Dayananda Sagar University

School of Engineering, Hosur Main Road, Kudlu Gate, Bengaluru-560 068

Introduction to IoT and Embedded Computing 20AM3610

20AM3610

SEMESTER – VI

Course Code: 20AM3610

Prof. Pradeep Kumar K

Dept. of CS&E (AIML)

DSU, Bangalore

20AM3610

Course Objectives:

- ● To understand the fundamental of IoT and appreciate the importance of communication between machines with reference to IoT.
- ● To understand the embedded systems including design techniques, controldriven architectures, and use of Internet for communication.
- ● See the mechanism of controls and sensing and use of Internet to take global decisions using IoT technology and see how it works.
- ● To understand, appreciate and develop ability to use various contemporary IOT communication protocols for transport, discovery and routing.
- ● To understand the methodologies to implement the software systems for embedded computing and methods of programming them.
- ● To appreciate the utilities of IoT through case studies

20AM3610

Course outcomes:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Program an embedded computing device such as Arduino and Raspberry Pi.	L2
CO2	Build an IoT system for sensing and decision making.	L3
CO3	Implement standard communication protocols for IoT to build large systems	L4
CO4	Appreciate and understand the use of IoT in systems such as home automation, smart lighting, smart parking etc	L4

20AM3610

Text Documents Requirement

- **TEXT BOOKS:**

1. Jeeva Jose, “Internet of Things”, Khanna Book Publishing Company, 2021.

2. Samuel Greengard, “The Internet of Things”, 1st Edition, MIT Press, 2015.

3. Peter Waher, Pradeeka Seneviratne, Brian Russell, Drew Van Duren, “IoT: Building Arduino-Based Projects”, 1st Edition, Packt Publishing Ltd, 2016

- **REFERENCES:**

Peter Waher, “Mastering Internet of Things: Design and create your own IoT applications using Raspberry Pi 3”, 1st Edition, Packt Publishing Ltd, 2018

David Hanes, Gonzalo Salgueiro, “IoT Fundamentals: Networking Technologies, protocols, and use cases for the Internet of Things”, Cisco Press, 8th impression 2021.

