Definition and History of IoT

The Internet of Things (IoT) has not been around that long. But the actual idea of connected devices had been around longer, at least since the 70s. Back then, the idea was often called “embedded internet” or “pervasive computing”. It was only in 1999 that the term ***‘internet of things’*** was coined by Kevin Ashton. Ashton used the phrase as the title of his presentation for a new sensor project he was working on, and it stuck from there. He meant to represent the concept of computers and machines with sensors, which are connected to the Internet to report status and accept control commands. Ashton introduced the definition of IoT, “comparing to the twentieth century, when all the data were uploaded on a computer by a person using additional devices, the twenty-first century presents us the gadgets that can collect and send data themselves. This is the essence of the Internet of Things: data is collected, processed, and transmitted by devices with no human impact needed.”

Simply stated, the **Internet of Things (IoT)** is a global network infrastructure of interconnected devices (such as sensors, actuators, personal electronic devices, laptops, tablets, digital cameras, smartphones, alarm systems, home appliances, or industrial machines, and other smart devices) that are enabled with technology of interacting and communicating with each other. The fundamental characteristics of IoT include interconnectivity, scalability, heterogeneity, and dynamic changes. IoT can be divided into three layers:

- **Perception Layer –** This is also called the physical layer. This is where the sensors and connected devices come into play as they gather various amounts of data as per the need of the project. These can be the edge devices, sensors, and actuators that interact with their environment.
- **Network Layer –** This is mainly messaging and processing information. The data that's collected by all of these devices needs to be transmitted and processed. That's the network layer's job. It connects these devices to other smart objects, servers, and network devices. The role of this layer is to connect all things together and allow them to share information with each other.
- **Application Layer:** The application layer is what the user interacts with. It's what is responsible for delivering application-specific services to the user. This can be a smart home implementation, for example, where users tap a button in the app to turn on a coffee maker.

Advantages and Challenges of IoT

Here are some ***advantages*** of IoT:

- **Saves Money:** The biggest advantage of IoT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted. IoT fundamentally proves to be very helpful to people in their daily routines by making the appliances communicate to each other in an effective manner, thereby saving and conserving energy and cost. Allowing the data to be communicated and shared between devices and then translating it into our required way, IoT makes our systems efficient.
- **Monitoring:** The second most obvious advantage of IoT is monitoring. Knowing the exact quantity of supplies or the air quality in your home can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.
- **Automation and Control:** Due to physical objects getting connected and controlled digitally and centrally with wireless infrastructure, there is a large amount of automation and control in the workings. Without human intervention, the machines are able to communicate with each other leading to faster and timely output.
- **Ease of Access:** You can easily access data and information that is sitting far from your location, in real time. This is possible because of the network of devices, a person can access any information sitting from any part of the globe. This makes it very convenient for people to go about their work, even if they are not physically present.
- **Communication:** Better communication is possible over a network of interconnected devices, making the communication of devices more transparent, which reduces inefficiencies. Processes, where machines have to communicate with each other, are made more efficient and produce better, faster results. The perfect example of this is machinery at a manufacturing or production unit.
- **Information:** It is obvious that having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

Below are the ***drawbacks/challenges*** of IoT:

