# 7.1t:transcript

Some of this today is going to sound like a weather forecast, we’re going to talk about Fog and Cloud. And how they relate to IoT.

It is estimated that by the end of 2020 will be 30 billion IoT devices worldwide, and in 2025, the number will exceed 75 billion connected things,

All these devices will produce huge amounts of data that will have to be processed quickly and in a sustainable way. To meet the growing demand for IoT solutions, fog computing comes into action on par with cloud computing

We’ve already got used to the technical term cloud, as we’ve discussed is a network of multiple devices, computers and servers connected to each other.

We can divide this into two part

The frontend — consists of client devices (computers, tablets, mobile phones).

The backend — consists of data storage and processing systems (servers) that can be located far away from the client devices and make up the cloud itself.

This is where FOG, comes in.

FOG computing is also known as Edge computing.

Distributed intelligence, with real time response. Usually connected 3G/4G/5G WiFi etc.

Cloud – Hundreds of devices

Core Network – Thousands of Devices

Fog Network – Tens of Thousands of devices

Smart things - IoT – Millions of devices

The term fog computing or fogging was coined by Cisco in 2014.

Fog and cloud computing are interconnected.

In nature, fog is closer to the earth than clouds; in the technological world, it is just the same, fog is closer to end-users, bringing cloud capabilities down to the ground.

If we were to give a definition of Fog we could say fog is the extension of cloud computing that consists of multiple edge nodes directly connected to physical devices.

CISCO designed a six pillar model, we’ll return to this in more detail later.

FOG nodes are physically much closer to devices if compared to our cloud systems, which is why they are able to provide instant connections.

The considerable processing power of edge nodes, FOG nodes, allows them to perform the computation of a great amount of data on their own, without sending it to the cloud.

Fog can also include cloudlets — small-scale and rather powerful data centres located at the edge of the network.

Their purpose is to support resource-intensive IoT apps that require low latency.

The main difference between fog computing and cloud computing is that cloud is a centralised system, while the fog is a distributed decentralised infrastructure.

Fog computing is a mediator between hardware and cloud servers.

It regulates which information should be sent to the server and which can be processed locally.

In this way, fog is an intelligent gateway that reduces data returning to the cloud enabling more efficient data storage, processing and analysis.

It is important to note that fog networking is not a separate architecture and it doesn’t replace cloud computing but rather complements it, getting as close to the source of data as possible.

The FOG technology is going to have the greatest impact on the development of IoT, embedded AI and 5G solutions, as they, like never before, demand agility and seamless connections.

The fogging approach has many benefits for the Internet of Things, plus other technologies such as AI.

But why do we need FOG?

* Low latency (fog is geographically closer to users and is able to provide instant responses)

* No problems with bandwidth (pieces of information are aggregated at different points instead of sending them together to one centre via one channel)

* Loss of connection is impossible (due to multiple interconnected channels)

* High security (because data is processed by a huge number of nodes in a complex distributed system)

* Improved user experience (instant responses and no downtimes satisfy users)

* Power-efficiency (edge nodes run power-efficient protocols such as Bluetooth, Zigbee or Z-Wave)

All this sounds great, but like many things in computing there are downsides, we are now introducing a more complex system.

Obviously extra equipment, new expertise is going to cost.

And FOG has limited scalability, it’s not as scalable as Cloud!

Cloud and Fog concepts seem very similar, but there are differences.

Cloud architecture is centralised and consists of large data centres that can be located around the globe, a thousand miles away from client devices. Fog architecture is distributed and consists of millions of small nodes located as close to client devices as possible.

Fog acts as a mediator between data centres and hardware, and hence it is closer to end-users. If there is no fog layer, the cloud communicates with devices directly, which is time-consuming.

In cloud computing, data processing takes place in remote data centres. Fog processing and storage are done on the edge of the network close to the source of information, which is crucial for real-time control.

Cloud is more powerful than fog regarding computing capabilities and storage capacity.

The cloud consists of a few large server nodes. Fog includes millions of small nodes.

Fog performs short-term edge analysis due to instant responsiveness, while the cloud aims for long-term deep analysis due to slower responsiveness.

Fog provides low latency; cloud — high latency.

A cloud system collapses without an Internet connection. Fog computing uses various protocols and standards, so the risk of failure is much lower.

Fog is a more secure system than the cloud due to its distributed architecture.

It’s the Fog architecture that will unleash the power of IoT, Fog computing and IoT are intertwined. And Fog and Cloud are intertwined.

