FOG COMPUTING

Your Journey into the Cold Wet Beyond Starts Here

OUR TEAM


Jeremy Hansen
Failed art class, took home the crayons.
Yu Chen
Cat Herder
Justin Hoy
Master Procrastinator
Brad Robinson
Risk Manager

TABLE OF CONTENTS

KEY ASPECTS

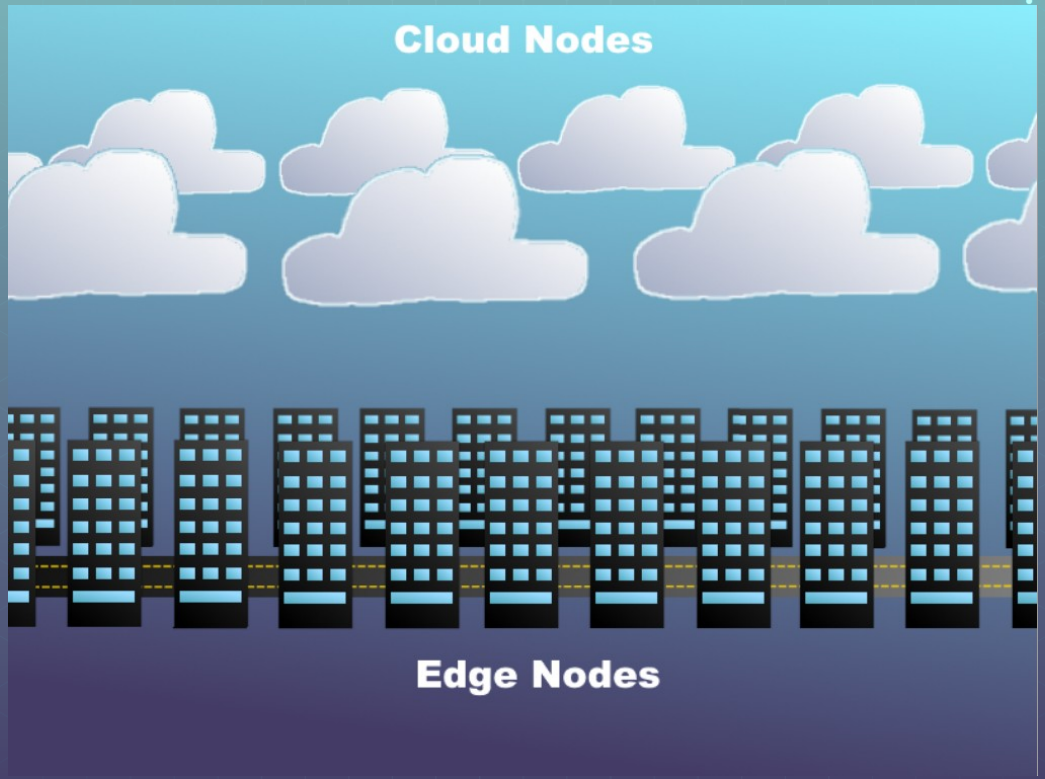
Poll Question 1:

What do you know about cloud computing?

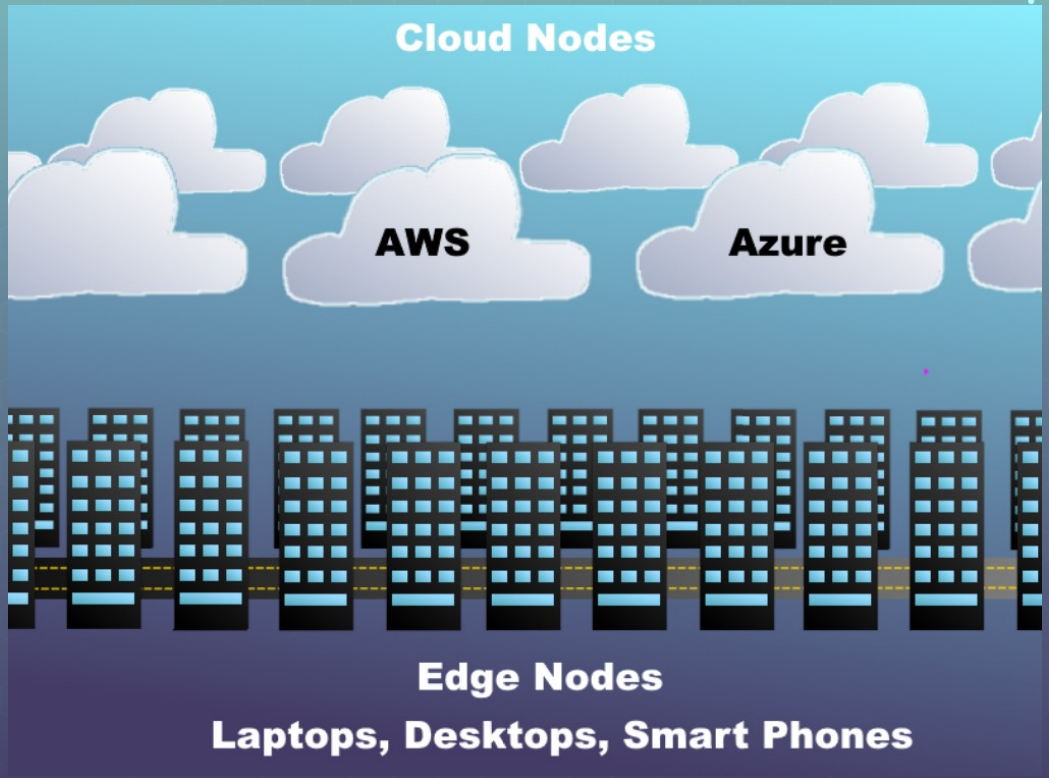
Please take a minute to answer the question on Smart Learning Suite.

