Chapter 2 IoT Network Architecture and Design

IoT Architecture: This is how data is supported, processed and communicated to the endpoints.

The design of IoT as it helps in scalability, management, adoption to changes and troubleshooting.

The IoT architecture is concerned with the operations of the systems whereas IT is concerned with the infrastructure that transports flows of any kind of data

1. Divers behind newtwork architecture

The difference between IT and IoT is how data is analyzed and transported along the intended devices.

The following are requirements that are driving new IoT architecture

1. Scale; the massive endpoints in IoT can only be met by using IPv6 unlike the use of IPv4 in IT like in NAT

2. Security; Exposure of the WSNs to the world, designing of endpoints with device level authentication.

3. Device with limited resources such as CPU, memory, speed; Wireless Network has to be designed to support these constrained devices.

4. Data Volumes; Distribution of data analytics from edge to cloud.

5. Legacy devices; Support for protocol translation over IP and ethernet.

6. Reat-Time analysis; Support for edge data analysis while designing.

2. Scale

Traditional IT Networks support a thousand devices but in IoT where millions of endpoints are interracting such architecture would break.

IoT introduces a model where a network can support a millions of endpoints and that is IPv6 which is the natural foundation of IoT network layer.

3. Security

Main concern of IT is protection of data against intrusion and theft. Perimeter firewalls are implemented but still hackers find the way to compromise data. However in IoT endpoints are located on the on the sensor networks making it more unsafe.

The IoT systems require consistent mechanism of authentication, encryption and intrusion prevention techniques

IoT Optimum Security;

1. Authenticate all entities involved in IoT e.g gateways, networks, service platforms.

2. Encrypt all the data that is being shared.

3. Comply with local data protection policy.

4. Management of IoT connection to detect anomalous behavior

5. Take holistic network-level approach.

3. Constrained Devices and Networks

Due to limited power, CPU and memory, the network connectivity provide lossy and support low data rates. Therefore IoT architecture needs a new connectivity technologies to meet both scale and constraint limitations.

4. Data; IoT generate lots of data that is vital to the businesses, Unstructured data can be revolutionarized so that insights can help create new business modls.

IoT are designed to to stagger data consumption by filtering and reducing unnecessary data going upstream and provide fastest response to devices.

5. Legacy Device Support

As the IoT is being deployed, the support for the older devices that are already present on the network.

Some older devices don’t support even IP but many of them support Protocols, so IoT must be capable of translating these older protocols or use a gateway to connect to these legacy endpoints to the IoT network

Comparing IoT Architectures

The concpt of comparing these architectures is to have understanding of how they support data, process and functions of the endpoint devices.

1. **One Machine to Machine (OneM2M)**

The devices communicating are programmed heterogenously using different systems, M2M provide a natural environment for these devices to interpolate through horizontal frameworks and RESTful APIs.

M2M architecture is made up of Application, Services and Network layers that promote interpolability.

2. **The IoT Reference Model.**

This architecture provides technical perspective of visualizing IoT such as edge computing, data storage and access.
It is made up of 7 layers; Physical, Connectivity,Edge Computing,Data Accumulation, Data Abstraction, Application and Collaboration & processes.
The IoT reference model separates the responsibilities along IT and IoT lines basing on queries, data and time.
The similarity between these models is that they have interconnected endpoints to the network to transport data by the application

A simplified IoT Architecture

This presents two parallel stacks which are intended to simplify the IoT architecture into basic building blocks to easy deployment in specific-usecase industries.

Core IoT Function Stack – It includes Things(Data mobility and transmission), Network(using gateways, topologies) and Appliations(interaction with smart objects).

IoT Data Management and Compute Stack – Provides a simplified way for objects to connect to a central cloud application where data is processed and analyzed.

These are built to be more scalable and efficient as objects generate large volumes of data that need to be analyzed in real time.

Data Center → Core Network → EndPoint.

Fog computing: Placing resources on network as near as possible to the object end-point.

Edge Computing: integrating processing resources in the IoT objects themselves

Chapter 3 Smart Objects ‘The Things’

These are physical objects that contain embedded tech interconnected and enabling communication amongst themselves in a meaningful way.

Example

A car has sensors of all types such as those for temperature, pressure, velocity and location. These are all aimed at providing data so as to improve safety and enhance maintenance.

The things in IoT include;

1. Sensors
2. Actuators
3. Smart Objects

1. Sensors

Sensor is a device that measures some physical quantity and converts it into a digital representational data which can be used by another device or humans.

Because of multidimensional sensing capability of these things, they can communicate externally and their environment thus making intelligent decisions

Categorizing sensors

- Active vs Passive whether a sensor produces an energy output or just receive the energy
- Invasive vs non-invasive; is sensor part of the environment it is measuring or just external
- Contact; Either sensors require physical contact with what they are measuring

Sensor Types basing on what they measure

- Position, either relative or absolute position like inclinometer, Potentiometer, proximity sensors.