I’m sure many of you are familiar with the term IoT, but we should start with a clear idea what IoT is.

The IoT is a network of physical objects such as wearable

Devices like a smart watch, home appliances a TV, a fridge or even a kettle, security systems, personal and commercial vehicles, nanotechnology, manufacturing equipment, and many more embedded with smart components such as microcontroller, data storage, software, sensors, and actuators.

These can also be connected to other devices and systems over the Internet.

In the smallest sense the “thing” may be an individual component, such as a smart light bulb in an office, or the building the office is in, as an item in a portfolio of assets being tracked.

The value of the IoT is in the data that is collected and then analysed to provide insights or actions, this is where Fog is so important to us.

I mentioned a few IoT devices a moment ago, some obvious some not so obvious.

Let’s just quickly go over the not so obvious ones!

Let’s start with sensors.

A sensor is a device that detects and responds to some type of input from the physical environment.

The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena.

The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing.

For an IoT Fog perspective it’s the data over the network we’d be interested in.

Obviously have sensors are very useful to us, but it would be good if we could alter the environment that was being sensed.

For example, if we were monitoring water flow, the sensor might tell us that more water is needed.

We could manually alter the valve controlling the flow, but it would be much better if the valve could be controlled by something other than us.

This is where an actuator comes in, an actuator is a device that moves or controls some mechanism. It turns a control signal into mechanical action such as an electric motor.

Actuators may be based on hydraulic, pneumatic, electric, thermal or mechanical means, but are increasingly being driven by software.

An actuator ties a control system to its environment.

The final part of this is microcontroller, this is the ‘smart’ in smart devices.

Microcontrollers can be thought of as tiny computers that are added to any physical object or space to give it some processing capability.

 They contain one or more computer processors, along with memory and programmable input/output peripherals all in a single integrated circuit.

They are different from the microprocessors that are found in personal computers because they are specifically designed for embedded applications where computing is not the sole purpose of the application.

While microcontrollers have less capability than a standard computer processor, their low cost makes them a more practical option for adding computing capabilities to an object, space, or process that doesn’t have them, the IoT environment

Before we continue we really do need to take note of Botnets.

Botnets have become one of the biggest threats to security systems today. Their growing popularity among cybercriminals comes from their ability to infiltrate almost any internet-connected device.

A size of a Botnet matters, the larger the better, remember what I said at the start 75 billion devices by 2025 ! Ok not all will be under control of one BotMaster, but a fair quantity could be implemented incorrectly.

Botnets can infect almost any device connected directly or wirelessly to the internet. PCs, laptops, mobile devices, DVR’s, smartwatches, security cameras, and smart kitchen appliances can all fall within the web of a botnet.

They can cause devastating Distributed Denial of Service Attacks

As said we’d come back to this, In 2015, Cisco introduced a suite of integrated and coordinated products known as the Cisco IoT System.

Cisco IoT System addresses the complexity of digitization with an infrastructure that is designed to manage large-scale systems of diverse endpoints and platforms, and the flood data they create.

The system consists of six critical technology pillars that, when combined together into an architecture, help reduce the complexities of digitization.

Let’s look at each of the pillars.

Network connectivity: Includes purpose-built routing, switching, and wireless products, these are designed for different environments and can be obtained in either rugged or non-rugged forms.

Fog computing: Provides Cisco’s fog computing, or edge data processing platform, IOx.

Data analytics: An optimized infrastructure to implement analytics and harness actionable data for both the Cisco Connected Analytics Portfolio and third-party analytics software.

As you can see the next pillar is security,

Security: Unifies cyber and physical security to deliver operational benefits and increase the protection of both physical and digital assets.

Cisco’s IP surveillance portfolio and network products with TrustSec security and cloud/cyber security products allow users to monitor, detect and respond to combined IT and operational technology attacks.

Management and automation: Tools for managing endpoints and applications.

Application enablement platform: A set of APIs for industries and cities, ecosystem partners and third-party vendors to design, develop, and deploy their own applications on the foundation of IoT System capabilities.

A final architecture we need to be aware of was designed by the IoT World Forum, the IWF.

This model serves as a common framework to help the industry accelerate IoT deployments. The reference model is intended to foster collaboration and encourage the development of replicable deployment models.

The IWF model gives us a systems that help simplify by breaking down complex systems.

Clarifies by provides additional information.

Identifies where specific types of processing is optimized across different parts of the system.

It gives standardisation, by providing a first step in enabling vendors to create IoT products that work with each other.

And it Organizes It, making the IoT real and approachable, instead of simply conceptual.