Revista de Sistemas de Informação da FSMA
n. 25 (2020) pp. 56-65

SISTEMAS DE INFORMAÇÃO
http://www.fsma.edu.br/si/sistemas.html

TRILHA PRINCIPAL

Models of Computing as a Service and IoT: an analysis of the current scenario with applications using LPWAN

Wesley dos Reis Bezerra, *Ph.D Candidate, PPGCC, UFSC*,
Fernando Luiz Koch, *Visiting Researcher, PPGCC, UFSC*, Carlos Becker Westphall, *Prof. Dr., PPGCC, UFSC*,

***Resumo*—A computação em nuvem é um paradigma que transformou a forma de entrega de computação em sistemas distribuídos. Entretanto ela tem encontrado alguns desafios com a chegada massiva de dispositivos IoT, fato que demandou uma evolução e a criação de novos paradigmas baseados na cloud. Neste novo cenário com muitos diferentes paradigmas, é necessário uma análise de suas características e desafios para saber qual o mais adequado a aplicação desejada. Este trabalho trás um levantamento sobre os paradigmas derivados da *cloud* e que são aplicáveis a IoT, assim como uma comparação de suas características e desafios; por fim, faz uma análise utilizando um cenário hipotético de piscicultura com IoT para avaliar os paradigmas elencados. Através deste estudo é possível ter-se uma base de análise dos paradigmas e seus desafio para um escolha adequada no desenvolvimento de soluções IoT utilizando LPWAN e *contrained devices*.**

***Palavras-chave*—Computação em Nuvem, Low Power WAN, Internet of Things**

Models of Computing as a Service and IoT: an analysis of the current scenario with applications using LPWAN

***Abstract*—**
This work provides the basis to understand and select Cloud Computing models applied for the development of IoT solutions using Low-Power Wide Area Network (LPWAN). Cloud Computing paradigm has transformed how the industry implement solution, through the commoditization of shared IT infrastructures. The advent of massive Internet of Things (IoT) and related workloads brings new challenges to this scenario demanding malleable configurations where the resources are distributed closer to data sources. We introduce an analysis of existing solution architectures, along with an illustrative case from where we derive the lessons, challenges, and opportunities of combining these technologies for a new generation of Cloud-native solutions.

***Index Terms*—Cloud Computing, Low Power WAN, Internet of Things**

Corresponding author: Wesley dos Reis Bezerra, *wesley-bez@gmail.com*

I. Introduction

Cloud Computing is the engine to modern Internet of Things (IoT) solution development. However, this paradigm was originally designed for the purpose of shared IT infrastructure, primarily allowing for business of any size to trade on-premise infrastructure by a rented resources [1], [2].

As workloads start to migrate to IoT-based solutions, there are new challenges around distribution, heterogeneity, volume, velocity, variety, security, vulnerability and others [3]–[6]. Hence, there is a need to evolve the Cloud Computing paradigm with malleability, distribution, and closer proximity to the data sources. This is the origin of mixed models like Edge Computing, Fog Computing, Mist Computing and others.

On the other hand, the utilisation of Low-Power Wide Area Networks (LPWAN) and *publish-subscribe protocols* like *AMQP*, *MQTT*, *STOMP*, and *CoAP*, is increasingly popular in Cloud-IoT solution design. New challenges in combining these models revolve around issues of synchronisation, configuration, security, vulnerability and others [4], [5], [7]. For instance, more sophisticated security mechanisms require larger computing capacity, such as processing, memory utilisation, and power consumption. Engineers must measure the trade-offs between performance, security, and expected device cost while designing secure IoT devices and deploying distributed Cloud Computing configurations.

We argue that these issues can be mitigated by selecting the appropriate model combination for the solution demand. Solution designers and application developers need to understand the characteristics and capability of the diverse configurations and how they align with the system requirements in hands. Therefore, our research question is:

> What is the best Cloud Computing model to be applied for a given application scenario involving Cloud-IoT-LPWAN?

We introduce an analysis of the existing models of Cloud Computing applicable for the development of solutions involving IoT, LPWAN and constrained devices. Our goal

is to provide the basis for researches and solution designers to compare and select technologies for product development. We acknowledge the limitations of this study as this is an extensive area, permeated by different challenges, opportunities and requirements. Nevertheless, we deem this analysis comprehensive enough to offer the basis for understanding and analysis of the combinations. This study provides three main contributions to the field:

1) a survey of Cloud Computing paradigms applicable for this application scenario;
2) an analysis of the challenges and opportunities in developing Cloud-native applications in this scope;
3) guidance on selecting the best combination of Cloud Computing model and LPWAN in different application scenarios.