- **Security:** A major challenge facing IoT is cybersecurity and data security, which is rising in importance due to increased vulnerability to attacks and data breaches. Anything connected to the Internet can be hacked. Security issues such as access control, secure communication, and secure data storage in IoT environments are becoming challenging. In the IoT context, data are considered sensitive because data will encapsulate various aspects of industrial operation, including highly sensitive information about products, business strategies, and companies. People's concern is that the IoT is being developed rapidly without due consideration of the profound security challenges involved. Ensuring the security of IoT products and services must be given a priority, and this requires collaboration across borders, sectors, and organizations.
- **Privacy:** The IoT can challenge the traditional expectations of privacy. The user may not be aware that an IoT device is collecting and sharing data about the user with third parties. In a world where all things are connected, individuals' right to privacy needs to be protected. In order to achieve a reliable and secure IoT environment, a number of privacy principles and security protocols must be implemented. Principles of informed consent, data confidentiality, and security must be safeguarded. Ensuring privacy rights and respect for users is needed for trust and confidence in IoT services.
- **Energy Consumption:** Energy consumption is a major concern because devices connected to IoT consume power. Providing power to sensors for a prolonged period of time is key to IoT being deployed successfully. Sensors must be self-sustaining because it is impossible to change batteries in billions of IoT devices around the globe. Transfer, storage, and processing of data are the major energy-consuming activities with an IoT. Improving energy efficiency has positive economic and environmental impacts and reduces operational cost.
- **Data Management:** This is a challenge because IoT sensors and devices are generating massive amounts of data that need to be processed and stored. Data collected from IoT devices may be transmitted from one jurisdiction to another with no roadblocks. Information may be transmitted across borders without the user knowing it. The application of IoT devices raises legal and regulatory issues that did not exist prior to these devices.

Platform Architecture of IoT

Below are the design parameters that enterprises must consider when choosing their IoT platform architectural model. These design parameters dictate the levels of control that a platform has on IoT devices, the hierarchical layer where the IoT platform processes data, and the geographic proximity of the IoT platform to an enterprise's northbound systems. ***Northbound system,*** also called northbound interface, is an interface that allows a particular component of a network to communicate with a higher-level component. Having chosen these design parameters, an enterprise will be able to deploy the appropriate IoT platform architecture to support its IoT solutions.

- **Operational Autonomy –** It is the level of authority granted to an IoT device to take actions on connected assets or to control data. Operational autonomy is the first IoT platform design parameter. Enterprises choose the level of operational autonomy of IoT devices based on requirements of the device, platform, and internal business and technology requirements. Under certain circumstances, an IoT device might function very autonomously using a set of predefined rules that determine the amount of control it can have on connected assets. Under other circumstances, an IoT device might have no autonomy to control a connected asset, thereby requiring control from some other source, platform, or application. There are four (4) levels of operational autonomy:
  - ***Fully Autonomous Control* –** It means s that authority is granted to the IoT device for various on-device or on-location control functions. For example, the IoT device on a connected ice cream vending machine might autonomously control the proper internal temperature of the machine to preserve the quality of the ice cream. If the internal temperature of the machine exceeded its threshold, then the IoT device would send a message to a back-end system notifying the machine owner.
  - ***Semi-Autonomous Control* –** It means that authority is granted to the IoT device for most circumstances, but for some actions, machine control will come from other sources. For example, while a water pump is operating within reasonable parameters, the IoT device can manage the pump's performance autonomously. However, to switch on or off the water pump, a rule is created that authorization needs to come from another source, like an operations control center system or another application.

