SEOULTECH

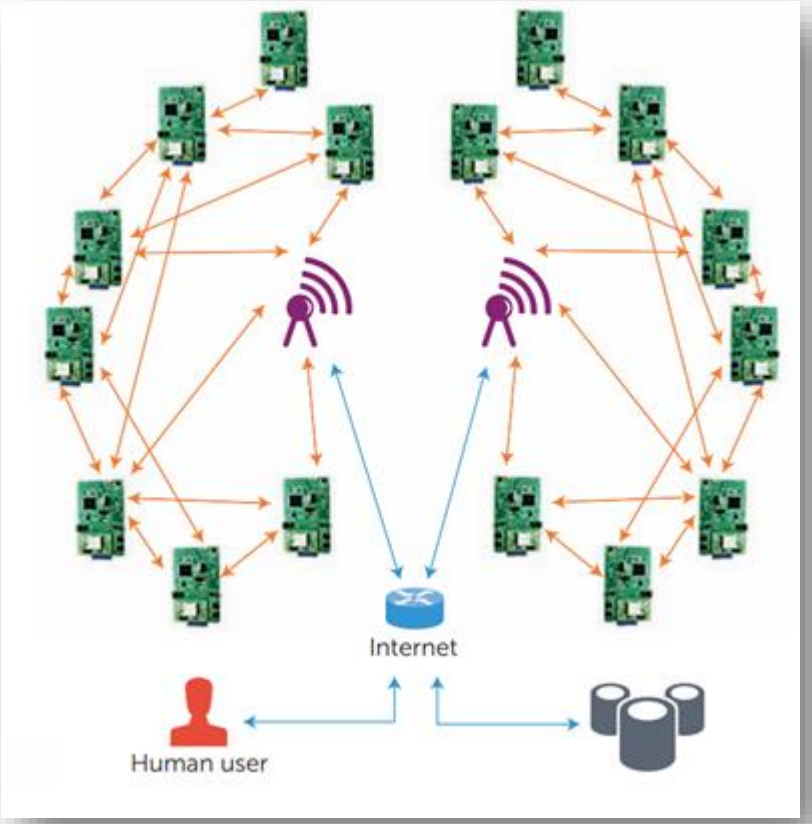
UCSLAB
Ubiquitous Computing & Security Laboratory

CHALLENGES OF CONNECTING EDGE AND CLOUD COMPUTING: A SECURITY AND FORENSIC PERSPECTIVE

2017. 11. 06
Presented by
Pradip Kumar Sharma
(pradip@seoultech.ac.kr)

TRADITIONAL WSN ARCHITECTURE

- A sensor network consists of tiny sensing devices deployed within an area of interest,
  - Such as a forest, within a building or along a motorway, to measure certain environmental factors,
  - Such as temperature, humidity, vibrations, pollution and so on.
- Such devices are typically only capable of computing simple tasks on the collected data,
  - such as simple aggregation and filtering operations,
  - and sending the collected information to base stations using short-range wireless communications.