Fog Computing - Key Aspects

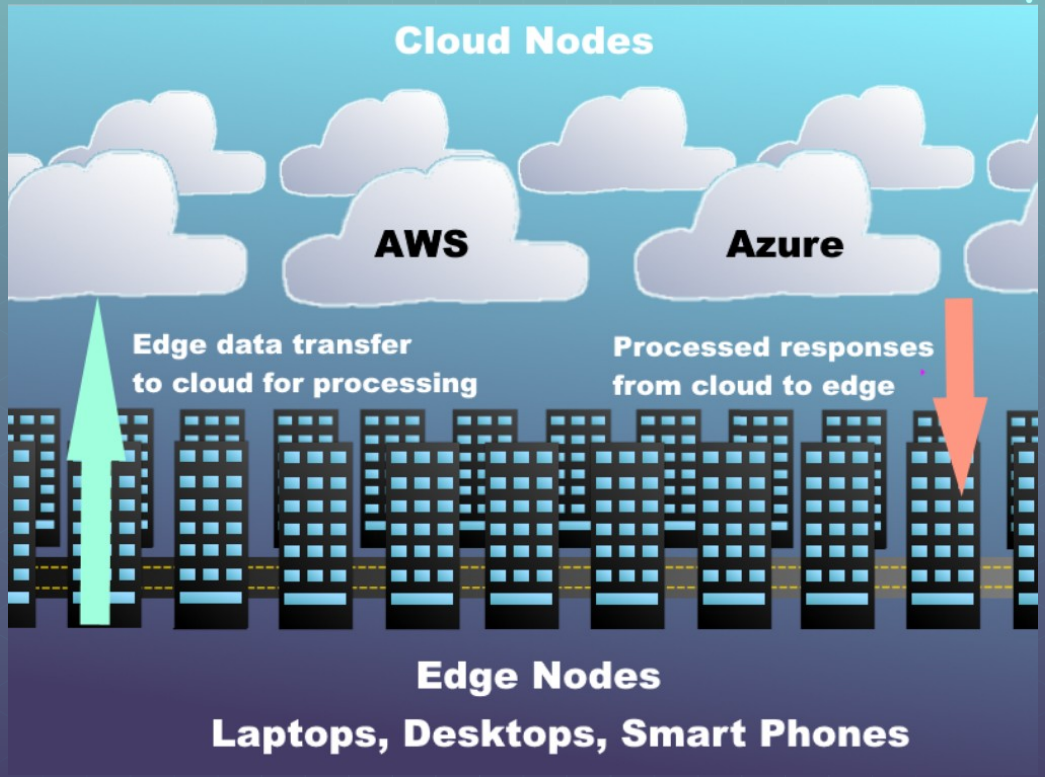
Fog Computing - Key Aspects



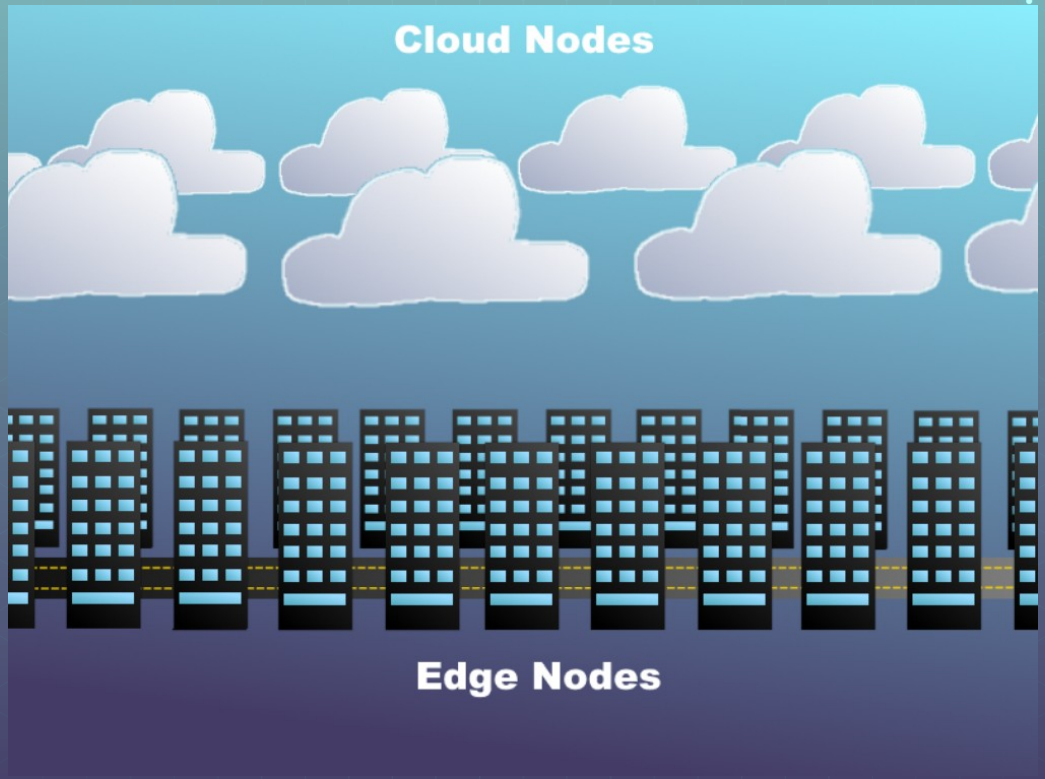
Fog Computing - Key Aspects



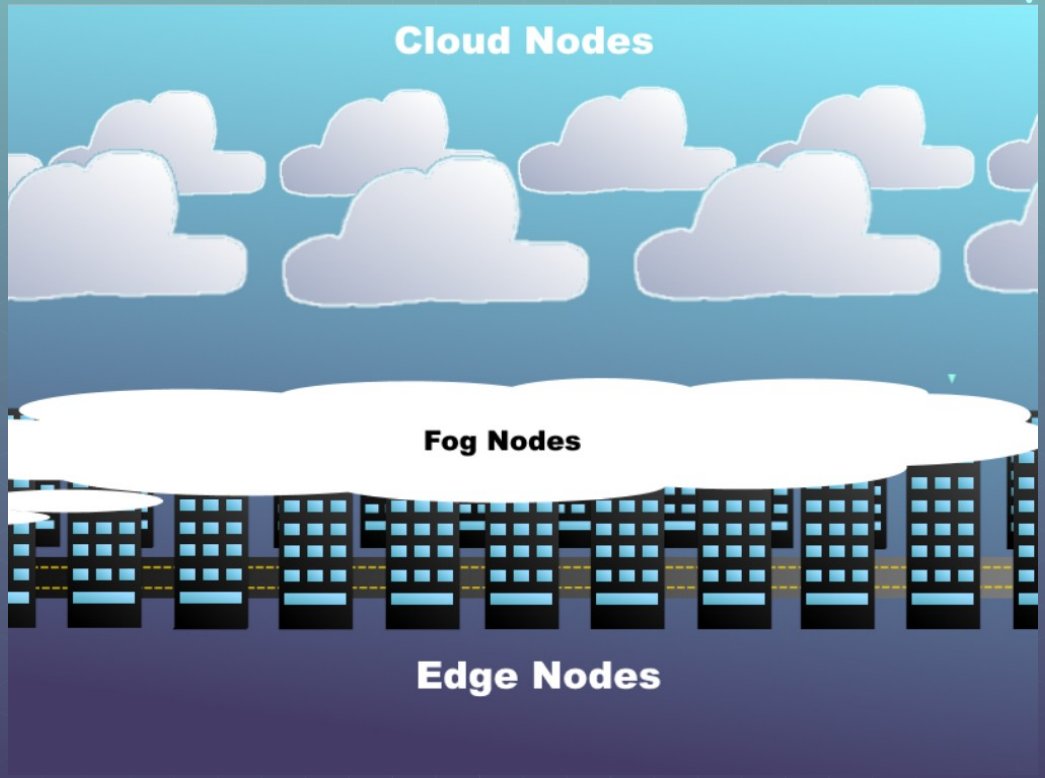
Fog Computing - Key Aspects



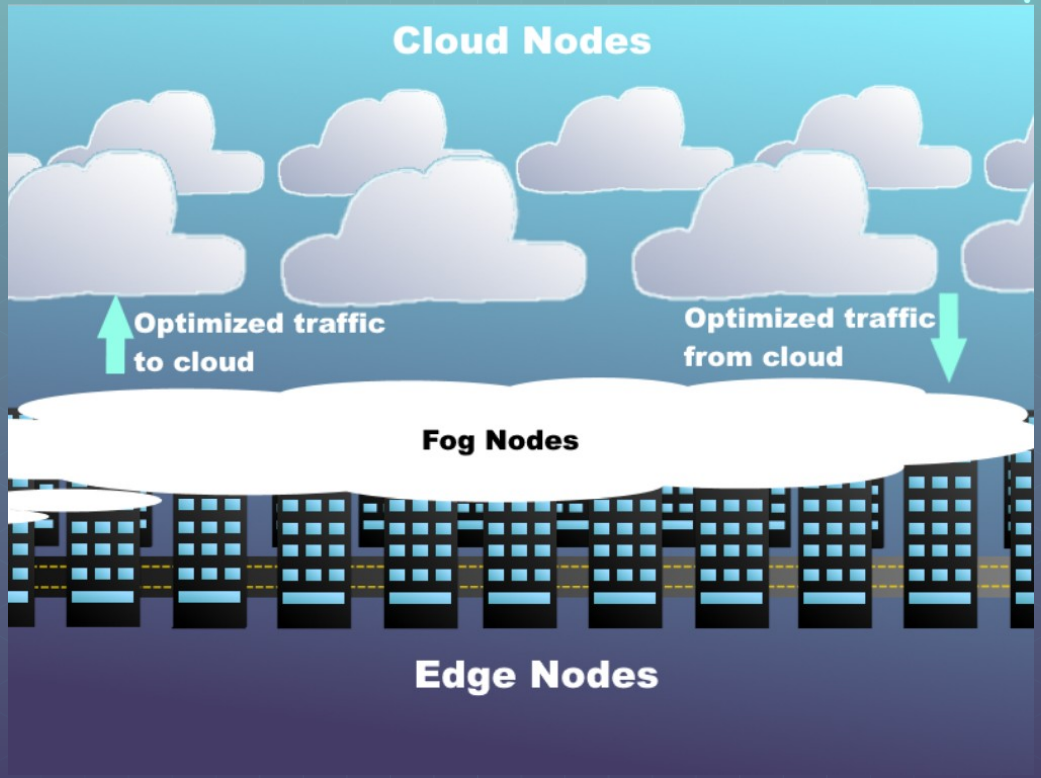
Fog Computing - Key Aspects



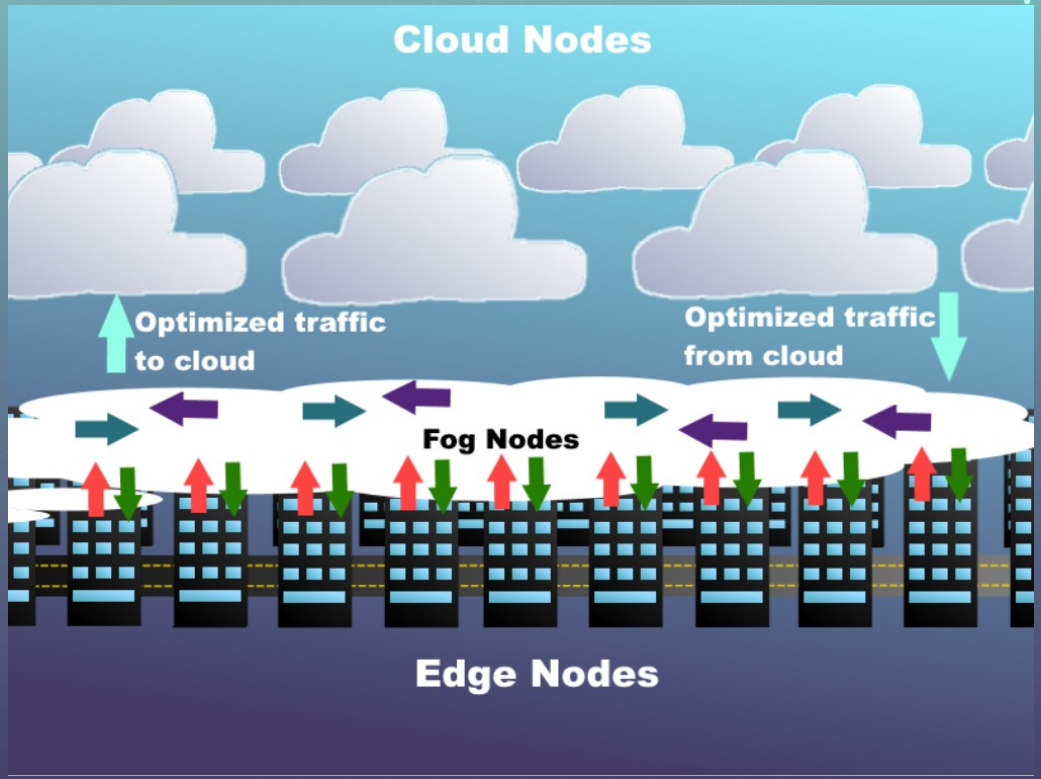
Fog Computing - Key Aspects



Fog Computing - Key Aspects



Fog Computing - Key Aspects



Key Aspects - Coexistence

Aspect	Fog Computing	Cloud Computing
Latency	Low	High
Geo Location	Local to data source	Remote from data source
Availability	Volatile but highly redundant	99.99% (guaranteed)
Processing Potential	Scalable but potentially volatile	Scalable
Use	Detailed processing of high volume, time-	Wide area aggregation of lower volume, less time-

Adapted from: [1] Mahmood, Zaigham. Fog Computing Concepts, Frameworks and Technologies. 2018. Web.