20AM3610

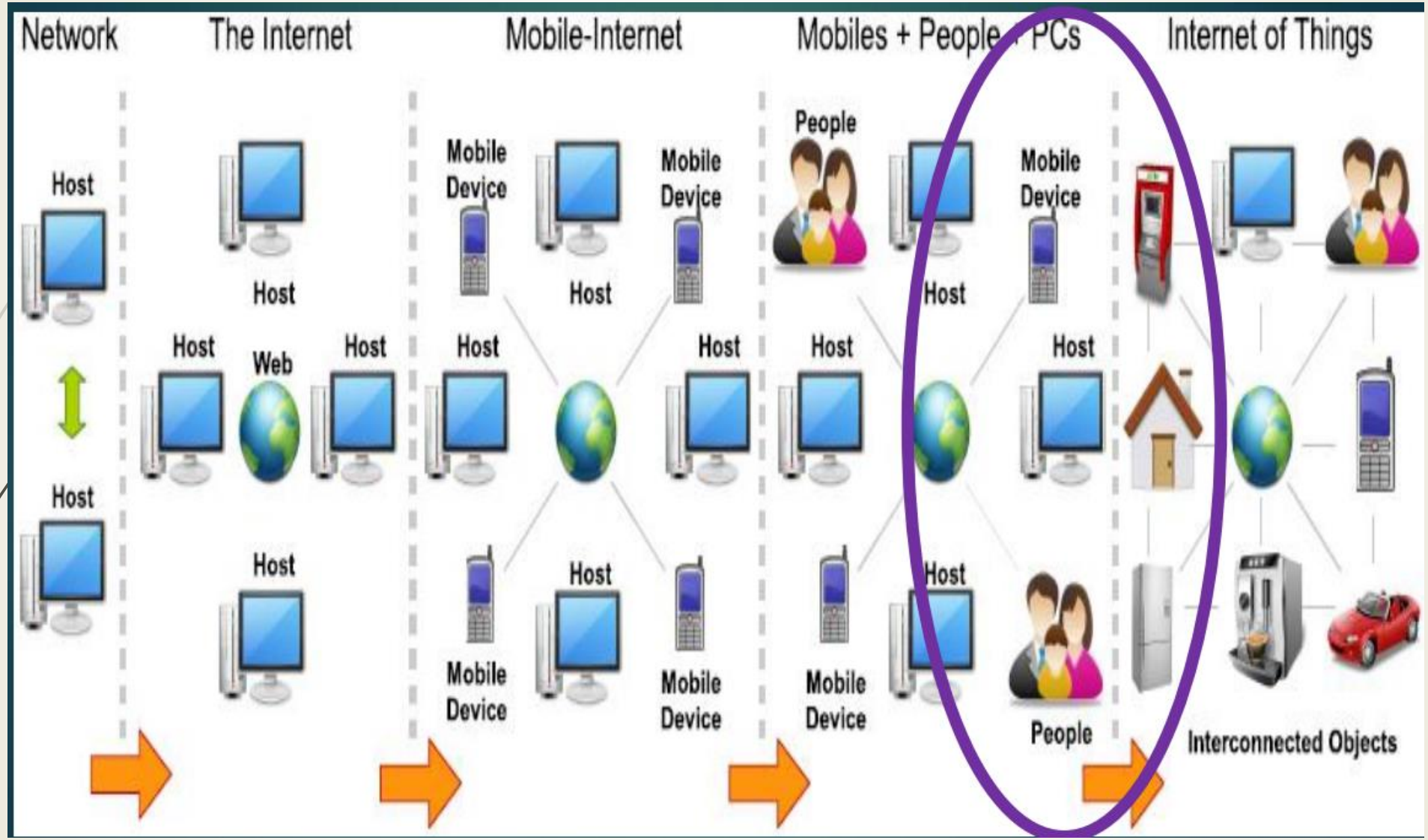
Module-1 : Introduction to IoT

- Introduction: Definition, Characteristics and Architecture of IOT Devices, Trends in the Adoption of IoT in modern applicants, Risks, Privacy, and Security.

