IoT). Switching over to wireless has made M2M communication much easier and enabled more applications to be connected.

In general, when someone says M2M communication, they often are referring to cellular communication for embedded devices. Examples of M2M communication in this case would be vending machines sending out inventory information or ATM machines getting authorization to dispense cash.

As businesses have realized the value of M2M, it has taken on a new name: the Internet of Things (IoT). IoT and M2M have similar promises: to fundamentally change the way the world operates. Just like IoT, M2M allows virtually any sensor to communicate, which opens up the possibility of systems monitoring themselves and automatically responding to changes in the environment, with a much-reduced need for human involvement. M2M and IoT are almost synonymous—the exception is IoT (the newer term) typically refers to wireless communications, whereas M2M can refer to any two machines—wired or wireless—communicating with one another.

Traditionally, M2M focused on "industrial telematics," which is a fancy way of explaining data transfer for some commercial benefit. But many original uses of M2M still stand today, like smart meters. Wireless M2M has been dominated by cellular since it came out in the mid-

2000’s with 2G cell networks. Because of this, the cellular market has tried to brand M2M as an inherently cellular thing by offering M2M data plans. But cellular M2M is only one subsection of the market, and it shouldn’t be thought of as a cellular-only area.

How M2M Works:

As previously stated, machine-to-machine communication makes the Internet of Things possible. According to Forbes, M2M is among the fastest-growing types of connected device technologies in the market right now, largely because M2M technologies can connect millions of devices within a single network. The range of connected devices includes anything from vending machines to medical equipment to vehicles to buildings. Virtually anything that houses sensor or control technology can be connected to some sort of wireless network.

This sounds complex, but the driving thought behind the idea is quite simple. Essentially, M2M networks are very similar to LAN or WAN networks, but are exclusively used to allow machines, sensors, and controls, to communicate. These devices feed information they collect back to other devices in the network. This process allows a human (or an intelligent control unit) to assess what is going on across the whole network and issue appropriate instructions to member devices.

M2M Applications:

The possibilities in the realm of M2M can be seen in four major use cases, which we’ve detailed below:

MANUFACTURING

Every manufacturing environment—whether it’s food processing or general product manufacturing—relies on technology to ensure costs are managed properly and processes are executed efficiently. Automating manufacturing processes within such a fast-paced environment is expected to improve processes even more. In the manufacturing world, this could involve highly automated equipment maintenance and safety procedures. For example, M2M tools allow business owners to be alerted on their smartphones when an important piece of equipment needs servicing, so they can address issues as quickly as they arise. Sophisticated networks of sensors connected to the Internet could even order replacement parts automatically.

HOME APPLIANCES

IoT already affects home appliance connectivity through platforms like Nest. However, M2M is expected to take home-based IoT to the next level. Manufacturers like LG and Samsung are already slowly unveiling smart home appliances to help ensure a higher quality of life for occupants. For example, an M2M-capable washing machine could send alerts to the owners’ smart devices once it finishes washing or drying, and a smart refrigerator could automatically order groceries from Amazon once its inventory is depleted. There are many more examples of home automation that can potentially improve quality of life for residents, including systems that allow members of the household to remotely control HVAC systems using their mobile devices. In situations where a homeowner decides to leave work early, he or she could contact the home heating system before leaving work to make sure the temperature at home will be comfortable upon arrival.

HEALTHCARE DEVICE MANAGEMENT

One of the biggest opportunities for M2M technology is in the realm of health care. With M2M technology, hospitals can automate processes to ensure the highest levels of treatment. Using devices that can react faster than a human healthcare professional in an emergency situation makes this possible. For instance, when a patient's vital signs drop below normal, an M2M-connected life support device could automatically administer oxygen and additional care until a healthcare professional arrives on the scene. M2M also allows patients to be monitored in their own homes instead of in hospitals or care centres. For example, devices that track a frail or elderly person's normal movement can detect when he or she has had a fall and alert a healthcare worker to the situation.