- Occupancy and Motion, sense stationary or movement signals – Electric Eye, Radar.

- Force Sensor, measures magnitude of force e.g force guage,touch, viscometer sensor.

- Pressure. Measure pressure on liquids or gasses e.g Barometer and Bourdon Guage.. others are flow, humidity, light sensors.

- Light; These detect the presence of light e.g infrared, flame detector and photodetector.

Sensor Use cases – smart farming

Sensors can be seen in smart farming to improve efficiency, sustainability and profitability. This includes use of GPS and satellite aerial imagery to determine field viability.

-Robots can be used in planting, harvesting and during irrigation.

-Real-time analysis and artificial intelligence to predict optimal crop yield and soil quality(salinity and pH levels)

-All these provide analyzeable data which can lead to productivity and crop yield

Actuators

These are devices that receive controlled signals either electric or digital command which trigger physical effect usually motion or force.

What happens in actuator.

A processor sends a signal to a device that translates the signal into some type of movement or useful work whose change has a measurable impact on a physical world.

Actuators can be categorized basing on motion type, power, binary or continuous, area of application and type of energy

Actuators categorized depending on energy types

-Mechanical; Levers, screw jack, hand crank

-Electrical; diodes, biopolar transistor.

-Electromechanical; Ac, Dc, step motor,

-Electromagnetic; Magnets and Solenoid

-Smart Material; Ion,bimetallic strip.

Sensors provide information but actuators provide action, they both intelligently and complementary work together.

E.g Sensors used to evaluate soil quality connected to valve controlled devices that trigger water, pesticides and fertilizers based on well-defined sensor readings for smart farming

Micro-Electro-Mechanical System(MEMS)

These micro machines combine both sensors and actuators on a very small scale known as microfabrication thus allowing mass production at very low costs. They can be found in inkjet printers, smart phones, automobiles

Embedding of micro-scale sensors and actuators in everyday objects is going to be the trigger that is going to make IoT pervasively cut across all commercialized industries world-wide

Smart Objects.

These are building block of IoT with capability of transforming everyday objects into a network of intelligent objects that are able to learn from and interact with their envirnment in a meaningful way.

A sensor can be only revolutionary if it can be connected to a network of other sesors so that intelligently they can coordinate with actuators.

This intelligent network beteen several sensors and actuators unlock the power of IoT

Smart object is sometimes interchangeably called smart sensor, smart device, intelligent device and other names

Characteristics of a smart object

-Processing Unit: It has a unit for acquiring data, processing and analyzing information received by sensors, controlling signals to the actuators.

-Sensors or and Actuators: Should contain either of the two or both or multiple working intelligently depending on the application.

-Communication device: Ability to interact in form of a network. Most of IoT smart objects are connected wirelessly because of cost infrastructure and ease of deployment.

-Power Source: Flexibility in consuming power from various scavenger sources. This varies from application to application

Sensor Network

Effective coordination, communicaton in a productive manner of sensors and actuators such as seen in smart homes. Distribution of various sensors leads to wireless sensor networks(WSNs)

Advantages of wireless Network

- Flexibility in deployment in hard to reach places
- Simplicity in scaling large nodes
- Lower implementation costs
- Easier long-term maintenance
- Better equipped to handle dynamic topology changes
- Effortless introduction of new node(actuator or sensor)

Disadvantages of wireless based solutions

- Less secure

- Lower Transmission speeds

- Greater level of impact

Wireless Sensor Networks(WSNs)

Made up of wirelessly connected smart objects known as **motes**

Wireless SANETs are reffered to as WSANs or simply WSN since the network is overwhelmmed by sensors and actuators are just a part.

Design constraints of Wireless Smart Objects

- Moderate CPU power
- Lossy Communications
- Narrowband media
- Power consumption

Individual sensor nodes are limited so they are deployed in numbers. Smart objects with limited processing, memory and power are called constrained nodes.

Deployment of many sensors gives ability to aggregate similar readings from close sensor nodes.

This data aggregation helps to reduce traffic in WSN.

The communication patterns of Smart Objects are Event-Driven, Periodic patterns,

Communication Protocols for WSNs

WSNs are moving from homogeneous networks(Made up of single sensor type) to networks made up of multiple sensor types that can mix between cheap and a few expensive ones.

WSNs are transitioning from single-purpose networks to multipurpose networks

Any communication protocol must deal with the inherent characteristics of WSNs like scalability, power and speed of transmission, security.

Sensors produce large data that needs to be processed, protocols need to define how this data is routed and flowed among the sensor nodes

These protocols provide a platform for a variety of IoT smart services.

These protocols have to be standardized which is a complicated task across multiple layers of the stack and across multiple industries.