20AM3610

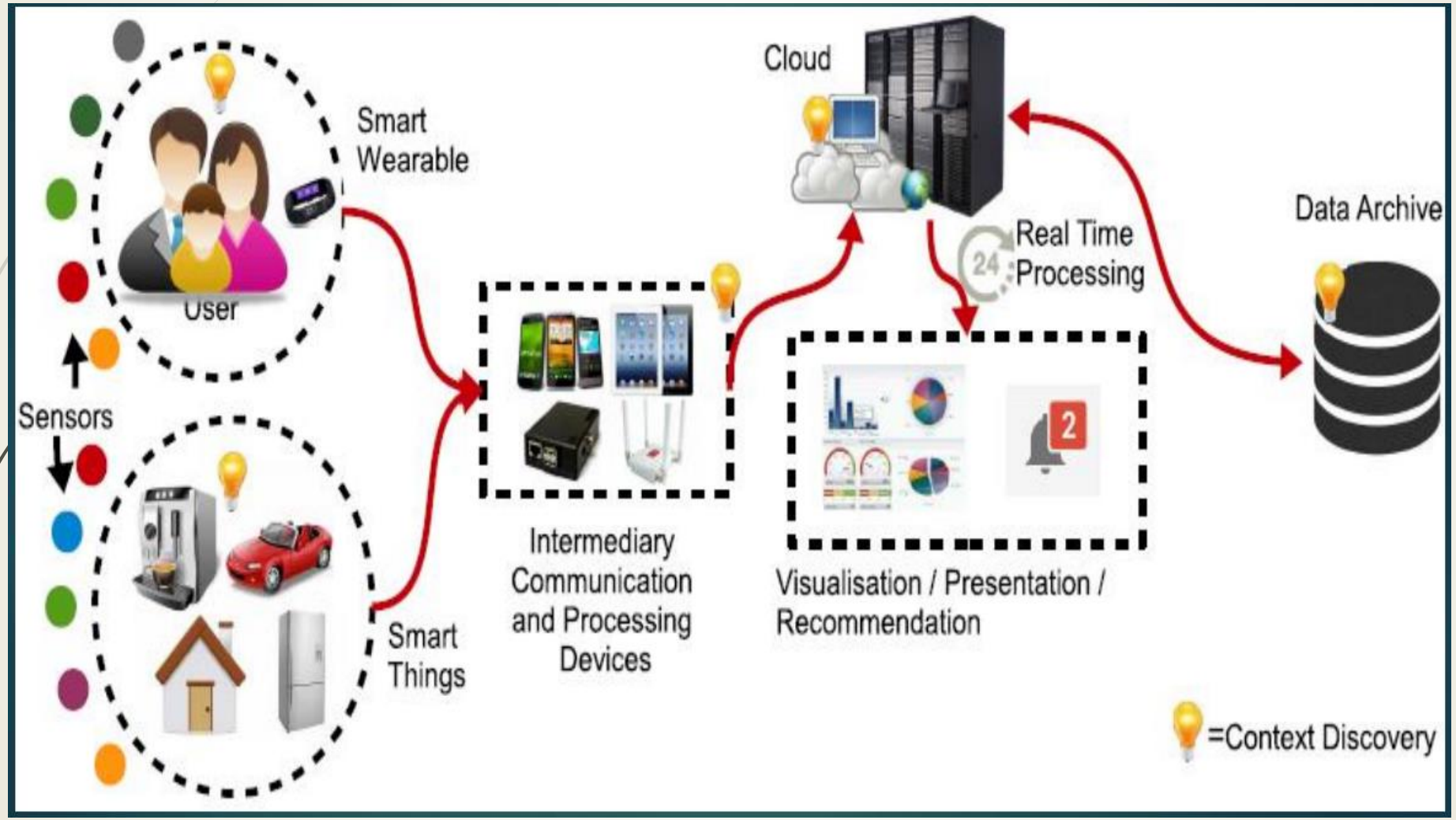
Introduction: Definition

- The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.
- IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.
- "Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist fire-fighters in search and rescue operations.
- These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices.


Network
The Internet
Mobile-Internet
Mobiles + People + PCs
Internet of Things
Host
Web
Mobile Device
People
Interconnected Objects

20AM3610

IOT Ecosystem



20AM3610

Ecosystem Components

- Device manufacturers
  - Sensors/actuators, smart appliances
- Network service providers
  - Operators, NMS providers
- Cloud service providers
  - Data centres, dBase, dWarehouse
- Platform providers
  - Middleware providers, SDKs
- 3rd party application developers
  - Analytics providers, tools, APIs

20AM3610

History of IoT

- The concept of the Internet of Things first became popular in 1999, through the Auto-ID Center at MIT and related market-analysis publications.
- Radio-frequency identification (RFID) was seen as a prerequisite for the IoT at that point. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Besides using RFID, the tagging of things may be achieved through such technologies as near field communication, barcodes, QR codes, bluetooth, and digital watermarking.