This work is organised as follows. Section II provides an overview of the background scenario. Section III introduces a survey of the Cloud Computing paradigms, support and challenges when applied for the problem scenario. Section IV analysis the support of the different paradigms when applied for an illustrative scenario. We conclude with a discussion of the lessons learned, challenges and opportunities in Section V.

II. Background

In this section, we present an overview of the current scenario involving Cloud Computing, connected devices, and the challenges and opportunities to combine Cloud-IoT-LPWAN.

A. Cloud Computing

Cloud Computing can be described as a a model to support shared Information Technology (IT) resource accessible on-demand through a network infrastructure [2]. It encompasses a pool of computational resources, like processing, storage, applications, and other services, which are made available through virtualised environments, accessed through the global network infrastructure. This form of computing is increasingly perceived as the 5th utility (after water, electricity, gas, and telephony), which provides the basic level of computing service that is considered essential to meet the everyday needs of the general community [8], [9].

Operationally, Cloud Computing is segmented in three types of services [2]: Infrastructure as a Service (IaaS), where the shared resources relate to computing infrastructure, like Virtual Machines, virtual disks, and others; Platform as a Service (PaaS), where the Cloud infrastructure provides virtualised operational platforms, and; Software as a Service (SaaS) where the consumer has access to shared software running on the Cloud. Each service model has its pros and cons and their adoption relates to the business requirements. For instance, the SaaS model has been widely used by software developing companies to provide solutions through *web platform* without the need to maintain the complete stack – hardware, OS, HTTP servers, and access; the Cloud SaaS provides all-in-one service accessible through the Web, also including maintenance, support, security, reliability, elasticity, scalability, and others.

The Cloud Computing model introduces a form of distributed computing boosted by a major business prerogative: trade the fixed cost infrastructure around on-premise computing by shared IT infrastructure with variable cost [1]. The business argument is that Cloud clients do not need to afford computing equity, including machinery and physical infrastructure, but instead rent this service from a Cloud provider who also takes care of maintenance, support, depreciation, Quality of Services, infrastructure, redundancy, safety, security, and others. Combine with advances in network communication and scalability of computing power, this model is rapidly becoming the *de facto* infrastructure for Digital Transformation strategies [10], [11].

B. Distributed Cloud Computing

However, as business start to migrate workloads to IoT-based solutions, there are many challenges to the Cloud Computing model to support the new computational demands [3]–[6]. The term IoT was introduced by Kevin Ashton in 1998 [5] and has been used to designate smart devices with internet connectivity. IoT is flourishing as an important tool to solve problems in several areas of knowledge, such as Smart Cities, Smart Buildings, Industry 4.0, Precision Agriculture, Health, Education, Connected Vehicles, and many others [3], [12], [13]. Each area of IoT application has its specified demands for network consumption, latency sensitivity, physical network layer, distribution, power consumption, and security. Due to this diversity, a large number of companies have developed IoT solutions leading to a heterogeneous and fragmented market [14].

Hence, there is a need to adapt the Cloud paradigm with malleability, distribution, and closer proximity to the data sources. This is the origin of mixed models like Edge Computing, Fog Computing, Mist Computing and others. There is an increased need for localised processing and storage in distributed IoT solutions. Even though usually IoT data is formed by small packages, due to the large number of devices, they generate large data volumes for communication, storage, and processing [15]. Therefore, there is a need to select the proper distributed cloud computing to support the requirements of specific IoT solutions [16].

Telemetry protocols have been incorporated into existing Cloud Computing services to address the issues of data volume and velocity in IoT configurations. To cite the main ones, MQTT [17], CoAP [18], DDS [19], AMQP [20], XMPP [21], STOMP [22] and HTTP19 are example of popular publish-subscribe protocols New challenges in combining these models revolve around issues of synchronisation, configuration, security, vulnerability and others [4], [5], [7]. For instance, more sophisticated security mechanisms require larger computing capacity,

such as processing, memory utilisation, and power consumption. Engineers must measure the trade-offs between performance, security, and expected device cost while designing secure IoT devices and deploying distributed Cloud Computing configurations.