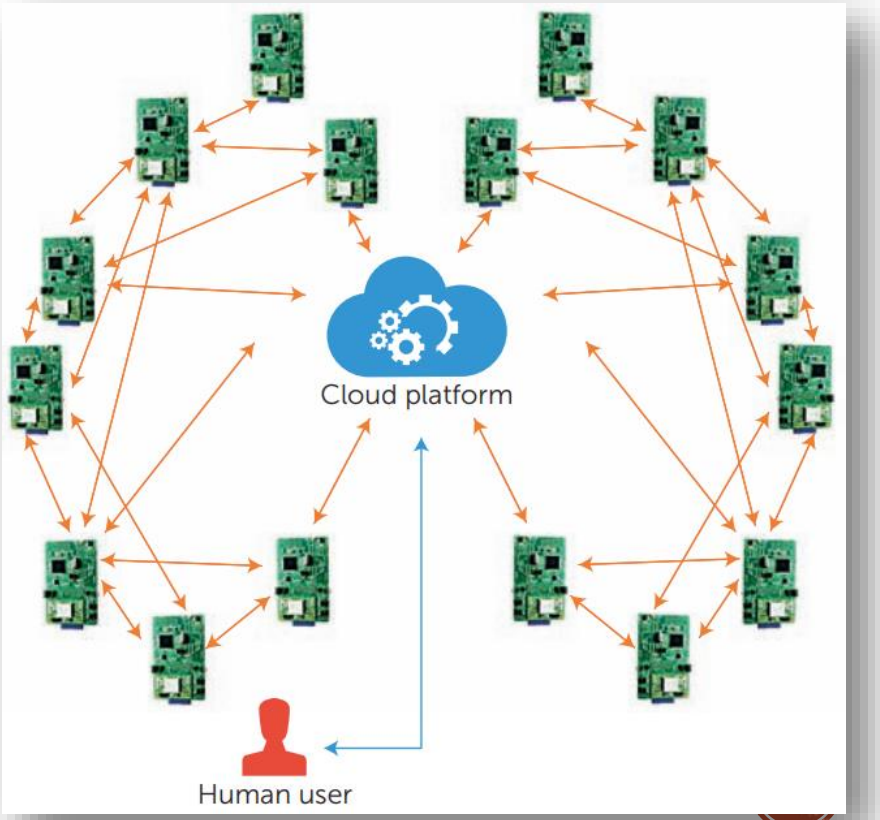


IOT-BASED ARCHITECTURE

- **Leverage cloud computing** to achieve
  - Faster and energy-efficient communications between sensing devices and the base stations, with a longer range.
  - Processing, storage, and analysis of the sensing data can be securely outsourced to the cloud.
  - In addition, we can presenting tiny devices as a service.

- As shown in the figure, the cloud has a central role in the overall infrastructure for data processing, storage, and analysis, as well as visualization is also known as Internet of Things (IoT).

- Building a content gathering and processing network from distributed devices based on clouds presents a series of challenges,
  - such as those relating to reliable content gathering, unreliable and heterogeneous sources, fast data delivery, real-time scheduling, cross-domain security, and cost efficiency.