20AM3610

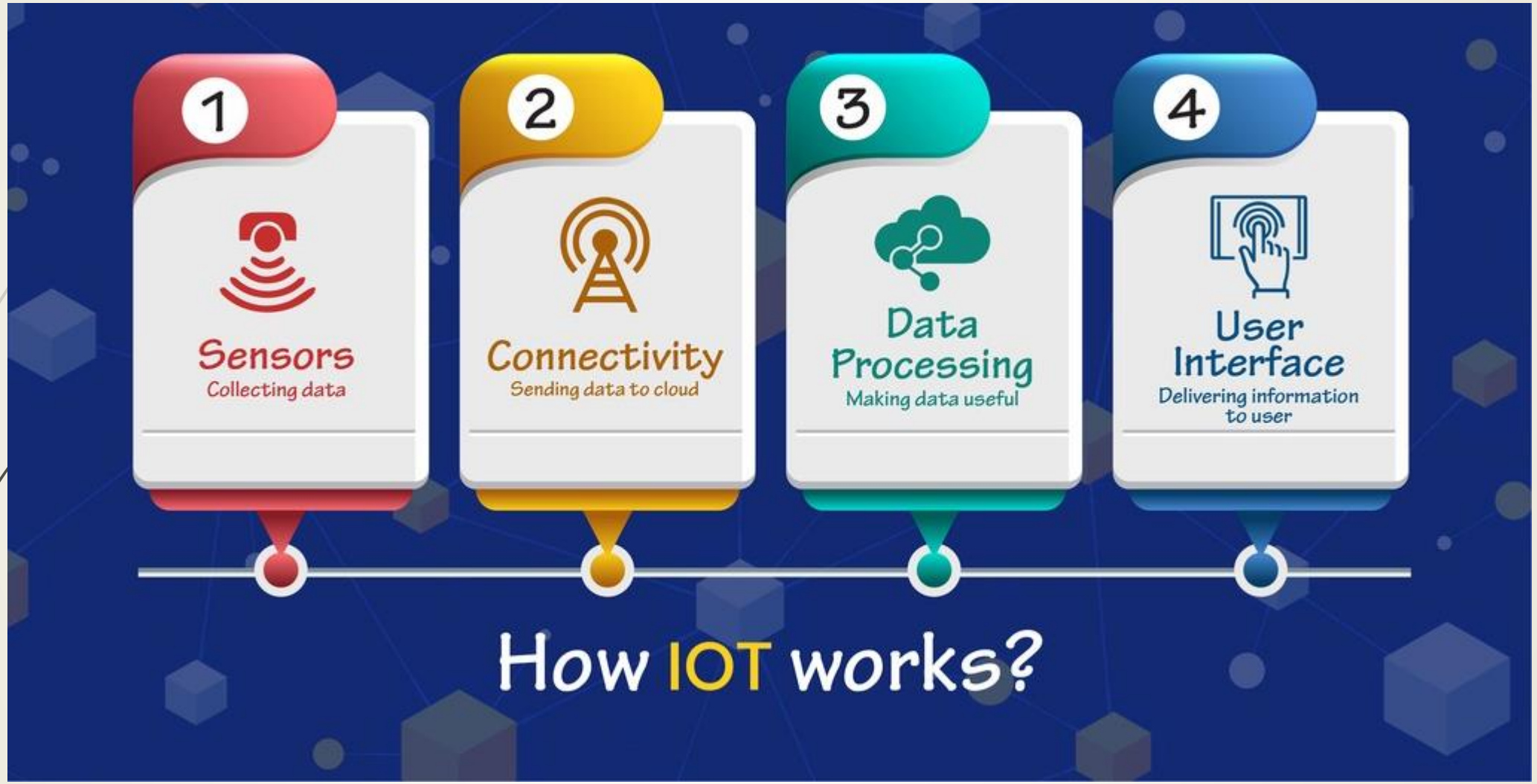
How IoT Works?

Internet of Things is not the result of a single novel technology; instead, several complementary technical developments provide capabilities that taken together help to bridge the gap between the virtual and physical world.

These capabilities include:

- ***Communication and cooperation***
- ***Addressability***
- ***Identification***
- ***Sensing***
- ***Actuation***
- ***Embedded information processing***
- ***Localization***
- ***User interfaces***

20AM3610


1
Sensors
Collecting data
2
Connectivity
Sending data to cloud
3
Data Processing
Making data useful
4
User Interface
Delivering information to user
How IOT works?

20AM3610

Internet of things definition and examples

- The term “Internet of Things” or IoT was first coined by Kevin Ashton in 1999. But it was only when Gartner added IoT to its list of new emerging technologies in 2011, that it started to gain global momentum. As of 2021, there were 21.7 billion active connected devices in the world today, out of which more than 11.7 billion (54 percent) are IoT devices. This means that there are more IoT devices in the world than there are non-IoT devices.
- IoT is an umbrella term that refers to the billions of physical objects or “things” connected to the Internet, all collecting and exchanging data with other devices and systems over the Internet.

20AM3610

Types of IoT

- **Consumer IoT** - Primarily for everyday use. Eg: home appliances, voice assistance, and light fixtures.
- **Commercial IoT** - Primarily used in the healthcare and transport industries. Eg: smart pacemakers and monitoring systems.
- **Military Things (IoMT)** - Primarily used for the application of IoT technologies in the military field. Eg: surveillance robots and human-wearable biometrics for combat.
- **Industrial Internet of Things (IIoT)** - Primarily used with industrial applications, such as in the manufacturing and energy sectors. Eg: Digital control systems, smart agriculture and industrial big data.
- **Infrastructure IoT** - Primarily used for connectivity in smart cities. Eg: infrastructure sensors and management systems.

Why is IoT Important?