C. Challenges and Opportunities

With the IoT bringing so many connected devices, some concerns come to the forefront, such as aspects of:

- security, where flaws are frequently reported by data manufacturers [4]–[6], system intrusion [23]–[25], and others;
- *data volume and data flows* pose a problem to IoT applications, where it is important to understand the characteristics of the data flow between: (i) *small and simple data streams*, e.g. coming from e.g. smart metering applications [26], and; (ii) *complex and larger data flows* , e.g. sources from images, patterns and matrices [27];
- *limited or heterogeneous networks*;
- *energy consumption*, which becomes a major challenge when applied to constrained devices [28], often designed to perform with a long battery life, e.g. ultra-long life battery can last for 10 years if the device is properly operated.

Finally, there is a surge of implementations around *Low Power Wide Area Network* (LPWAN), where devices connect to centralised services through wireless protocols with limited data transmission and radio link.

III. Survey

As IoT-based solutions start to take hold of the market, it became clear that Cloud-centred solutions imposed severe restrictions in terms of latency, heterogeneity, volume, velocity, variety, security, vulnerability and others. For that, new concepts of distributed Cloud Computing started to emerge in the market, each bringing new solutions and challenges of their own.

Computing as a service has gone through several stages of development. It can be used in virtual automation through Virtual Machine Environment (VME), the virtualisation of services in Software Define Networks (SDN), and the distributed models like Fog Computing, Mist Computing, Mobile Edge Computing, Mobile Cloud Computing, and Superfluid Computing, between others.

In what follows, we introduce these alternative models and explain how they support application scenarios involving Cloud-IoT-LPWAN. We also interwove an analysis of the challenges and opportunities in developing Cloud-native applications in this scope.

A. Cloud Computing-IoT

There are some case where Cloud Computing looks like the ideal option for IoT. This model provides low cost processing and storage, availability, well-known programming resources, and others The concept works well in situations where wither there is good connectivity or no demand for real-time processing. Popular examples are applications of video security in home automation that store streams on the Cloud. Li et al [29] presents the example of Connected Vehicles Cloud Computing where vehicle-bounded sensor devices connect to Cloud-centred infrastructure for services. Figure 1 depicts the solution architecture, composed of:

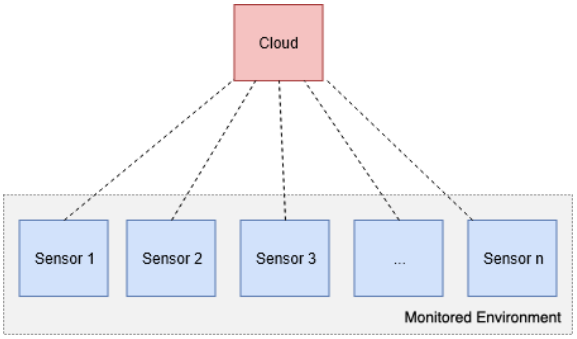

Fig. 1. Cloud Computing-Centred IoT Architecture

1) *cloud layer*, providing centralised processing and storage;
2) *service consumers layer*, which in the case of IoT applications service consumers are sensors.

Sensors must be connected either directly through Application Program Interfaces (APIs) or through a Protocol Gateway. All services are performed on the Cloud infrastructure, including processing, storage, and any other add-value service. If location information is needed, the gateway (or sensor) must include location information such as pre-configured or from a GPS, as the central service lacks awareness of location [30].

This architecture presents challenges to support IoT-based applications mainly due to volume, latency, heterogeneity, security, and others. Basu et al [31] list some important challenges, such as: data segregation, data location, data incomplete data, monitoring and data logging, problems associated with the security of Virtual Machines and their environment, and even natural disasters. Subramanian et al [32] enlist confidentiality and integrity among the main security challenges.

Other requirements are authentication, auditing, and legal security requirements. The latter is important because the data is subject to regulations in some countries. Sha et al [12] describe the challenges around heterogeneous network technologies, privacy, large scale of systems, and management of trust. Stergiou et al [33] corroborate to the narrative, listing key challenges around heterogeneity, performance, reliability, big data and monitoring.