CHALLENGES OF CLOUD COMPUTING

Transport Cost Too High

Too Much Data

Latency Too High

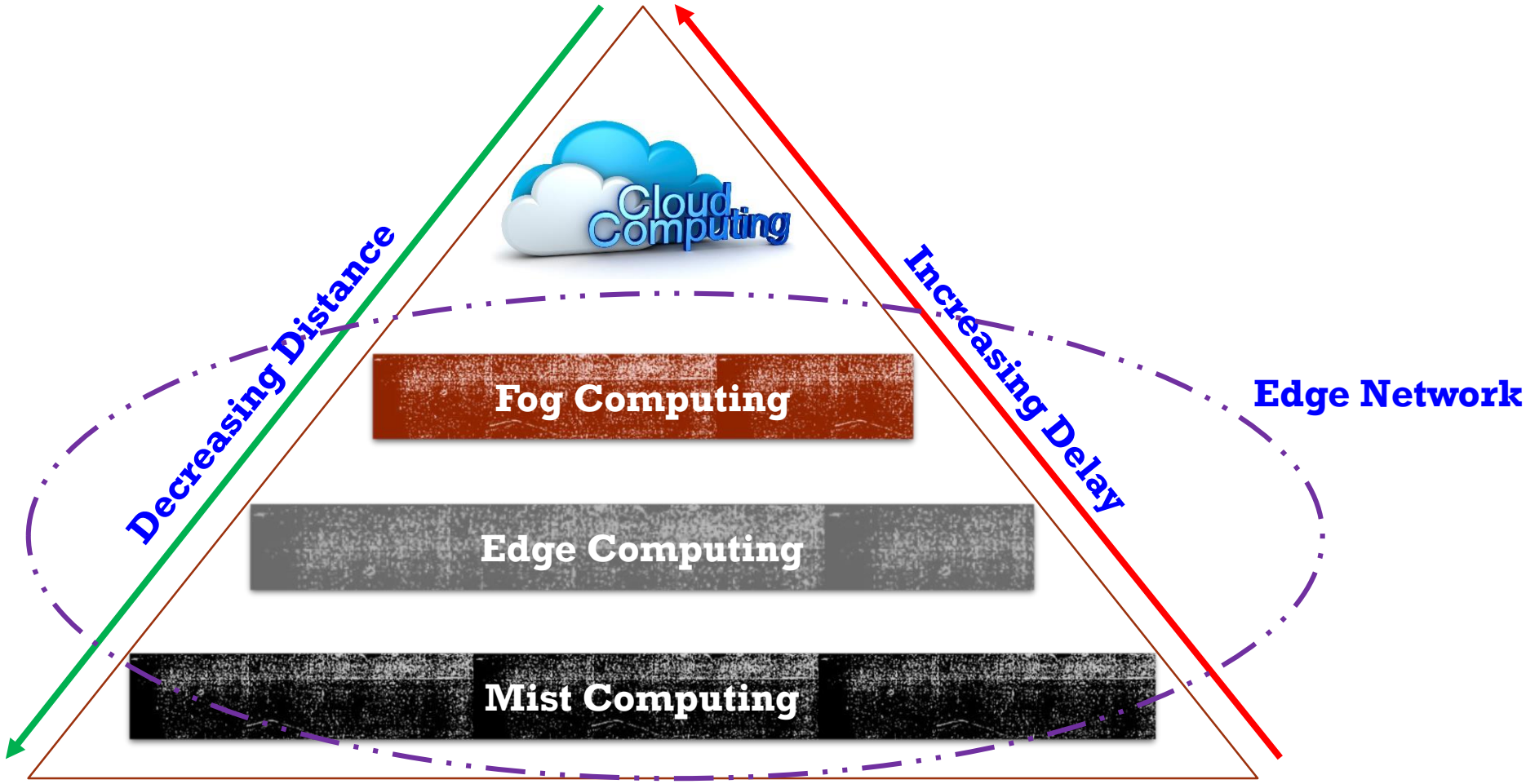
Resiliency Impractical

FOG COMPUTING, EDGE COMPUTING, MOBILE EDGE COMPUTING - WHICH ONE?