- To generate new business models and revenue streams
- To improve business decisions through data-driven insights from IoT data
- To increase productivity and efficiency of business operations
- To enhance customer experience

Examples of IoT Devices

- **Home Security :** The key driver behind smart and secure homes is IoT. A variety of sensors, lights, alarms and cameras (all of which can be controlled from a smartphone) are connected via IoT to provide 24x7 security.
- **Activity Trackers:** Smart home security cameras provide alerts and peace of mind. Activity trackers are sensor devices that can monitor and transmit key health indicators in real-time. You can track and manage your blood pressure, appetite, physical movement and oxygen levels.
- **Industrial Security and Safety:** IoT-enabled detection systems, sensors and cameras can be placed in restricted areas to detect trespassers. They can also identify pressure buildups and small leaks of hazardous chemicals and fix them before they become serious problems.
- **Augmented Reality Glasses:** Augmented Reality (AR) glasses are wearable computer-enabled glasses that help you get extra information such as 3D animations and videos to the user's real-world scenes. The information is presented within the lenses of the glasses and can help users access Internet applications.
- **Motion Detection:** Motion sensors can detect vibrations in buildings, bridges, dams and other large-scale structures. These devices can identify anomalies and disturbances in the structures that could lead to catastrophic failures. They can also be used in areas susceptible to floods, landslides, and earthquakes.

20AM3610

Top 5 Most Popular IoT Devices in 2023

- **Google Home Voice Controller:** Google Home voice controller is one of the most popular IoT devices out there today. It provides voice-enabled services like alarms, lights, thermostats, volume control and lots more.
- **Amazon Echo Plus Voice Controller:** Amazon Echo Plus voice controller is another popular and reliable IoT device on the market. It provides voice-enabled services like answering phone calls, setting timers and alarms, checking the weather, and lots more.
- **August Doorbell Cam:** August Doorbell Cam is an IoT device that allows you to answer your door from any remote location. It constantly captures motion changes and suspicious activity in your doorstep.
- **August Smart Lock:** August Smart Lock is a proven and reliable security IoT device that helps users to manage their doors from any remote location. It helps keep thieves away and provides an extra layer of security for your home.
- **Foobot:** Foobot is an IoT device that can accurately measure indoor pollution. It helps to improve the air quality in houses, cafes, workplaces, and other indoor public spaces.

20AM3610

Characteristics and Architecture of IOT Devices

- Characteristics of the Internet of Things :
- **Connectivity:** Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. For example, connection between people through internet devices like mobile phones ,and other gadgets, also connection between Internet devices such as routers, gateways, sensors, etc.
- **Intelligence and Identity :** The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.
- **Scalability :** The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous, and it should be handled appropriately.
- **Dynamic and Self-Adapting (Complexity):** IoT devices should dynamically adapt themselves to the changing contexts and scenarios. Assume a camera meant for the surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon, night).