Interaction Activity

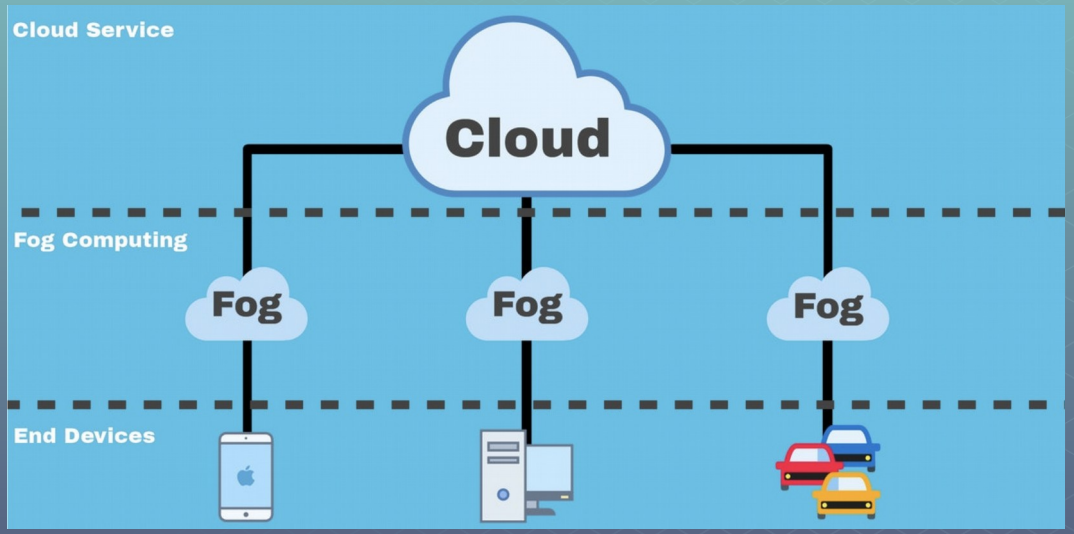
APPLICATIONS

Cloud Model

[2] Source: https://www.fastmetrics.com/blog/tech/what-is-cloud-computing/

- Cloud computing provide great scalability, cost reduction, mobility, and control, and can process and mine large data sets
- However, it‘s sometimes too far to process data and respond in real time
- Can be a problem in certain environments where operations require instant response, or where internet connectivity is less than ideal

Solution? Fog Model



[3] Source: https://www.itprc.com/fog-computing/

- Place servers (fog devices) closer to the end users. They react quickly to changes in the streaming data coming from the end user. They can also request certain computations to take place in the cloud servers, and interact with other fog devices located in different areas.
- Huge value in access to real-time information and analytics, which helps businesses and individuals make critical split-second decisions.

Scenarios

VEHICULAR COMMUNICATIONS

Using the cameras, GPS, radar and other sensors as fog nodes to gather and process data to realize real-time driving, smart traffic lights, etc.

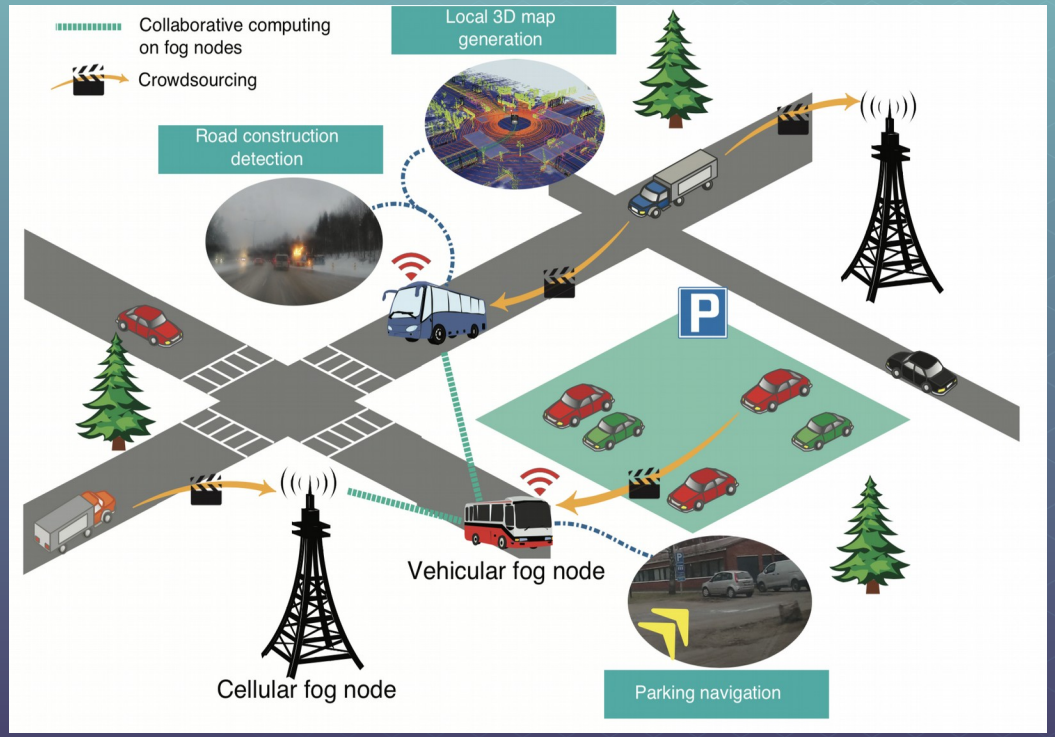
SMART GRID

An improved distribution network of electricity using information and communication technology (ICT)-based infrastructure to save energy.