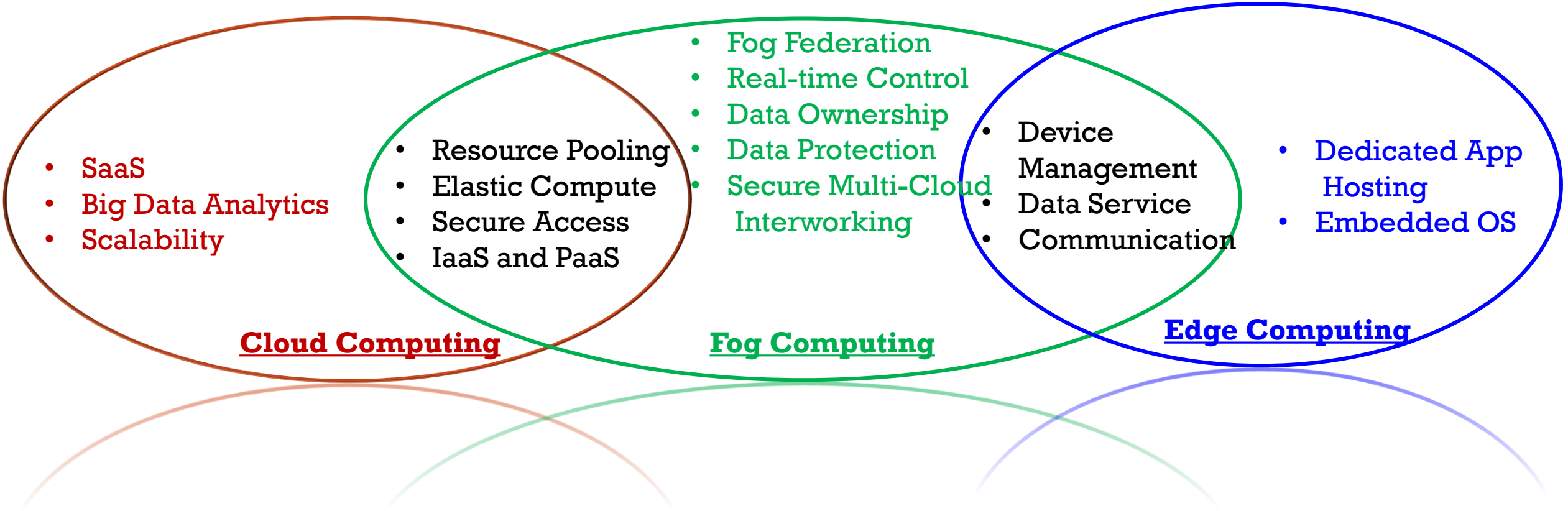
- **Trends:**
  - **Cloud computing (CC)** is more and more used, including private/local and mixed cloud development
  - However, traditional CC **centralization** (processing ,storage, latency delay, bandwidth..) may lead to some **limitations**
  - **Novel services and applications like IoT, mobility-related, would be better served by decentralized systems**
  - **Edge networking devices and even user terminals – more powerful**
    - in terms of processing, storage, communication capabilities

- **Result: recent attempts to push CC capabilities to the network edge:**
  - **Fog/Edge Computing**
  - **Mobile Edge Computing**
  - **Mist Computing**

CLOUD vs FOG vs EDGE vs MIST COMPUTING



CLOUD COMPUTING VS FOG COMPUTING VS EDGE COMPUTING



Source: https://www.nebbiolo.tech/wp-content/uploads/whitepaper-fog-vs-edge.pdf

CLOUD COMPUTING VS FOG COMPUTING

Requirements	Cloud Computing	Fog Computing
Latency	High	Low
Location of Servers	Within internet	At the edge close to nodes
Distance between the client & Server	Multiple hops	Few hops
Security	Varies amongst providers	Can be more defined and customized
Location awareness	No	Yes
Geo. Distribution	Centralized	Distributed
No. of Server Nodes	Few	Very large
Support for Mobility	Limited	Supported
Real-time Interactions	Supported but may be difficult to achieve & costly	Supported
Type of last mile connectivity	Leased line	Wireless

KEY FEATURES EDGE AND FOG COMPUTING

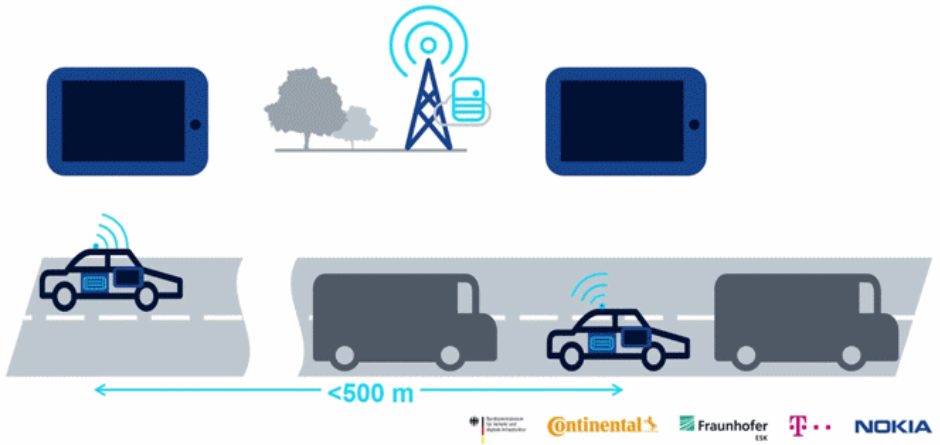
Key Features	Fog	Edge
App Hosting	Yes	Limited
Data Service at Edge	Yes	Yes
Device & App Management	Yes	Yes
Security	E2E, Data Protection, Session & Hardware Level	Partial Point Solution VPN, FW
Elastics Compute/ Resource Pooling	Yes	No
Modular Hardware	Yes	No
Virtualization with Windows Support	Yes	TBD
Real-time Control High Availability	Yes	No