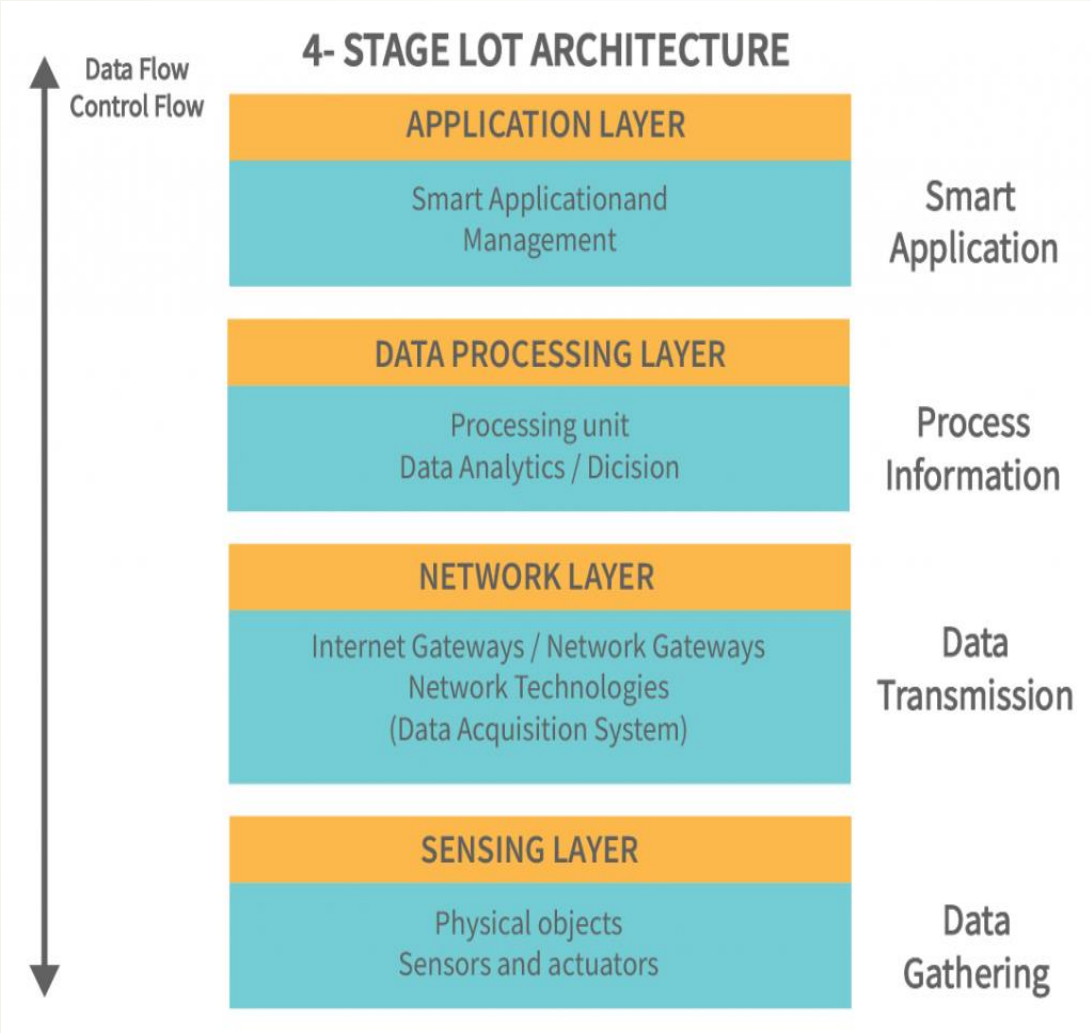
- **Architecture:** IoT architecture cannot be homogeneous in nature. It should be hybrid, supporting different manufacturers ' products to function in the IoT network. IoT is not owned by anyone engineering branch. IoT is a reality when multiple domains come together.
- **Safety:** There is a danger of the sensitive personal details of the users getting compromised when all his/her devices are connected to the internet. This can cause a loss to the user. Hence, data security is the major challenge. Besides, the equipment involved is huge. IoT networks may also be at the risk. Therefore, equipment safety is also critical.
- **Self Configuring:** This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.
- **Interoperability:** IoT devices use standardized protocols and technologies to ensure that they can communicate with each other and with other systems. Interoperability is one of the key characteristics of the Internet of Things (IoT). It refers to the ability of different IoT devices and systems to communicate and exchange data with each other, regardless of the underlying technology or manufacturer.

- Examples of standards used in IoT include:

1. MQTT (Message Queuing Telemetry Transport) – A publish/subscribe communication protocol used for IoT device communication.
2. CoAP (Constrained Application Protocol) – A lightweight communication protocol for IoT devices with limited resources.
3. Bluetooth Low Energy (BLE) – A wireless communication technology used for IoT devices with low power consumption requirements.
4. Wi-Fi – A wireless communication technology used for IoT devices that require high data transfer rates.
5. Zigbee – A low-power, low-cost wireless communication technology used for IoT devices.

20AM3610

Architecture of Internet of Things (IoT)



Sensing Layer:

The sensing layer is the first layer of the IoT architecture and is responsible for collecting data from different sources.

- This layer includes sensors and actuators that are placed in the environment to gather information about temperature, humidity, light, sound, and other physical parameters.
- These devices are connected to the network layer through wired or wireless communication protocols.

Network Layer:

- The network layer of an IoT architecture is responsible for providing communication and connectivity between devices in the IoT system.
- It includes protocols and technologies that enable devices to connect and communicate with each other and with the wider internet.
- Examples of network technologies that are commonly used in IoT include WiFi, Bluetooth, Zigbee, and cellular networks such as 4G and 5G.
- Additionally, the network layer may include gateways and routers that act as intermediaries between devices and the wider internet, and may also include security features such as encryption and authentication to protect against unauthorized access.