Health Monitoring System

An IoT-based healthcare system used for acquiring different vital signs such as ECG, EMG, body temperature, blood pressure in a real-time, unobtrusive and efficient way.

Vehicular Communications



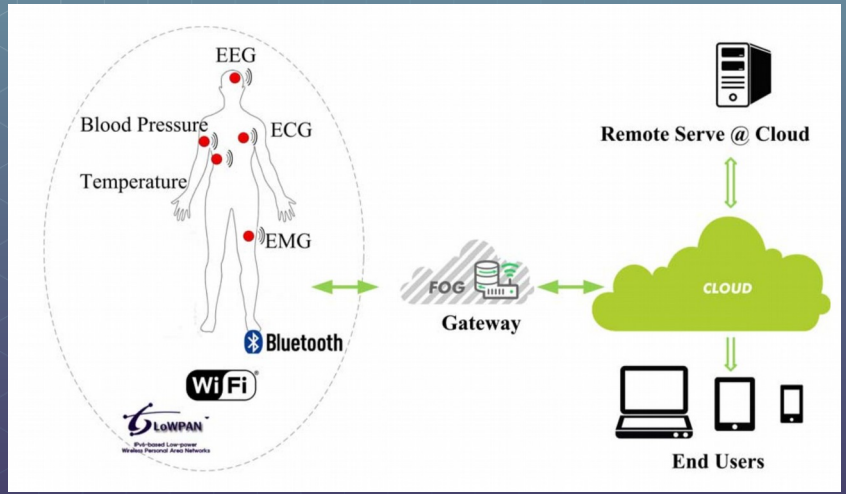
- 2 Type of Fog Nodes: Cellular & Vehicular - Dash cameras capture important details of the environment outside of the vehicles, radar, GPS
- Big Volume of data especially from video
- Use case by update cycle:

  *Short cycle: Driving assistance, smart traffic lights

  *Moderate to long cycle: Parking assistance, infrastructure improvement recommendations, crime scene reconstruction

Health Monitoring

- Implantable or wearable sensor nodes to collect and transmit the data over a wireless network via communication protocols
- Smart Fog Gateway Example: ECG feature extraction for preliminary assessment
- Real-time notification and location awareness



[4]

TECHNICAL DEMONSTRATION

iFogSim

- We need an evaluation platform that enables the quantification of resources within an IoT or Fog computing infrastructure
- Thus we introduce the most widely used fog simulator, an extension of the well-known CloudSim [10] simulator built at the Cloud Computing and Distributed Systems lab in the University of Melbourne
- Used to model IoT and Fog environments and measure the impact of resource management techniques in terms of latency, network congestion, energy consumption, and cost

Architecture

- The architecture of Fog computing environment in iFogSim is comprised of multiple layers, with each layer responsible for specific tasks to facilitate operation of higher layers.

- The bottommost layer comprises of IoT devices that is those that interact with real world and are the source of data

Every device in the Fog Network can be represented by 2 types:

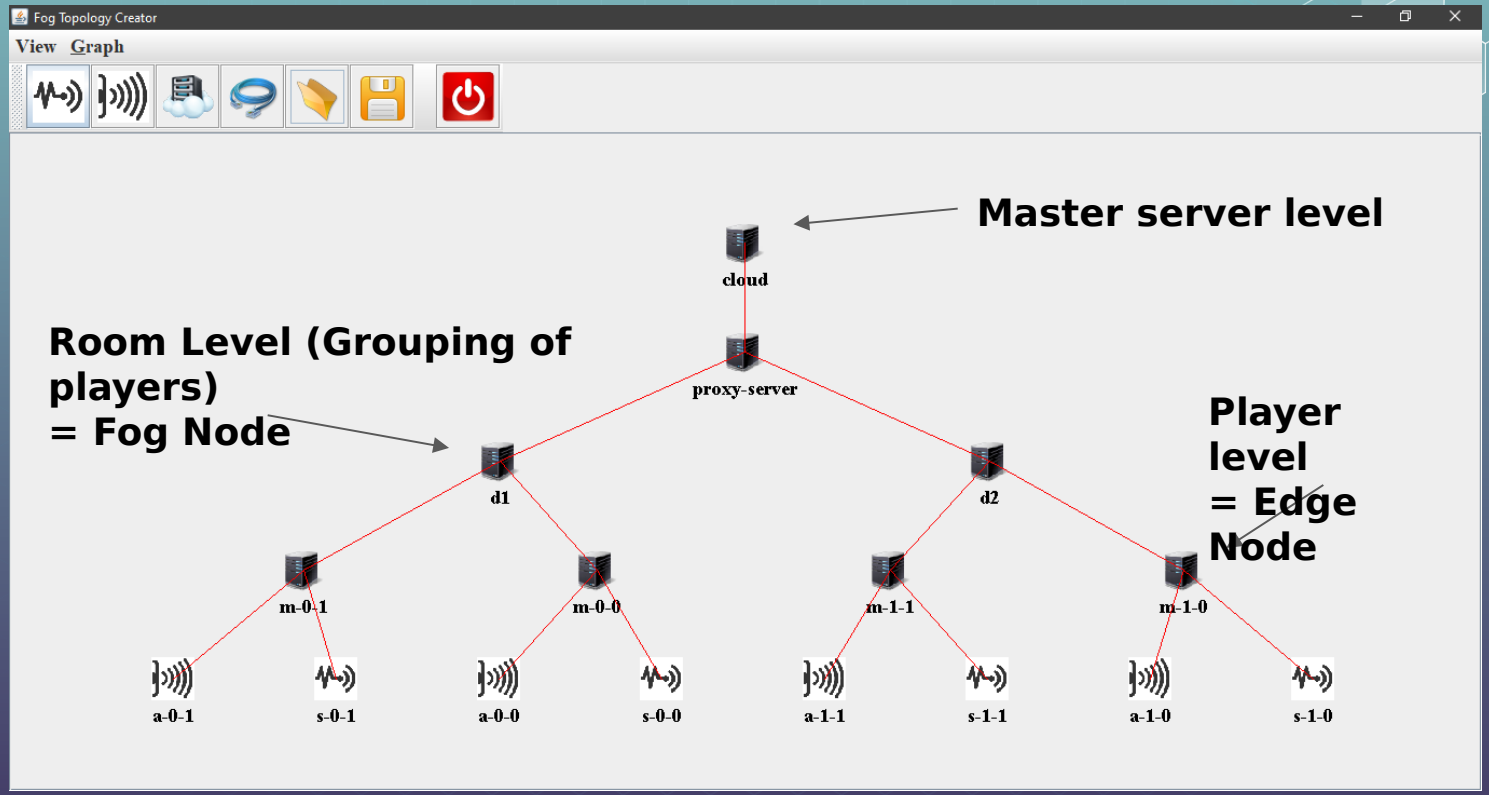
Sensors: act as the source of data for applications and are distributed in different geographical locations, sensing the environment and emitting observed values to upper layers via gateways for further processing.