DIFFERENCES BETWEEN TRADITIONAL EDGE AND FOG COMPUTING

Edge Computing	Fog Computing
Device aware and few services aware, unaware of the entire domain	Device independent, intelligent, and aware of the entire fog domain
Limited control in the edge domain	Controls all devices in the domain
Cloud unaware	Extends cloud to Fog level in a continuum
Limited network scope	Complete network scope
Uses Edge Controllers that are focused on edge device command and control	Uses fog nodes that are very versatile and capable of performing a variety of functions like RT Control, application hosting and management.
Security scope is limited to devices	End-to-End security
Analytics scoped to a single device	Fog Analytics enables collection, processing and analysis of data from multiple devices in the edge for analysis, machine learning, anomaly detection and system optimization.

MOBILE EDGE COMPUTING (MEC)

Brake Scenario Using MEC



Turn Signal Using MEC

Source: http://inside5g.com/mobile-edge-computing-used-to-support-assisted-driving/

MIST COMPUTING

- Lightweight computing residing within the network fabric at the extreme edge of the network fabric using microcomputers and microcontrollers.
- Feed into Fog Computing nodes and potentially onward towards the Cloud Computing platforms
- Not a mandatory layer of fog computing.

PROS & CONS of CLOUD, FOG, EDGE, AND MIST COMPUTING

	Cloud Computing	Fog Computing	Edge Computing	Mist Computing
Pros	❑ Easy to scale ❑ Low cost storage ❑ Based on internet driven global network on robust TCP/IP protocol	❑ Real time data analysis ❑ Take quick actions ❑ Sensitive data remains inside the network ❑ Cost saving on storage and network ❑ More scalable than edge computing	❑ It simplifies internal communication by means of physically wiring physical assets to intelligent PAC (programmable automation controller) to collect, analysis and process data. ❑ PACs then use edge computing capabilities to determine what data should be stored locally or sent to the upper layer for further analysis	❑ Local decision making data ❑ Works with fog computing and cloud platform
Cons	❑ Latency/Response time ❑ Bandwidth cost ❑ Power consumption ❑ Privacy, security, and legal issues	❑ Fog computing relies on many links to move data from physical asset chain to digital layer and this is a potential point of failure.	❑ Less scalable ❑ Interconnected through proprietary networks with custom security ❑ Cannot do resource pooling	

FOG COMPUTING: CONNECTING EDGE SENSING AND CLOUD COMPUTING

- IoT-based infrastructures have a wide range of applications,
  - spanning from small-size application for smart appliance,
  - and patient monitoring to large scale settings,
  - such as smart cities and smart nations.