Data processing Layer:

- The data processing layer of IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing, and interpreting data from IoT devices.
- This layer is responsible for receiving raw data from the devices, processing it, and making it available for further analysis or action.
- The data processing layer includes a variety of technologies and tools, such as data management systems, analytics platforms, and machine learning algorithms.
- These tools are used to extract meaningful insights from the data and make decisions based on that data.

Application layer :

- The application layer of IoT architecture is the topmost layer that interacts directly with the end-user.
- It is responsible for providing user-friendly interfaces and functionalities that enable users to access and control IoT devices.
- This layer includes various software and applications such as mobile apps, web portals, and other user interfaces that are designed to interact with the underlying IoT infrastructure.
- It also includes middleware services that allow different IoT devices and systems to communicate and share data seamlessly.
- The application layer also includes analytics and processing capabilities that allow data to be analyzed and transformed into meaningful insights. This can include machine learning algorithms, data visualization tools, and other advanced analytics capabilities.

Trends in the adoption of IoT in modern applications

20AM3610

- What Future Trends Will Drive IoT..?

- **Growth will continue to accelerate:** If indications are anything to go by, IoT is not nearing its peak, quite the opposite. As the cost of computing power, sensors, and high-bandwidth networking continue to fall, the adoption of IoT will continue to accelerate.
- **Focus on improving operations and asset utilisation:** One of the primary drivers behind any digital transformation is to do more with less. Operation-centric use cases seem to be the central focus for businesses looking to adopt IoT, even outpacing those concerned with supply chain and smart connected consumer products.
- **IoT initiatives will continue to deliver success:** 80% of IoT adopters believe it's crucial to business success. They also think they will see 30% ROI because of their investment, not to mention the hidden benefits. We believe businesses will continue to enjoy these remarkable success rates adopting IoT in the future.
- **The gap between early adopters and followers will grow:** As we've seen with many other digital disruptions, early birds get the worm. Companies that have already rolled out IoT in some form are also planning the highest future rollouts. Clearly, they've experienced something that's driving them to pursue IoT even more vigorously.
- **APAC will continue to catch up to North America and Europe:** North America and Europe have a tradition of leading the way for many new technologies, and IoT is no different. However, adoption and innovation in the APAC region are growing considerably, narrowing the gap to its Western counterparts.

IoT Privacy and Security: Challenges and Solutions

20AM3610

- IoT brought users huge benefits; however, some challenges come along with it.
- Cybersecurity and privacy risks are the primary concerns of the researchers and security specialists cited. These two are posing a considerable predicament for many business organizations as well as public organizations.
- Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies.
- This vulnerability is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet requiring novel security solutions.
- It is, however, unfortunate that the users do not often have the required acknowledgment of the security impacts until the time when a breach has occurred, causing massive damages such as loss of crucial data.
- With the ongoing security breaches which have compromised the privacy of users, the appetite of the consumers for poor security is now declining. There were a lot of vulnerabilities in modern automotive systems.

Security

20AM3610

The IoT is diverse from traditional computers and computing devices, makes it more vulnerable to security challenges in different ways:

- Many devices in the Internet of Things are designed for deployment on a massive scale. An excellent example of this is sensors.
- Usually, the deployment of IoT comprises of a set of alike or nearly identical appliances that bear similar characteristics. This similarity amplifies the magnitude of any vulnerability in the security that may significantly affect many of them.
- Similarly, many institutions have come up with guides for risk assessment conduction. This step means that the probable number of links interconnected between the IoT devices is unprecedented. It is also clear that many of these devices can establish connections and communicate with other devices automatically in an irregular way. These call for consideration of the accessible tools, techniques, and tactics which are related to the security of IoT.

- The consumers are required to trust the Internet of Things devices and the services are very secure from weaknesses, particularly as this technology continues becoming more passive and incorporated in our everyday lives.
- With weakly protected IoT gadgets and services, this is one of the very significant avenues used for cyber attacks as well as the exposure of the data of users by leaving data streams not protected adequately.
- The nature of the interconnection of the IoT devices means if a device is poorly secured and connected it has the potential of affecting the security and the resilience on the Internet internationally.
- This behavior is simply brought about by the challenge of the vast employment of homogenous devices of IoT. Besides the capability of some devices to be able to mechanically bond with other devices, it means that the users and the developers of IoT all have an obligation of ensuring that they are not exposing the other users as well as the Internet itself to potential harm.