Actuators: operate at the bottommost layer of the architecture and are responsible for controlling a mechanism or system. Actuators are usually designed to respond to changes in environments that are dictated by applications on the basis of information captured by sensors

VR Game Example

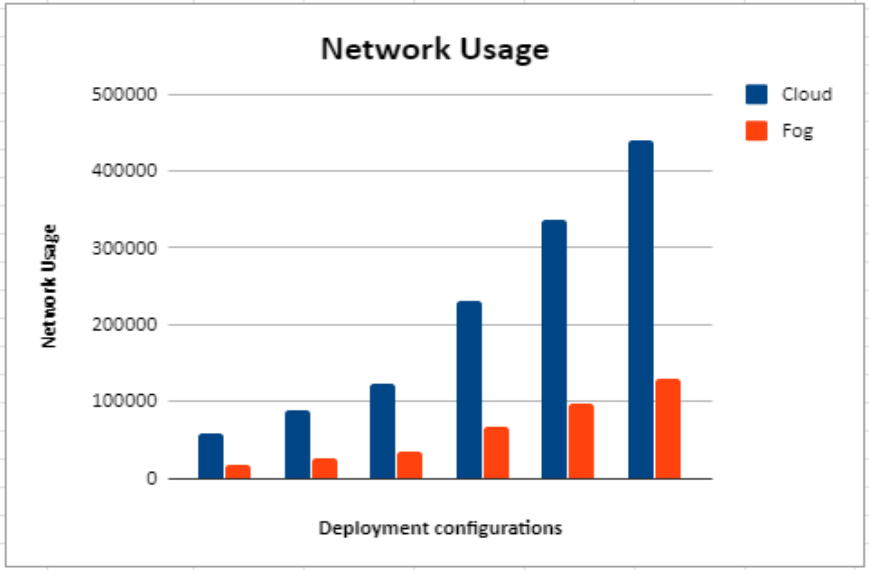
- A simulation of a latency sensitive smartphone multi-component application which allows player to interact with one another through EEG sensors (device used to record electrical activity of the brain)
- To allow players to interact in real time, the application demands a high level of quality of service (ie. minimum latency) between components
- The infrastructure to host the application consists of a single cloud node, an ISP proxy, several gateways, and smartphones (actuators) connected to EEG sensors

Topology


Fog Topology Creator
View Graph
Master server level
cloud
Room Level (Grouping of players)
= Fog Node
proxy-server
Player level
= Edge Node
d1
d2
m-0-1
m-0-0
m-1-1
m-1-0
a-0-1
s-0-1
a-0-0
s-0-0
a-1-1
s-1-1
a-1-0
s-1-0

iFogSim Technical Demo

	A	B	C	D
1	Number of rooms	Users/room	Cloud	Fog
2	2	4	58346.82	17947.2
3	3	4	89113.06	25940.8
4	4	4	122227.78	33934.4
5	4	8	230406.54	65908.8
6	4	12	336674.24	97883.2
7	4	16	440946.86	129857.6



- Increasing the amount of rooms (WIFI gateways) and players increases the overall load on the entire network and thus increasing the latency between layers.

- However we notice that in a cloud network the usage is larger, which makes sense as we are propagating more data between layers, opposed to fog which seeks to eliminate this by using intermediate nodes to do computations upfront.

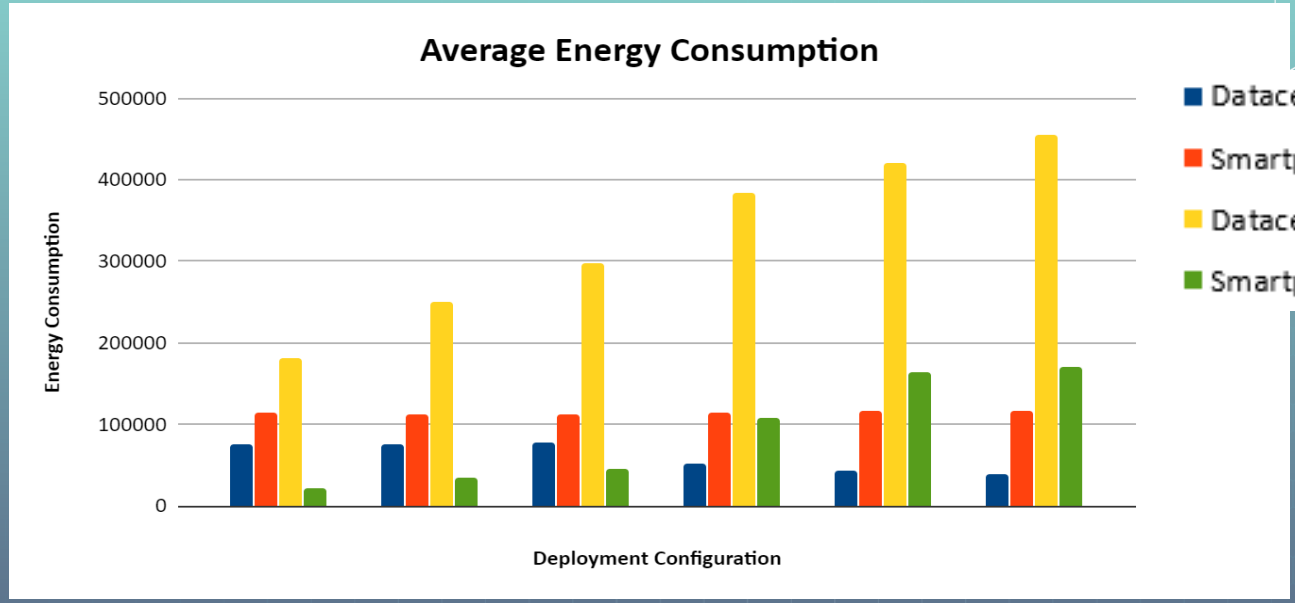
- In general, uncontrolled growth of a network in a cloud-based execution can lead to network congestion and can exponentially degrade an application's performance.