B. Fog Computing

Fog Computing is a model of distributed Cloud Computing designed to cope with the growth of IoT environment and issues of latency inherent to this configuration [30], [34]. Yi et al [7] postulate that this model will be the

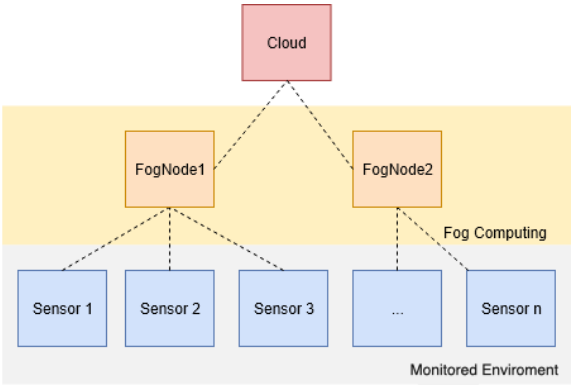

Fig. 2. Fog Computing Architecture

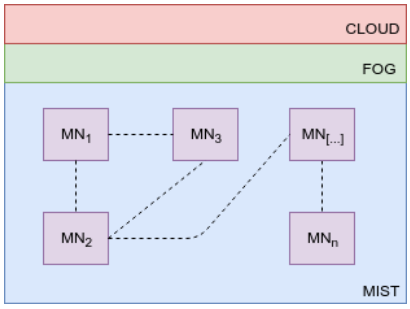

Fig. 3. Mist Computing Architecture

internet of the future due to the number of existing devices and the arrival of more devices in the market.

This model is organised in three layers, as depicted in Figure 2:

1) Cloud with the classic CC model and centralised computing;
2) Fog Nodes are central part of the architecture; these can be either physical components or virtual components and are tightly coupled with smart devices or network access nodes, providing computational resources to these devices.
3) Sensor Nodes providing the data sources in the edge layer.

This model is inherently distributed geographically, providing resources near the data sources where they are usually most necessary. For example, in case of IoT and wearable devices, impeding restrictions of processing and storage in these devices demand for Fog Nodes to deliver situated resources.

However, the multi-layered nature of this model increases its implementation complexity. One direct impact of this extra complexity is on security. Yi et al [7] describes the challenges of Fog Computing around the choice of virtualisation technologies to be applied, along with the issues of latency, network management, security, and information privacy. Luan et al [30] includes challenges around application development of applications, scalability, and distribution.

DSouza et al [1] mentions that Fog Computing's multi-level collaboration brings a new set of problems around identity management, resource access management, distributed decision, dynamic load balancing, quality of service and security. Vaquero et al [15] mentions that in order for Fog Computing to become reality, developers must first solve its many challenges around synchronisation, device discovery, management, security, standardisation, accountability, billing of mobile applications.

C. Mist Computing

Mist Computing (MC) plays an important role in the migrating computation power to the systems' edge. This model extents *Fog Computing* by adding an extra layer placed closer to the edge, below the Fog Nodes [35]. Figure 3 depicts the architecture:

1) *Cloud Computing* provide centralised services, when needed, such as monitoring, updates, central data repository, offloading processing, and others.
2) *Fog Computing* provides distributed capabilities and group control over the mist nodes, bridging with Cloud Computing services when required; for instance, *Fog Nodes* may provide resources like regional storage, processing offloading, monitoring, software updates, and others.
3) *Mist Nodes* are located at the border, providing local resources and processing, with connectivity with their peers and requesting resources from them.

Mist Nodes are usually implemented through devices that offer basic computational power, such as Arduinos, Nodemcus, and other microcontrollers and microchips. A practical example of Mist Computing implementation exist in automated vehicles where the multiple elements are connected to a central car unit (Fog), which can connected to other cars for collaboration and collective intelligence.

The key concept is to promote interaction between *Mist Nodes* as much as possible, refraining from utilising centralised services or devices. The architecture can be conceptualised as a model in which network edge devices have predictable accessibility and provide their communication and computational resources as a service [36]. Mist Nodes can distribute software processes to run on service providers on their own. That is, Mist Computing favours a model of computing "a hop away" [37].

Mist Computing brings computing power deeper into the edge, embedding processing in microcontrollers and System on Chips [38]. This model can provide a flexible environment for execution of customised programs [36]. However, Mist Nodes do not have the computational power of a Fog Node so they must be used in complement. In situations where applications demand processing or storage, these requests can be offloaded to Fog Nodes, which in turn can relay to Cloud Computing.

This architect can be leveraged to extend the capacity of constrained devices, like mobile sensors, and promote fast processing at the very edge of the system. Being an integral part of the edge, Mist Computing provides the lowest latency possible for an IoT application. However,

it suitable only for a restricted number of application scenarios considering the constrained computing capabilities and implicit distribution.