SMART UTILITY MANAGEMENT

In the new age of energy efficiency, automation will quickly become the new normal. As energy companies look for new ways to automate the metering process, M2M comes to the rescue, helping energy companies automatically gather energy consumption data, so they can accurately bill customers. Smart meters can track how much energy a household or business uses and automatically alert the energy company, which supplants sending out an employee to read the meter or requiring the customer to provide a reading. This is even more important as utilities move toward more dynamic pricing models, charging consumers more for energy usage during peak times.

The Value of M2M:

Growth in the M2M and IoT markets has been growing rapidly, and according to many reports, growth will continue. Strategy Analytics believes that low power, wide-area network (LPWAN) connections will grow from 11 million in 2014 to 5 billion in 2022. And IDC says the market for worldwide IoT solutions will go from $1.9 trillion in 2013 to $7.1 trillion in 2020.

Many big cell operators, like AT&T and Verizon, see this potential and are rolling out their own M2M platforms. Intel, PTC, and Wipro are are all marketing heavily in M2M and working to take advantage of this major industry growth spurt. But there is still a great opportunity for new technology companies to engage in highly automated solutions to help streamline processes in nearly any type of industry. We're certain we'll see a huge influx of companies who begin to innovate in this area in the next five years.

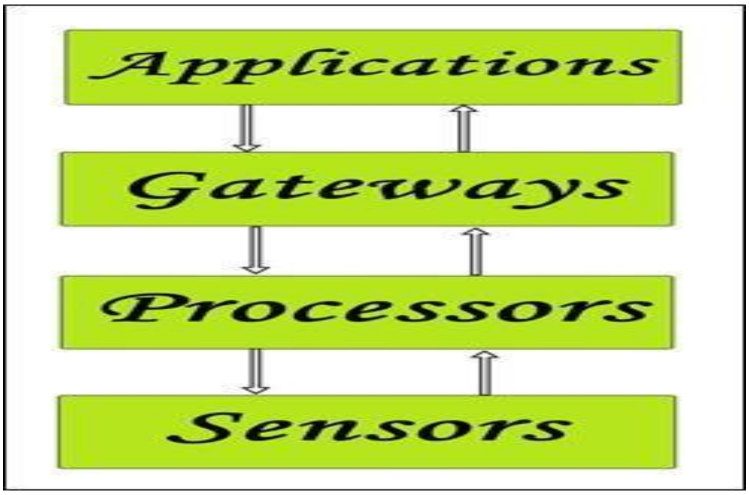
However, as the cost of M2M communication continues to decrease, companies must determine how they will create value for businesses and customers. In our mind, the opportunity and value for M2M doesn't lie in the more traditional layers of the communication world. Cell carriers and hardware manufacturers, for example, are beginning to look into full-stack offerings that enable M2M and IoT product development. We strongly believe value lies in the application side of things, and the growth in this industry will be driven by smart applications from this point forward.

Companies shouldn't think about IoT or M2M for the sake of IoT or M2M. Instead, they should focus on optimizing their business models or providing new value for their customers. For example, if you're a logistics company like FedEx or UPS, you have obvious choices for automated logistics decisions made by machines. But if you're a retailer, the transition to automation may not be as obvious. It's one thing to think of a "cool" automated process—say, creating advertising that is automatically tied to a specific customer through the use of M2M technology—but before you move forward with the process, you have to consider the value you're getting out of it. How much does it cost to implement? Will any company considering a move into the IoT space needs to understand what its business model is, how it will make money, and how it will provide value for customers or internal processes.

Functional blocks of an IoT ecosystem:

IoT don't exist in a void. A lone sensor isn't really good for anything, nor is a bunch of them, for that matter, unless they are all connected to one another and to platforms that generate data for further use. This is what we call an Internet of Things (IoT) ecosystem – a broad network of connected and interdependent devices and technologies that are applied by specialists towards a specific goal, such as the creation of a smart city.

Obviously, there are limitless applications to the IoT and therefore we can speak of endless coexisting IoT ecosystems. But if you boil what is happening in the ecosystem down to the bare essentials, you will come up with a simple schema: a **device** collects data and sends it across the **network** to a **platform** that aggregates the data for future use by the **agent**. And so we have the key components to an IoT ecosystem: devices, networks, platforms, and agents. Let's discuss them in more detail.
Four things form basic building blocks of the IoT system –sensors, processors, gateways, applications. Each of these nodes has to have its own characteristics in order to form an useful IoT system.



