Public Spaces in the Edge

Public Spaces are challenging and complicated scenarios for the next generation of distributed systems.

They can include Smart Cities, Smart Grids, Smart Transportation Systems, IoT (Internet of Things), or IoE (Internet of Everything).

In smart cities, application performance has never been more important to the user experience because, simply put, citizens act as customers. A citizen can’t have a traffic light experiencing connectivity issues – the ramifications are too serious. Similarly, workers can’t afford to lose access to their place of work. Smart infrastructure needs to be ‘always up.’

Example 5GCity Project

5GCity’s main aim is to build and deploy a common, multi-tenant, open platform that extends the (centralized) cloud model to the extreme edge of the network, with a demonstration in three different cities (Barcelona, Bristol and Lucca), and thus advance the state of the art to solve the main open research challenges in the 5G-based edge virtualization domain previously mentioned, including the neutral host perspective in dense deployment environments such as cities.

5GCity will essentially turn a city into distributed, third party, multi-tenant edge infrastructure, extending the cloud model all the way to the edge while enabling dynamic, fast, and interoperable provisioning of 5G-based services.

*[The 5GCity platform will embody a hierarchical architecture embedding network, compute and storage resources distributed across Small Cells and deployed at various technical spaces throughout the city: in lamp posts, urban furniture, street cabinets, and traditional data centres.]*

The public space is the confluence of a vast number of Personal and Social Spaces that interact in public spaces – streets, buildings, stadiums etc

Another strong argument for edge computing is the efficency and real-time interactions,

it delivers fast responses to users or devices since **M2M** – Machine 2 Machine communication is more efficient if they do not require the intervention of a central party.

The IoE implies a variety of heterogeneous mobile and fixed computing devices interacting with each other in different ways.

**Trust and Control:**

Every end-user participates in the public space through its own mobile devices and sensors.

Unlike cloud computing where there is a degree of trust in the service provider, edge computing may contain resources from diverse and ad hoc providers

A mobile user in the public space may switch between different service providers and contexts that may compromise its security and privacy.

Due to the huge variety of interactions with service providers and sensors, there is a need for novel technologies to preserve their security and privacy across domains.

For instance, in the case of the **neutral host** scenario, for some applications (hospital, banks, local police, etc.) it is very important to ensure that citizens data is processed only in compute nodes trusted from the viewpoints of the hardware and software configuration, device owner, geographic position, etc.

Similarly, there are mission critical 5G use cases such as automotive, Industrial IoT where security flaws put at risk the life of the smart city citizens

*[Neutral host infrastructure comprises a single, shared network solution provided on an open access basis to all* Mobile Network Operators  *and is used to resolve poor wireless coverage and capacity inside large venues or other busy locations. They are usually deployed, maintained and operated by a third-party provider and they are designed to support the full range of MNO technologies.]*

Also, edge distributed technologies should help end-users to perform threat analysis and to protect accordingly from close-by risky interactions. Since Edge servers may not be physically secured like a data center, and may be accessible by third-parties, additional supervision of the device is needed in order to ensure that security and privacy are not compromised.

As the user moves in the public space, he/she may generate flows of information that may compromise her own privacy. The interactions of the user that requires access to Cloud technologies should guarantee the confidentiality and security of users content and sensitive information.

Edge-centric Computing trust mechanisms should make end-users active participants of the public space, instead of the passive citizen as a sensor of the centralized smart city, it should shift to the active participation of users in their local communities.

**Humans**:

Humans are the most important factor to take into account in these novel distributed systems.

Human behavior is of paramount importance as a valuable information for adaptive distributed systems.

For example, one goal of the Smart City may be to optimize energy usage, but another **key goal is to improve the quality of life of its citizens.**

Edge distributed systems may even use personal information to provide personalized advice to some citizens. For example, if one is allergic to **Ragweeds (Ambrozie)** , she could receive different path recommendations that avoid risky zones.

There are also some studies regarding face recognition using edge servers, avoiding storing personal information in the cloud.

Here the information flows are bidirectional between humans and platforms. On the one hand, users generate their own flows of information that may share with the IoE environment.

They can make public some personal information, or they can even capture and contribute information with their own devices (user’s sensors).

On the other hand, the public space and their different service providers (advertising, entertainment, social, public institutions, sensors) may also generate information flows that may be of interest for humans and their devices.

In this case, the user’s intelligent agent may receive these information flows and react to them according to their user’s interests.

**Proximity and Intelligence**:

In the public space, proximity is very relevant both for analyzing close-by information and for storing local information. Like in Fog Computing , one of the key characteristics of Edge-centric Computing is its proximity to end-users and its support for mobility.

Vehicular networks allow connected cars to communicate with each other to cooperatively share information to make decisions on traffic and road conditions. These can be extended to share compute capacity to perform these analytics. This allows a collection of parked or slow-moving vehicles to form a fog of resources among proximate ones.

With the progress of M2M and IoT, the amount of data generated from Giga-ordered sensors in urban areas might become Exabyte order. In such huge data, it is difficult to store all of the data in remote cloud servers with reasonable costs.

In general, neighboring geospatial data might have strong correlation not present in distant geospatial data. Thus, it might be suitable for storing neighboring geospatial data in local edge servers (controlled by community networks, users or institutions) and providing local dependent services using those data.

Since such geospatial data are welled out continuously everywhere, all of such big data cannot be stored in the cloud. Thus, we need to study about

- what information processing are needed for treating such huge data,

- what analytic mechanisms are useful for those geospatial data,

- how and when we can discard sensing data welled out continuously

- how to protect user’s data obtained from user edge sensors.

The solutions for such questions can really provide future safe and smart urban life to people.

**Conclusions**

Nowadays, more and more services are pushed from the cloud to the edge of the network because processing data at the edge can ensure shorter response time and better reliability

Edge-centric Computing is a novel paradigm that moves the locus of control of Cloud Computing applications and services to the edges of the network. It would be more efficient to process or massage data at the edge of the network.

An edge may be a mobile device, a wearable device but also a nano-datacenter or a user-controlled device.

Edge-centric Computing allows users to retake control of their information, leveraging user’s resources and even reducing response times make edge-centric computing appealing to novel personal and social online services.

Edge-centric Computing is the natural confluence of peer to-peer and cloud computing to create hybrid architectures that combine stable resources with mobile terminals. It overcomes the limitations of P2P models *(churn, availability)* while providing security and privacy to hybrid Edge services