- With cloud, these modules are separated by links with long-latency and leading to high degree of network use

- Such situations can be better avoided if a fog-based straegy is adopted where information is preprocessed closer to the source of data. The computations are prioritized on the gateways—thereby reducing the effective network use.

	A	B	C	D	E	F
1						
2	Number of rooms	Users/room	Cloud	Fog	Cloud	Fog
3	2	4	75420.01107	114457.3839	181781.4488	22560
4	3	4	76376.50718	111766.6816	251352.913	33840
5	4	4	76727.95638	112704.3602	298739.6404	45120
6	4	8	51485.18903	114932.4936	383015.442	108570
7	4	12	42896.29049	115610.5323	420059.7107	163090
8	4	16	39337.77175	117126.3227	454863.577	170610
9						
10			Datacenter in Fog execution	Smartphone in Cloud execution	Datacenter in Cloud execution	Smartphone in Fog execution

- The tradeoff comes at a price. By increasing the amount of players in a fog environment, you reduce energy consumption of cloud data centers while slightly increases energy consumption of edge devices



- So the question then becomes whether to put a priority on better latency and better game experience at the lost of lower battery life for your players.

- Note that the energy consumption of each device type is the sum of energy consumption of all devices belonging to that type.

RISKS & CHALLENGES

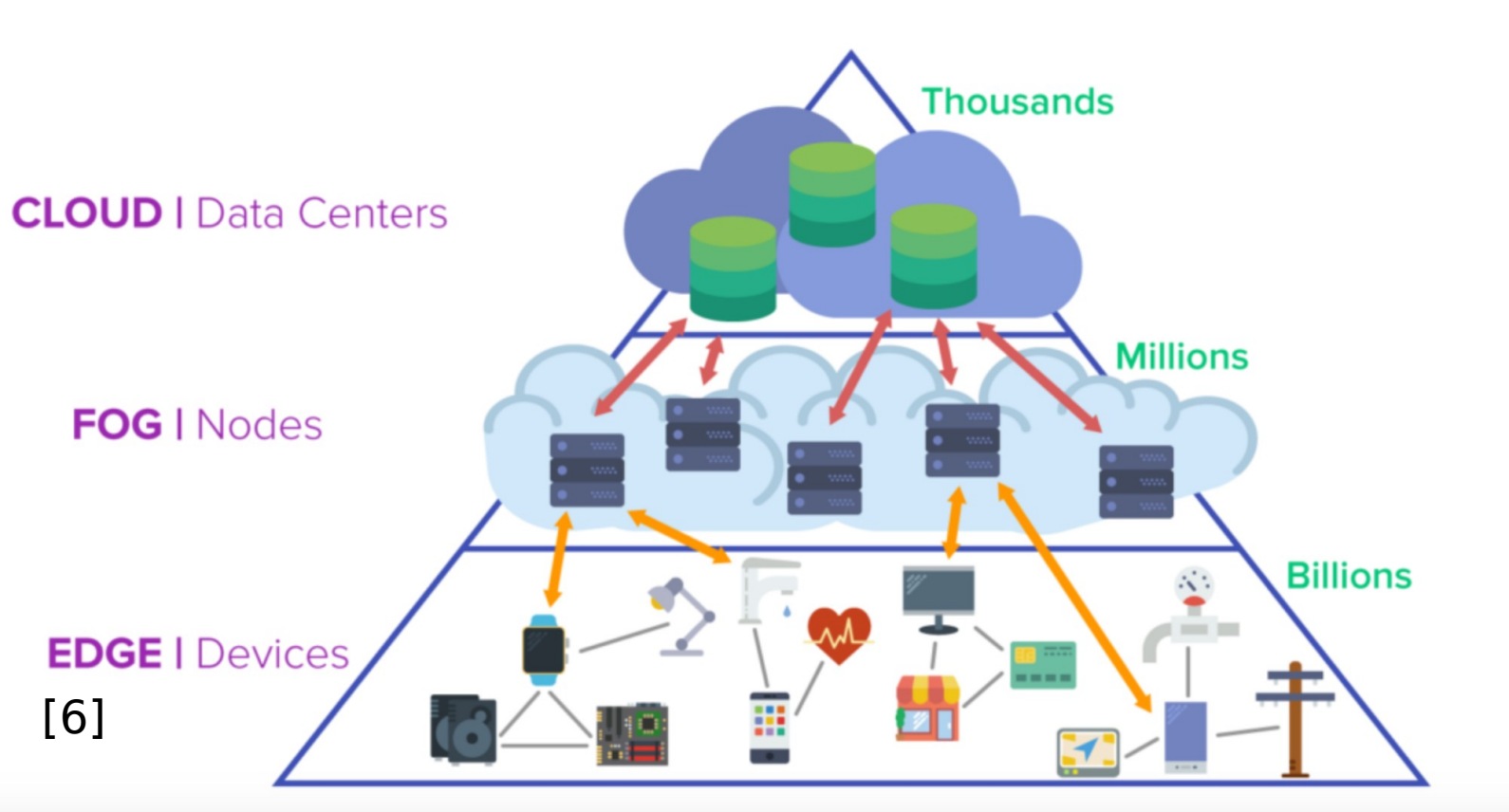
RISK & CHALLENGES

“As a growing number of communication devices join the internet we will soon face a foggy and cloudy world of interconnected smart devices” [5]

In General the Challenges are:

- **PRIVACY/LEGAL**
- **IMPLEMENTATION**
- **ENGINEERING**
- **SECURITY**

RISK & CHALLENGES



[6]

RISK & CHALLENGES

PRIVACY CHALLENGES:

EU has implemented the General Data Protection Regulation

- **PERSONAL DATA**
  any data relating to an identifiable person
- **DATA SUBJECT**
  a natural person
- **CONTROLLER**
  natural or legal person who determines the conditions for processing data
- **PROCESSOR**
  natural or legal person who processes data on behalf of

[5]

RISK & CHALLENGES

PRIVACY CHALLENGES:

General Data Protection Regulation :

“DATA PROTECTION BY DESIGN”

- **Controller will implement procedures to protect rights of the data subject**
- **Processor has a legal contract with the Controller**
- **Processor will take all required measures to assist controller in ensuring compliance with GDPR**