Simplified block diagram of the basic building blocks of the **IoT**

Sensors:

- These form the front end of the IoT devices. These are the so-called "Things" of the system. Their main purpose is to collect data from its surroundings (sensors) or give out data to its surrounding (actuators).
- These have to be uniquely identifiable devices with a unique IP address so that they can be easily identifiable over a large network.
- These have to be active in nature which means that they should be able to collect real-time data. These can either work on their own (autonomous in

nature) or can be made to work by the user depending on their needs (user-controlled).

- Examples of sensors are gas sensor, water quality sensor, moisture sensor, etc.

Processors:

• Processors are the brain of the IoT system. Their main function is to process the data captured by the sensors and process them so as to extract the valuable data from the enormous amount of raw data collected. In a word, we can say that it gives intelligence to the data.

• Processors mostly work on real-time basis and can be easily controlled by applications. These are also responsible for securing the data – that is performing encryption and decryption of data.

• Embedded hardware devices, microcontroller, etc are the ones that process the data because they have processors attached to it.

Gateways:

• Gateways are responsible for routing the processed data and send it to proper locations for its (data) proper utilization.

• In other words, we can say that gateway helps in to and fro communication of the data. It provides network connectivity to the data. Network connectivity is essential for any IoT system to communicate. LAN, WAN, PAN, etc are examples of network gateways.

Applications:

• Applications form another end of an IoT system. Applications are essential for proper utilization of all the data collected.

• These cloud-based applications which are responsible for rendering the effective meaning to the data collected. Applications are controlled by users and are a delivery point of particular services.

• Examples of applications are home automation apps, security systems, industrial control hub, etc.

IoT devices:

As we said earlier, there are many scenarios in which IoT can be employed and they all require different devices. Here, at the most basic level, we can speak of sensors (i.e. devices that sense things, such as temperature, motion, particles, etc.) and actuators (i.e. devices that act on things, such as switches or rotors).

Rarely, though, will a smart solution make do with just one type of an IoT sensor or an actuator. If you think of a smart surgical robot, for example, it will require hundreds, if not thousands, of components that measure different parameters and act accordingly. But even apparently less complicated solutions aren't truly that easy. Consider running a smart farm – for a plant to grow, it's not just a matter of measuring the humidity of the soil, but also its fertility; it's also a matter of providing proper irrigation based on insolation, and much more. So you need not just one, but many sensors and actuators that all have to work together.

Group devices into two categories

Basic Devices:

Devices that only provide the basic services of sensor readings and/or actuation tasks, and in some cases limited support for user interaction. LAN communication is supported via wired or wireless technology; thus, a gateway is needed to provide the WAN connection.

Advanced Devices:

In this case the devices also host the application logic and a WAN connection. They may also feature device management and an execution environment for hosting multiple applications. Gateway devices are most likely to fall into this category.

device
network
agent
platform

Here are some examples of IoT devices:

- Smart home devices: Smart thermostats, smart lights, smart locks, smart smoke detectors, smart coffee makers, smart refrigerators, smart speakers, smart TVs, smart doorbells, smart garage door openers, smart baby monitors, and smart pet feeders.
- Wearable devices: Smartwatches, fitness trackers, smart glasses, and smart hearing aids.
- Industrial devices: Industrial sensors, actuators, and control systems.

- Agricultural devices: Soil moisture sensors, crop health sensors, and livestock monitoring devices.
- Medical devices: Implantable medical devices, wearable medical devices, and remote patient monitoring devices.
- Other: Asset tracking devices, smart city devices, and smart retail devices.

IOT GATEWAYS

An IoT gateway is a physical device or virtual platform that connects IoT devices to the cloud. It acts as a central hub, routing data between IoT devices and the cloud. Gateways also perform a variety of other functions, such as data aggregation, filtering, and security.