  - ***Non-Autonomous Control* –** It means that machine control comes from another source, not from the IoT device. Non-autonomous control of an IoT device is fairly common when a device has very low processing power. For example, a smart traffic management system requires rapid analysis of data from thousands or tens of thousands of assets. Data from the entire system are required to make real-time decisions about traffic flow, parking, bus systems, and rail transport. In this case, non-autonomous control of IoT devices is most suitable.
  - ***Multi-Layer Control* –** It means that machine control occurs at the global layer and optionally at the regional or localized layer. For example, an enterprise might have 15 globally distributed facilities manufacturing specialty plastics. This enterprise might choose to implement IoT solutions for factory floor automation, smart logistics tracking, and personnel surveillance.
- **Data Processing Depth –** It is the hierarchical layer where machine-related data is analyzed and acted upon. This design parameter helps enterprises stipulate the level at which IoT data is processed. Data processing can be completed by one or many isolated machines or a cluster of interconnected machines. The depth of data processing is related to the performance on each machine individually and on the cluster of machines. There are three (3) options for the level of data processing:
  - ***Localized Processing* –** It means that data are processed on-device. There are numerous reasons why data are processed on-device, including mobile network bandwidth or coverage constraints, latency concerns, intensive data processing requirements, and data security concerns. For example, autonomous driving vehicles use localized, on-device data processing to handle driver and vehicle safety functions where communications latency could be an issue.
  - ***Centralized Processing* –** It means that data are processed at a single location. In the case of centralized processing, an IoT platform processes data from one or more connected assets at a centralized location. Sometimes they choose this processing when there are security or privacy concerns associated with the collected IoT data. For example, a medium-sized enterprise might be running a fleet management solution to track its high-value assets during transportation. This enterprise might choose to do all of its IoT data processing at a centralized location to keep the location of fleet cargo secure.
  - ***Distributed processing* –** It means that data are processed on multiple devices and in multiple locations. This type of processing affords the most flexibility for an enterprise that wants to process and analyze IoT data. In addition, distributed processing allows an enterprise to manage multiple IoT solutions with different architectures at multiple locations.
- **Integration Topology –** It is the relative closeness of the IoT platform to a customer's northbound business systems and peer platforms. Integration topology is the third IoT platform design parameter. Enterprises can decide the relative closeness of the IoT platform to its northbound business systems and peer platforms. An enterprise's decision on integration topology is based on various technology and business requirements. Sometimes an enterprise's decision is most strongly based on data privacy and security issues, while other times, it is based on the current location of legacy industrial management systems. There are two (2) options for the integration topology:
  - ***Adjacent Location* –** It means that the IoT platform is located in the same geo-location or logical hierarchy as an enterprise's most relevant northbound business system or peer platform. Enterprises that choose an adjacent location for these systems often have data privacy or security issues associated with their solutions. It is also possible that enterprises wish to minimize the risks associated with latency or communications failures across the systems.
  - ***Non-Adjacent Location* –** It means that the IoT platform is located in a different geo-location or logical hierarchy as an enterprise's most relevant northbound business system or peer platform. There are many reasons why an enterprise would choose non-adjacency of its platforms and systems. The most obvious reason would be to gain the cost benefits of having distributed data systems. For example, a municipality with a connected street light solution might use a non-adjacent IoT platform. The risks of data privacy and security are minimal for the sensor data on connected street lights, while the cost savings of having a platform hosted in a multi-tenant vendor environment fits within a municipality's budget.

Smart Devices and Systems

An ***intelligent device*** is any type of equipment, instrument, or machine that has its own computing capability. On top of this definition is a ***smart device***, capable of communicating with other devices within the environment. It can perform intelligent operations on its own behavior with respect to its functionality and its relevant surrounding environment. These devices must have a minimum set of physical components to be categorized as smart devices. These components are as follows:

- **Power Component:** A power component is any source of power being provided to a device. This may be provided in a variety of ways, such as a mains power supply, battery, solar, etc. It may be a one-time battery charge or a replenishable supply of power scavenged from the environment. A power component has the responsibility of providing all electrical components of a device with sufficient power to operate within reasonable parameters. A power component must be aware of the energy demands of the device and be able to operate the device within normal working parameters.
- **Memory Component:** A smart device is able to make intelligent decisions on its own behavior with respect to its environment. Almost all embedded systems contain internal memory to store operations. The reason this is such an important component with regards to the smart device is that the requirement of memory will increase with the complexity of the operations being performed by the smart device. The memory component is split up into processor memory, cache, volatile and non-volatile memory. It takes a logical view of the physical components being independent of any implementation.
- **Communications Interface Component –** This component lets a device communicate with other devices and service within its smart space. This is an important component because if a device is to be able to interact with other devices within its smart space and let other devices and services interact with it, it must provide a means of communication to these other devices. There is no standard communications interface component, but the basis of the smart device model is that any communications interface is possible. This model is independent of how devices communicate (physical links) but does reinforce the fact that there must be a means of device access by the environment if a device is to interact with the smart space environment.