[5]

RISK & CHALLENGES

PRIVACY CHALLENGES:

General Data Protection Regulation :

- **PSEUDONYMIZATION** of data so it cannot be attributed to a particular person
- **LIMITATIONS** to data quality and duration of storage based on necessity
- **CONSENT** by data subject must be given and can be withdrawn at any time
- **RIGHT TO BE FORGOTTEN** when the data is no longer required for the purpose it was collected

[5]

RISK & CHALLENGES

IMPLEMENTATION CHALLENGES:

- **Who owns and operates the FOG servers?**
- **XaaS i.e. Infrastructure as a service**
- **“Indie FOG”**
- **Scheduling of network resources difficult because of sheer number of IoT devices**
- **Large number of FOG nodes means some will fail - SDN software defined network could be disrupted**
- **End devices have limited battery**

[7]

RISK & CHALLENGES

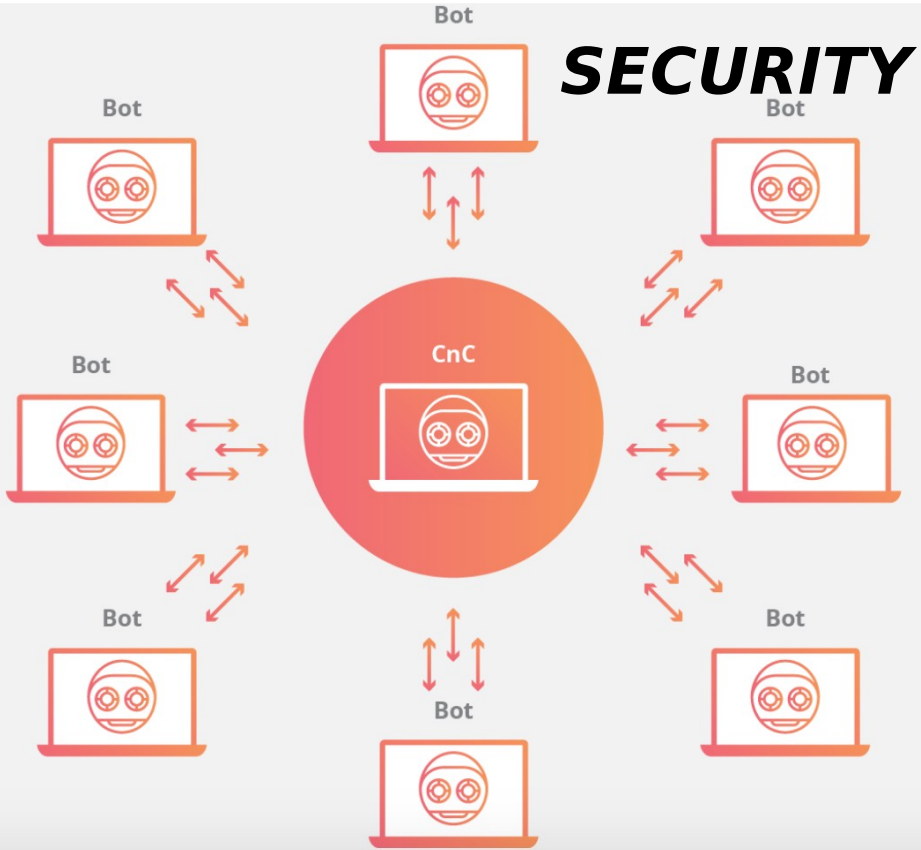
ENGINEERING CHALLENGES:

- **Devices are mobile and must move from one FOG node to another - how is this engineered?**
- **Complex with many devices many interactions**
- **integrating 5G likely important**
- **Possibly Bell and other CSP's offer XaaS**
- **SDN software defined networks enable downloading 5G traffic to local FOG node**
- **CRAN cloud radio access network enabled by cell networks**
- **FRAN fog radio access network enabled**

[8]

RISK & CHALLENGES

SECURITY CHALLENGES



[9]

RISK & CHALLENGES

SECURITY CHALLENGES:

- **IPv6 network layer protocol means most IoT devices (BILLIONS) can have an IP address and may be vulnerable a network security breach**
- **DDoS distributed denial of service attack, eg MIRAI bot attacks**
- **AES advanced encryption standard to secure communication between devices**
- **Datagram Transport Layer Security or lightweight security algorithms**
- **ML to recognize security breaches and react in real-time**

[10]

Bibliography

[1] Mahmood, Zaigham. Fog Computing Concepts, Frameworks and Technologies. 2018. Web.

[2] What Is Cloud Computing & How Does It Work? access on Nov.30, 2019 [Online]. Available: https://www.fastmetrics.com/blog/tech/what-is-cloud-computing/

[3] access on Nov.30, 2019 [Online]. Available:https://www.itprc.com/fog-computing/

[4] Tim Keary,"What Is Cloud Computing" access on Nov.30, 2019 [Online]. Available: https://www.itprc.com/fog-computing//

[5] Gia, T.N., Jiang, M., Rahmani, A.M., Westerlund, T., Liljeberg, P. and Tenhunen, H., 2015, October. Fog computing in healthcare internet of things: A case study on ecg feature extraction. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 356-363). IEEE.

[6] G.Gultekin Varkonyi, Sz. Varadi, Atilla Kertez, "Legal Aspects of Operating IoT in the Fog", in Fog and Edge Computing: Principles and Paradigms, R. Buyya and S.N. Srirama Eds. John Wiley & Sons Incorporated, 2019, pp. 411-431.

[7] Real Time API, "edge computing for beginners " accessed Nov 29, 2019,[Online]. Available: http://realtimeapi.io/edge-computing-for-beginners.com.

[8]] Ahmit Cihat Baktir, et.al., "Addressing the Challenges in Federating Edge Resources", in Fog and Edge Computing: Principles and Paradigms, R. Buyya and S.N. Srirama Eds. John Wiley & Sons Incorporated, 2019, pp. 25-45.

[9]] Adel Nadjaran Toosi, et.al., "Management and Orchestration of Network Slices in 5G, Fog, Edge and Cloud", in Fog and Edge Computing: Principles and Paradigms, R. Buyya and S.N. Srirama Eds. John Wiley & Sons Incorporated, 2019, pp. 79-96.

[10] IoT for AlII, "Mirqi Botnet DDoS " accessed Nov 29 2019,[Online]. Available: http://iotforall.com

THANKS