IoT gateways are important because they allow IoT devices to communicate with the cloud and with each other in a secure and efficient way. Gateways also help to reduce the amount of data that needs to be transmitted to the cloud, which can save money and improve performance.

Here are some of the key benefits of using IoT gateways:

- Security: Gateways can provide a layer of security between IoT devices and the cloud. This is important because IoT devices are often vulnerable to cyberattacks. Gateways can implement security measures such as encryption, authentication, and authorization to protect data from unauthorized access and modification.
- Efficiency: Gateways can help to improve the efficiency of IoT systems by aggregating and filtering data before it is sent to the cloud. This can reduce the amount of data that needs to be transmitted, which can save money and improve performance.
- Scalability: Gateways can help to scale IoT systems by providing a central hub for connecting and managing IoT devices. This can make it easier to add and remove devices from the system, and to manage the data flow between devices and the cloud.
- Local processing: Gateways can perform local processing of data from IoT devices. This can reduce the amount of data that needs to be sent to the cloud, and it can also improve the performance of IoT applications that require real-time data processing.

DATA MANAGEMENT:

Data management in IoT is the process of collecting, storing, processing, and analyzing data from IoT devices. This data can be used to improve the performance of IoT systems, to develop new products and services, and to make better decisions.

Data generation

- Data generation is the first stage within which data is generated actively or passively from the device, system, or as a result of its interactions.
- The sampling of data generation depends on the device and its capabilities as well as potentially the application needs.
- Usually default behaviors for data generation exist, which are usually further configurable to strike a good benefit between involved costs,

Data acquisition

- Data acquisition deals with the collection of data (actively or passively) from the device, system, or as a result of its interactions.
- The data acquisition systems usually communicate with distributed devices over wired or wireless links to acquire the needed data, and need to respect security, protocol, and application requirements.
- The frequency of data acquisition overwhelmingly depends on, or is customized by, the application requirements (or their common denominator).
- The data acquired at this stage (for non-closed local control loops) may also differ from the data actually generated.

Data validation

- Data acquired must be checked for correctness and meaningfulness within the specific operating context.
- This is usually done based on rules, semantic annotations, or other logic.
- As real-world processes depend on valid data to draw business-relevant decisions **Example**, imposed range limits on the values acquired, logic checks, uniqueness, correct time-stamping, etc.

- In addition, semantics may play an increasing role here, as the same data may have different meanings in various operating contexts, and via semantics one can benefit while attempting to validate them.
- Failure to validate may result in security breaches.
- Tampered-with data fed to an application is a well known security risk as its effects may lead to attacks on other services, privilege escalation, denial of service, database corruption, etc.

Data storage

- The data generated by M2M interactions is what is commonly referred to as "Big Data."
- Machines generate an incredible amount of information that is captured and needs to be stored for further processing.
- As this is proving challenging due to the size of information, a balance between its business usages vs. storage needs to be considered; that is, only the fraction of the data relevant to a business need may be stored for future reference.

Data processing

- Data processing enables working with the data that is either at rest (already stored) or is in-motion (e.g. stream data).
- The scope of this processing is to operate on the data at a low level and "enhance" them for future needs.
- Typical examples include data adjustment during which it might be necessary to normalize data, introduce an estimate for a value that is missing, re-order incoming data by adjusting timestamps, etc.

Data analysis

- Data available in the repositories can be subjected to analysis with the aim to obtain the information they encapsulate and use it for supporting decision-making processes.
- The analysis of data at this stage heavily depends on the domain and the context of the data.
- For instance, business intelligence tools process the data with a focus on the aggregation and key performance indicator assessment.
- Data mining focuses on discovering knowledge, usually in conjunction with predictive goals.

Privacy

Data such as patient medical data, data for supplying goods in a company from and to different locations, and changes in inventories, may need privacy and protection from conscious or unconscious transfer to untrustworthy destinations using the Internet. Privacy is an aspect of data management and must be remembered while designing an application. The design should ensure privacy by ensuring that the data at the receiving end is considered anonymous from an individual or company.