- When it comes to authentication, for instance, IoT faces various vulnerabilities, which remain one of the most significant issues in the provision of security in many applications.
- The authentication used is limited in how it protects only one threat, such as Denial of Service (DoS) or replay attacks.
- Information security is one of the significant vulnerable areas in the authentication of IoT due to the prevalence of applications which are risky due to their natural multiplicity of data collection in the IoT environment.
- If we can, for instance, take an example of contactless credit cards. These cards are capable of permitting card numbers and names to be read without the authentication of IoT; this makes it possible for hackers to be able to purchase goods by using a bank account number of the cardholder and their identity.
- One of the most prevalent attacks in the IoT is the man in the middle, where the third-party hijack communication channel is aimed at spoofing identities of the palpable nodes which are involved in network exchange.

Privacy

- The perspective of the usefulness of the IoT is dependent on how well it can respect the privacy choices of people.
- Concerns regarding the privacy and the potential harms that come along with IoT might be significant in holding back the full adoption of IoT. It is essential to know that the rights of privacy and user privacy respect are fundamental in ensuring users' confidence and self-assurance in the Internet of Things, the connected device, and related services offered.
- A lot of work is being undertaken to ensure that IoT is redefining the privacy issues such things as the increase of surveillance and tracking. The reason for the privacy concerns is because of the omnipresent intelligence integrated artifacts where the sampling process and the information distribution in the IoT may be done nearly in any place.
- The ubiquitous connectivity via the Internet access is also an essential factor that helps in understanding this problem because unless there is a unique mechanism put in place, then it will be decidedly more comfortable to access the personal information from any corner of the world

20AM3610

Interoperability

- A fragmented environment of proprietary IoT technical implementation is known to inhibit value for users. Even though full interoperability is not always feasible across products and services, the users may not like buying products and services where there is no flexibility and concerns over dealer lock-in. Poorly planned IoT gadgets might mean that there will be a negative consequence for the networking resources that they connect to.
- Cryptography is another essential aspect that has been used for many years to provide defense against security loopholes in many applications. An effective defensive mechanism against the attacks perpetrated is not possible using one security application. It, therefore, requires different layers of security against the threats to the authentication of IoT.
- By the development of more advanced security features and building these features into products, hacks may be evaded. This evasion is because the users will buy products that already have proper security features preventing vulnerabilities. Cybersecurity frameworks are some of the measures put forward to ensure that IoT is secure.

- Moreover, some several factors and concerns might have an impact on compromising the efforts to secure the Internet of Things devices; these include:
- **Occasional update:** usually, IoT manufacturers update security patches quarterly. The OS versions and security patches are also upgraded similarly. Therefore, hackers get sufficient time to crack the security protocols and steal sensitive data.
- **Embedded passwords:** IoT devices store embedded passwords, which helps the support technicians to troubleshoot OS problems or install necessary updates remotely. However, hackers could utilize the feature for penetrating device security.
- **Automation:** often, enterprises and end-users utilize the automation property of IoT systems for gathering data or simplifying business activities. However, if the malicious sites are not specified, integrated AI can access such sources, which will allow threats to enter into the system.

- **Remote access:** IoT devices utilize various network protocols for remote access like Wi-Fi, ZigBee, and Z-Wave. Usually, specific restrictions are not mentioned, which can be used to prevent cybercriminals. Therefore, hackers could quickly establish a malicious connection through these remote access protocols.
- **Wide variety of third-party applications:** several software applications are available on the Internet, which can be used by organizations to perform specific operations. However, the authenticity of these applications could not be identified easily. If end-users and employees install or access such applications, the threat agents will automatically enter into the system and corrupt the embedded database.
- **Improper device authentication:** most of the IoT applications do not use authentication services to restrict or limit network threats. Thereby, attackers enter through the door and threaten privacy.
- **Weak Device monitoring:** usually, all the IoT manufacturers configure unique device identifiers to monitor and track devices. However, some manufacturers do not maintain security policy. Therefore, tracking suspicious online activities become quite tricky.

20AM3610

IoT Security Challenges

- Lack of physical security
- Botnet attacks
- Lack of visibility
- Data privacy
- Ransomware

IoT Security Solutions

- Use IoT Security analytics
- Endpoint Detection & Response (EDR)
- Secure APIs
- Improve Network Visibility
- Encrypted Communication
- Authentication

20AM3610


Thank
You