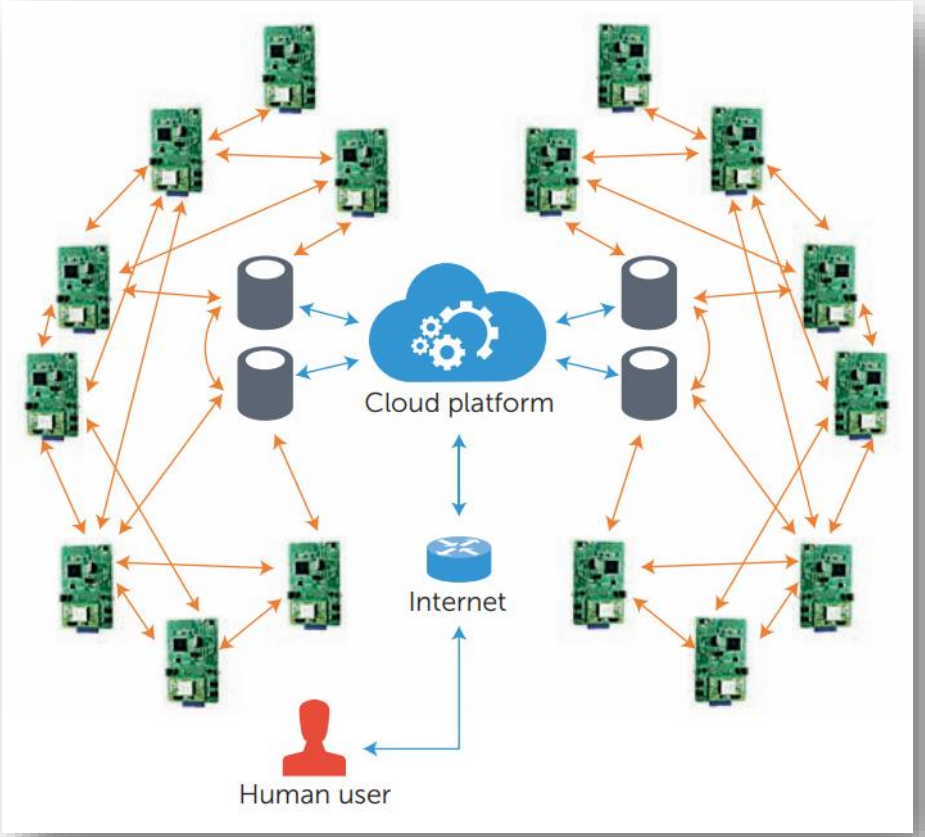
- In a typical real-world deployment, the size of these sensing networks is significant,
  - both in terms of interconnected devices and the volume of data to be processed and stored.

- Thus, there has been an increased focus on IoT and big data analytics research.

- It is also generally accepted that the centralized processing architecture,
  - is inadequate to deal with the scale of existing and emerging IoT infrastructures in smart cities and smart nations.

FOG COMPUTING: CONNECTING EDGE SENSING AND CLOUD COMPUTING

- While federating clouds can provide increased storage and computing capabilities; one recent trend is fog computing.
- In fog computing, a set of devices is placed in between the sensing devices and the cloud.
- As illustrated in Figure, the edge of the IoT and cloud computing is interleaved by an intermediary level, with devices that aggregate data acquired and sent to the cloud.
  - It has been suggested that architectures based on fog computing can improve the performance of IoT deployment
    - In terms of reduced response time, and reduced energy consumption.



FOG COMPUTING RISKS

- The use of wireless communications to interconnect the nodes can result in the system being vulnerable to jamming, sniffer, and other kinds of attacks.
- Such problems have been widely investigated within the context of ad-hoc networks and WSN,
- and solutions include using encrypted communications or channel-based authentication.
- In fog computing, however, the exchange of data is significant,
  - In terms of volume and veracity, and traditional network-level security enforcement is unlikely to be adequate due to its demanding energy usage.
  - Hence, designing effective lightweight solutions is a topic of ongoing interest.

FOG COMPUTING RISKS

- Similar to cloud computing, in fog computing, data and their processing are outsourced to the nodes, making such data vulnerable to a potentially wider array of threats.

- Due to the nature of fog computing deployment, there is a higher possibility that data sent to/through resource-constrained nodes to be compromised (e.g. due to lack of security measures on these nodes),

  - Resulting in information leakage and other malicious exploitation of the outsourced data and/or the results of the outsourced computations.

- Solutions proposed for cloud computing, such as data integrity schemes, searchable/ homomorphic encryption, and auditable data storage, may find limited application in fog computing

  - Due to the high data and task migration among fog nodes and the cloud.