Following are the components of the privacy model:

- Devices and applications identity-management
- Authentication
- Authorisation

- Trust
- Reputation

A suitable encryption of identification of data source enforces privacy. Device ID management provides for privacy. The analysed decrypted data is an input to application, service or process. IoT or M2M data have to be for the beneficiary individual person or company only.

Secure Data Access

Access to data needs to be secure. The design ensures the authentication of a request for data and authorisation for accessing a response or service. It may also include auditing of requests and accesses of the responses for accountability in future. Example 2.4 described how a layer provides the confidentiality and authorisation using AES-128 and CCM. End-to-end security is another aspect while implies using a security protocol at each layer, physical, logical link and transport layers during communication at both ends in a network.

Data Source and Data Destination

ID: Each device and each device resource is assigned an ID for specifying the data of source and a separate ID for data destination.

Address: Header fields add the destination address (for example, 48-bit MAC address at Link layer, 32-bit IPv4 address at IP network and 128-bit IPv6 address at IPv6 network) and may also add the port (for example, port 80 for HTTP application).

Data Characteristics, Formats and Structures

Data characteristics can be in terms of temporal data (dependent on the time), spatial data (dependent on location), real-time data (generated continuously and acquired continuously at the same pace), real-world data (from physical world for example, traffic or streetlight, ambient condition), proprietary data (copy right data reserved for distribution to authorised enterprises) and big data (unstructured voluminous data).

Data received from the devices, formats before transmission onto Internet. The format can be in XML, JSON and TLV (Section 3.1.3). A file can be MIME type for Internet (Section 3.1.5).

BUSINESS PROCESS IN IOT

A business process in IoT is a collection of activities that use IoT devices to collect, process, and analyze data to achieve a business goal. IoT business processes can automate tasks, improve efficiency, and create new revenue opportunities.

Here are some examples of IoT business processes:

- Smart manufacturing: An IoT business process in smart manufacturing might use sensors to collect data on machine performance, product quality, and inventory levels. This data can then be used to automate production lines, identify potential problems before they occur, and optimize inventory levels.
- Smart retail: An IoT business process in smart retail might use sensors to track customer movement and product selection. This data can then be used to improve store layout, merchandising strategies, and customer service.
- Smart agriculture: An IoT business process in smart agriculture might use sensors to monitor crop health, soil moisture levels, and weather conditions. This data can then be used to optimize irrigation, fertilization, and pest control practices.
- Smart healthcare: An IoT business process in smart healthcare might use wearable devices to monitor patient vital signs and activity levels. This data can then be used to provide remote patient monitoring, early detection of health problems, and personalized treatment plans.

IoT business processes can be implemented in a variety of ways. Some companies choose to develop their own IoT business processes using open source software and hardware. Others choose to use commercial IoT platforms that offer pre-built business process templates.

When designing an IoT business process, it is important to consider the following factors:

- Business goals: What are the specific business goals that the IoT business process is trying to achieve?
- Data needs: What data is needed to achieve the business goals?
- IoT devices: What IoT devices will be used to collect the data?
- Data processing: How will the data be processed and analysed?
- Security: How will the data be protected from unauthorized access and modification?

IoT business processes can be complex, but they can also be very rewarding. By implementing IoT business processes, companies can improve their efficiency, productivity, and profitability.

Here are some of the benefits of using IoT business processes:

- Improved efficiency: IoT business processes can automate tasks and streamline workflows, which can lead to significant efficiency gains.

- Increased productivity: IoT business processes can help employees to be more productive by providing them with the data and tools they need to do their jobs effectively.
- Reduced costs: IoT business processes can help companies to reduce costs by automating tasks, improving efficiency, and reducing waste.
- New revenue opportunities: IoT business processes can help companies to create new revenue opportunities by developing new products and services, or by improving the customer experience.

Everything as a service (XaaS)

Everything-as-a-Service (XaaS) in IoT refers to the delivery of any IoT-related product, service, or solution on a subscription basis over the internet. This includes everything from IoT devices and sensors to data storage, processing, and analytics to IoT application development and deployment.