Smart Appliances and Smart Home Technologies

There are different types of smart appliances and smart home technologies. Each of these with different uses, types of connection, and interaction. The following are the main characteristics of the smart home systems in terms of user interfaces, smart hardware, and software platforms:

- **Energy Portal:** Energy portals are informatics-based application that delivers energy consumption information which was usually imperceptible to the consumer in a more user friendly way with information being explained in an easy to understand display of information. This type of application provides more detailed and direct feedback than traditional bills and is usually provided as a service from energy utilities. It receives energy consumption information from smart meters, smart appliances, and other smart products within the household. It allows users to act on the information given and remotely control appliances. Some of its interfaces include smartphones, web-based applications, and computer software, and it communicates with the users using Wi-fi or LAN. Its interaction is bi-directional, which allows for interaction with other smart home products.
- **In-Home Displays:** In-home displays are simple interfaces that provide immediate energy use feedback for the consumer, also having the ability to send pricing signals. The type of information given is usually very simple and direct. These devices are connected to the home energy network via a traditional normal meter and communicate with other peripheral devices through a home area network. It is also programmable to send energy pricing signals. Some of its interfaces include device display and peripheral displays, and it communicates wirelessly. Its interaction is uni-directional, which is from the device to the user.
- **Load Monitors:** Load monitors give a simple piece of energy consumption information of an energy consumption device. These are connected between the power outlet and the actual device and give the energy consumption of the device. The type of information given by load monitors is usually limited to the energy consumption and eventually a calculation of costs associated with this consumption, if these parameters are imputed by the user. It is installed between energy plugs and the appliances, and receives

real-time energy consumption information directly from individual appliances. Its interaction is also uni-directional.

- **Smart Appliances:** Smart appliances are defined as appliances that are communication-enabled. This communication platform can be used to offer multiple classes of functionalities like demand-side flexibility. On the energy aspect of smart appliances, these have the capability to receive, interpret and act on a signal received from an energy provider and adjust its operation according to the settings chosen by the energy consumer. It has the ability to change the appliance's consumption pattern and has the possibility to adapt its consumption to energy produced on-site. Its interface includes device displays, peripheral displays, web applications, and energy portals. Its interaction is bi-directional between the user and energy utilities and communicates thru wired and wireless communication.
- **Smart Thermostats:** Smart thermostats ultimately have the same main functionality as traditional thermostats that is to control the temperature from an HVAC system. The added features of these devices in comparison with traditional ones are the added programming allowed, self-learning algorithms of the consumption patterns, and intuitive interfaces with an easy user experience.
- **Smart Lights:** Smart lights are lighting devices that incorporate normal lighting with embedded technology that allow for automatic control. These products are equipped with sensors and microprocessors that can detect environmental light or occupancy and act upon prompts defined by the user. Smart lights allow users to adjust the lighting need by scheduling times and reduce over illumination, thus reducing the energy consumption associated with lighting. Due to its smart features, smart lights can be remotely controlled and even support demand response programs in response to inputs from energy utilities.
- **Smart Plugs:** Smart plugs are devices that come between an energy plug and an energy consumption appliance. These devices have the characteristic to turn non-smart appliances into smart ones due to the incorporated intelligent features. A smart plug allows for appliances connected to it to be remotely controlled and provides feedback on the energy consumption of the appliance.
- **Smart Hubs:** Smart hubs are devices that aggregate several smart connected devices within the smart home environment. The main objective of smart hubs is to integrate the functionalities of all these devices and communicate with all in a concerted way within a home network. Its interface includes hub display, web and smartphone applications, and it communicates via Wi-fi or blutetooth.

References:

Components of smart device and smart device interactions (n.d.). Citing sources. Retrieved on October 7, 2021, from https://www.researchgate.net/publication/252264581
IOT platform architecture (2018). Citing sources. Retrieved on October 7, 2021, from https://www.idglat.com/
Sadiku, M., (2019). *Emerging internet-based technologies.* CRC Press.
Serrenho, T. & Bertoldi, P. (2019). *Smart home and appliances: State of the art.* Publications Office of the European Union.