- Such a migration occurs also within the cloud, but in a protected environment.

FOG COMPUTING RISKS

- In a fog platform, such a migration occurs along wireless networks in an un-protected context.
  - This results in more potential for attackers to conduct Man-in-the-Middle attacks targeting events during data and task migration.
  - It is possible to have compromised and camouflaged fog nodes seeking to intersect data and tasks that users outsource with the aims of exfiltration valuable information or injecting false data within the infrastructure.

- Another key security method to protect a cloud infrastructure from external attacks is access control.

- However, as fog nodes do not belong to a single administrative domain,
  - it is possible that nodes do not even belong to an administrative authority.

- In addition to the potential of having conflicting access control policies,
  - owners of fog nodes would likely need to propagate their access control policies through some third-parties trusted nodes.
  - Such a delegation model can potentially be abused by an adversary (e.g. highjack the policies and use them to facilitate attacks against fog nodes).

LEGAL DEVELOPMENTS

- There are also considerable concerns relating to data protection and personal privacy in a fog computing deployment.
  - The European Parliament and Council has established a working party to study data protection issues due to IoT,
    - to jointly protect the privacy rights of the individual without limiting the potential benefits offered by IoT.

- A solution identified by the working party is to
  - let users have complete control of their personal data and requiring organizations
  - to rely on consent as a basis when implementing privacy and data protection in their products and services.

- The General Data Protection Regulation (GDPR),
  - issued by the European Parliament on 24 May, 2016
  - and expected to be applied by all state members from 25 May, 2018, provides a legal framework.
  - Specifically, it tightens existing legal requirements by requiring data controllers to demonstrate that consent from individuals with respect to their personal data have been obtained.
  - In other words, individuals must have expressed a clear affirmative act of consent to IoT and/or other service providers.

LEGAL DEVELOPMENTS

- In addition to regulating issue relating to consent,
  - GDPR introduced the right to be forgotten, and portability rights when personal data across the EU boundaries are outsourced to the cloud.
  - The second aspect relates to data breaches, where GDPR requires IoT and other service providers to implement a general mandatory notification regime in the event of personal data breaches, and to adequately identify and respond to these security breaches.

- So, what is the best course of action from now to the time that GDPR is in force?

- IoT and related service providers should
  - review their current systems with respect to data privacy to identify possible issues,
  - delete data that is not necessary and may represent only a potential risk,
  - appoint a data protection officer (or outsource it to a third party), and
  - plan the implementation of technical, organizational, and policy solutions for privacy.

SUMMARY

- We posit that fog computing may ease the challenges of enforcing the protection of individuals' privacy and data protection rights.

- For example, in a cloud environment a key privacy challenge is the lack of user control on data outsourced to public clouds. In fog computing, however, the more powerful processing machines are located closer to the user.

- Hence, personal data is pushed locally to fog nodes that can be controlled directly by the user, while the public clouds or the further nodes only receive aggregated values that are less of a privacy risk to an individual's privacy rights.

- Such fog nodes can enforce the individual privacy rights and consent indication according to the Service Level Agreements, which detail the standard or expectations required in mutual data exchanges and processing between end-users' IoT devices and fog nodes.

REFERENCES

- Esposito, C., Castiglione, A., Pop, F., & Choo, K. K. R. (2017). Challenges of Connecting Edge and Cloud Computing: A Security and Forensic Perspective. *IEEE Cloud Computing*, *4*(2), 13-17.
- ***https://www.youtube.com/watch?v=RjMS15V_7nQ***
- ***https://www.nebbiolo.tech/wp-content/uploads/whitepaper-fog-vs-edge.pdf***
- ***http://inside5g.com/mobile-edge-computing-used-to-support-assisted-driving/***
- **https://medium.com/@YogeshMalik/fog-computing-edge-computing-mist-computing-cloud-computing-fluid-computing-ed965617d8f3**


Thank you!