This approach allows businesses and individuals to access and use a wide range of services without the need to own or maintain the underlying infrastructure or resources. When combined with the Internet of Things (IoT), it can lead to innovative solutions and business models. Here's how "Everything as a Service" and IoT can intersect:

1. **Infrastructure as a Service (IaaS):** This provides the foundational computing, storage, and networking resources needed to support IoT deployments. Organizations can rent virtual machines, storage, and network resources in the cloud to host IoT platforms and applications.
2. **Platform as a Service (PaaS):** IoT PaaS offerings provide a ready-made platform for developing, deploying, and managing IoT applications. They often include tools for data processing, device management, and analytics. Developers can focus on application development without worrying about the underlying infrastructure.
3. **Software as a Service (SaaS**): IoT SaaS solutions offer complete IoT applications or services that can be accessed over the internet. These services can include remote monitoring, predictive maintenance, and analytics platforms, among others.
4. **Data as a Service (DaaS):** DaaS providers offer access to curated and real-time IoT data streams. Organizations can subscribe to these services to obtain valuable data for analysis and decision-making.
5. **Device as a Service (DaaS):** This involves leasing IoT devices or sensors rather than purchasing them outright. DaaS providers may also include device management services, ensuring that devices are maintained and updated throughout their lifecycle.
6. **Function as a Service (FaaS):** FaaS, also known as serverless computing, allows organizations to run code in response to specific events or triggers in an event-driven architecture. This is useful for building serverless IoT applications that only consume resources when needed.
7. **Security as a Service (SECaaS):** IoT devices and networks require robust security measures. SECaaS offerings provide security services such as authentication, encryption, threat detection, and access control to protect IoT deployments.

8. **Edge as a Service (EaaS):** EaaS solutions extend cloud computing capabilities to the edge of the network, allowing data processing and analysis to occur closer to IoT devices. This reduces latency and bandwidth usage.
9. **Connectivity as a Service (CaaS):** CaaS providers offer connectivity solutions, including IoT-specific cellular plans, satellite connectivity, or Lora WAN network access.
10. **Blockchain as a Service (BaaS):** BaaS offerings provide blockchain-based services for securing IoT data and transactions, especially in applications where data integrity and trust are critical.
11. **Compliance as a Service (CompaaS):** CompaaS offerings help organizations ensure that their IoT deployments comply with industry-specific regulations and data privacy laws, such as GDPR or HIPAA.

ROLE OF CLOUD IN IOT

The cloud plays a vital role in the Internet of Things (IoT) by providing the infrastructure and services needed to connect, manage, and process data from IoT devices. Cloud computing offers a number of benefits for IoT applications, including:

- **Scalability:** Cloud computing can easily scale up or down to meet the changing needs of IoT applications. This is important because IoT applications can generate a large volume of data, which can be difficult to store and process on-premises.
- **Reliability:** Cloud computing platforms are designed to be highly reliable and available. This is important for IoT applications, which often need to collect and process data in real time.
- **Security:** Cloud computing platforms offer a variety of security features to protect data from unauthorized access and modification. This is important for IoT applications, which are often vulnerable to cyberattacks.

In addition to these general benefits, the cloud also offers a number of specific services for IoT applications, such as:

- **Device management:** Cloud-based device management platforms can be used to provision, configure, and monitor IoT devices. This can help to automate and simplify the process of managing IoT devices at scale.
- **Data collection and storage:** Cloud-based data collection and storage platforms can be used to collect and store data from IoT devices. This data can then be used to power IoT applications and to generate insights.
- **Data analytics:** Cloud-based data analytics platforms can be used to analysed data from IoT devices to extract meaningful insights. This information can then be used to improve decision-making, to optimize operations, and to develop new products and services.
- **Application development and deployment**: Cloud-based application development and deployment platforms can be used to develop and deploy IoT applications. This can help to reduce the time and cost of developing and deploying IoT applications.

The cloud is an essential component of many IoT systems. By providing the infrastructure and services needed to connect, manage, and process data from IoT devices, the cloud enables IoT applications to scale, be reliable, and be secure.

1. IoT Cloud Computing provides many connectivity options, implying large network access. People use a wide range of devices to gain access to cloud computing resources: mobile devices, tablets, laptops. This is convenient for users but creates the problem of the need for network access points.
2. Developers can use IoT cloud computing on-demand. In other words, it is a web service accessed without special permission or any help. The only requirement is Internet access.
3. Based on the request, users can scale the service according to their needs. Fast and flexible means you can expand storage space, edit software settings, and work with the number of users. Due to this characteristic, it is possible to provide deep computing power and storage.
4. Cloud Computing implies the pooling of resources. It influences increased collaboration and builds close connections between users.
5. As the number of IoT devices and automation in use grows, security concerns emerge. Cloud solutions provide companies with reliable authentication and encryption protocols.
6. Finally, IoT cloud computing is convenient because you get exactly as much from the service as you pay. This means that costs vary depending on use: the provider measures your usage statistics. A growing network of objects with IP addresses is needed to

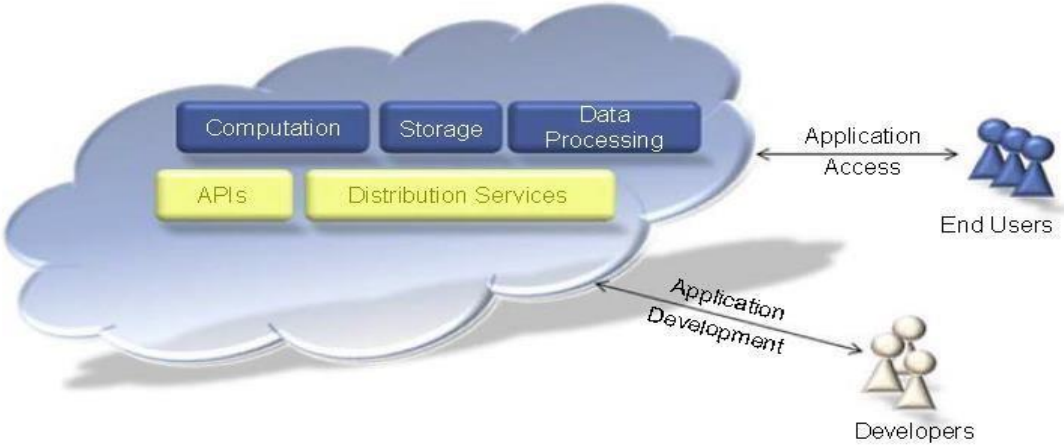


FIGURE:OVERVIEW OF CLOUD COMPUTING

connect to the Internet and exchange data between the components of the network. assigned and

reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth. Ø **Rapid Elasticity.**

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

Measured Service.

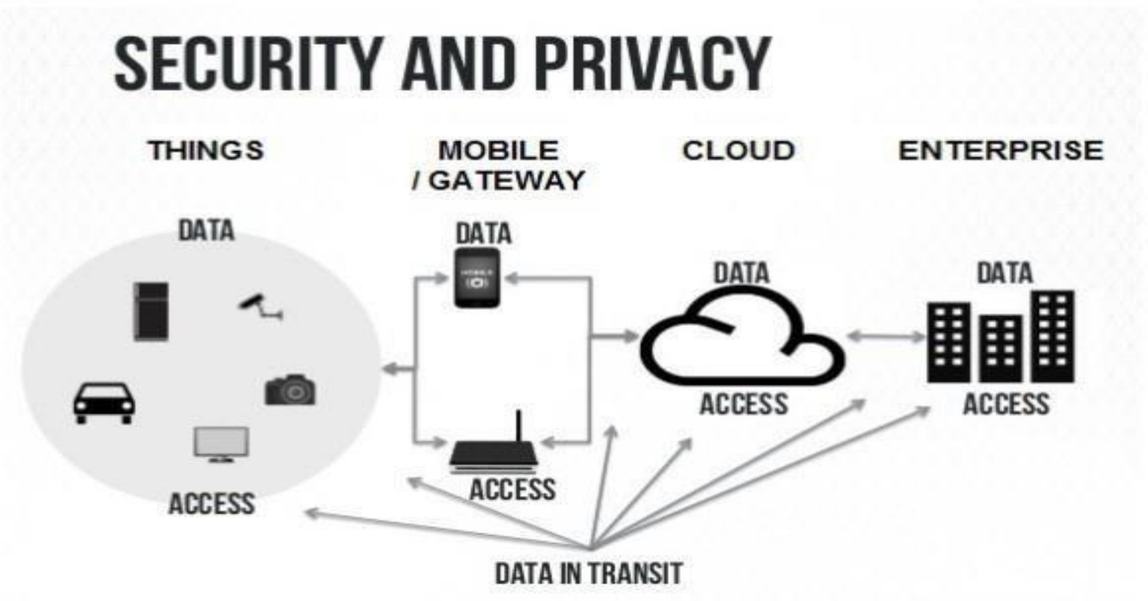
- ✓ Cloud systems automatically control and optimize resource use by leveraging a metering capability, at some level of abstraction, appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts).
- ✓ Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

SECURITY ASPECTS IN IOT

Security is a critical aspect of the Internet of Things (IoT), as IoT devices are often vulnerable to cyberattacks. IoT devices are often connected to the internet and to each other, which makes them an attractive target for hackers. Additionally, IoT devices often collect and store sensitive data, such as personal information and financial data.

There are a number of security risks associated with IoT devices, including:

- Unauthorized access: Hackers can gain unauthorized access to IoT devices and steal data or take control of the devices.
- Data breaches: Hackers can exploit vulnerabilities in IoT devices to steal data, such as personal information, financial data, and intellectual property.
- Denial-of-service (DoS) attacks: Hackers can launch DoS attacks against IoT devices to overwhelm them and make them unavailable.
- Man-in-the-middle (MitM) attacks: Hackers can intercept communications between IoT devices and steal data or modify the data.
- Malware infections: IoT devices can be infected with malware, which can then be used to steal data, take control of the devices, or launch attacks against other devices.



There are a number of things that can be done to improve the security of IoT devices, including:

- Use strong passwords: All IoT devices should use strong passwords that are difficult to guess or crack.
- Keep software up to date: Software updates often include security patches, so it is important to keep all IoT device software up to date.
- Use a firewall: Firewalls can help to protect IoT devices from unauthorized access.
- Use a VPN: VPNs can encrypt data transmitted between IoT devices and the cloud, which can help to protect data from unauthorized access.
- Use a security solution: There are a number of security solutions available for IoT devices, such as intrusion detection systems and intrusion prevention systems.

  It is also important to be aware of the security risks associated with IoT applications. IoT applications should be designed with security in mind, and should use best practices such as data encryption and authentication.

Here are some additional tips for improving the security of your IoT devices:

- Only connect IoT devices to trusted networks: Avoid connecting IoT devices to public Wi-Fi networks, as these networks are often less secure than private networks.
- Disable unnecessary features and services: If you don't need a particular feature or service on an IoT device, disable it. This can help to reduce the attack surface of the device.
- Be careful about what information you share: Only share necessary information with IoT devices and applications.
- Monitor your IoT devices: Use a security solution to monitor your IoT devices for suspicious activity.

DIFFERENCE BETWEEN IOT AND M2M

Basis	IoT	M2M
Abbreviation	Internet of Things	Machine to Machine
Communication	IoT sensors automation	Communicates directly between machines
Connection	The connection is via using various communication types	Point-to-Point Connection
Communication protocols	HTTP, Ftp, Telnet, etc are used	Communication technology techniques and traditional protocols are used.
Intelligence	Objects are responsible for decision-making	Observation of some degree of intelligence
Technology	Hardware and Software based technology	Hardware-based technology
Data Delivery	Depending on the Internet protocol	Devices can be connected through mobile or other networks
Internet Connection	An active Internet connection is required	Devices do not rely on an internet connection
Scope	Many users can connect at a time over the Internet	Communicate with a single machine at a time
Business Type	B2C(Business to Customers) and B2B(Business to Business)	Only B2B(Business to Business) is used
Open API support	IoT supports open API Integrations	M2M does not support open API
Data Sharing	Data is shared with applications that tend to improve the end-user experience	Data is shared with the communication parties themselves.