Preden et al [39] describes the challenges of *Mist Computing* related to communication complexity and self-management, as a result of the dependence of a central component. For Yogi et al [40] list as challenges: low storage capacity, limited bandwidth, and resistance from solution developers to adopt the model. Vasconcelos et al [41] argues that the challenges are common to Fog Computing, and the most characteristic challenge is related to the complexity brought by the dynamic topology. Suarez-Albela et al.[42] list challenges related to security, as the use of security mechanisms such as encryption demand a require energy consumption by the devices.

D. Mobile Cloud Computing

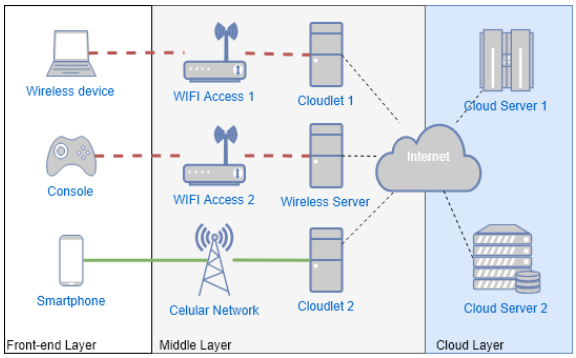

Fig. 4. Mobile Cloud Computing Architecture

Mobile Cloud Computing (MCC) is about the provisioning of data and storage closed to the mobile user. In its most elementary form it refers to an infrastructure where both data processing and storage take place outside the mobile device [7]. The concept of mobile cloud relates to pervasive devices sharing their support services and heterogeneous resources, such as network band, processing, content, and others [43]. The architecture contains three layers as depicted in Figure 4:

1) *Front-end layer*, where either user interfaces or services request applications are located, usually running on mobile devices; this layer works by requesting service from external providers, through offloading processing and storage.
2) *Middle layer*, promotes offloading access to computing power hosted on servers, wireless network, or *cloudlet* [44].
3) *Cloud layer*, provides the back-end infrastructure to respond to all requests.

Mobile Cloud Applications can transport computing, energy and data storage out of phones and into the Cloud. This allows to create a new range of solutions not only for mobile phone applications but also a range of other solution niches [45].

In order to prevent delays in processing the data due to latency or network bottlenecks, the network segment between the *front-end* and the *middle layer* must support high throughput. Moreover, the communication link between the *middle layer* and the *cloud* is usually the Internet, thus subject to intermittent connections, latency, and security issues. Hence, real-time applications must be processed in the *middle layer*. The element responsible for bringing *cloud* capabilities close to the mobile device are the *cloudlet* [43].

Au et al [46] argues that the key challenges for this model are related to data and authentication, including: authentication of mobile users and devices, security in data communication and storage, data integrity, data search, and secure data sharing. Leppanen and Riekki [47] enlist as challenges offloading, scheduling, monitoring, resource tracking, context awareness, and remote service availability. Challenges and issues of heterogeneity in Mobile Cloud Computing are largerly discussed in [14].

Sekaran, Vikram and Chowdary [48] present the issue of security and Distributed Denial of Services (DDoS), and describe different ways to prevent these attacks in MCC. Noor et al [49] list as the main challenges security, privacy, bandwidth control, data transfer, data management, synchronisation, energy efficiency and heterogeneity.

E. Mobile Edge Computing

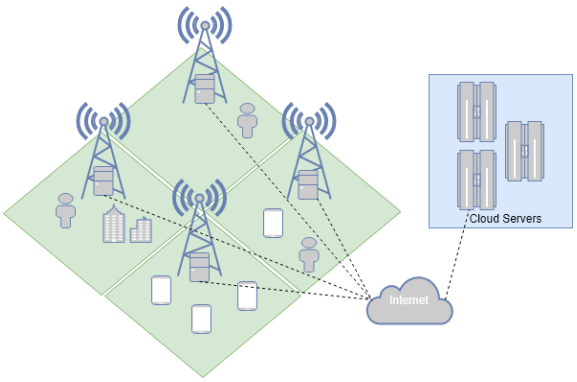

Fig. 5. Mobile Edge Computing Architecture [50]

Mobile Edge Computing (MEC) utilises the infrastructure based on mobile networks to provide connectivity to edge devices. This architecture has the purpose of bringing computing resources, mainly processing and storage, near to the data sources. Services are deployed directly at base stations or in smart cells, as for instance Femtocells, Picocells, Nanocells, and others. This approach relies on the infrastructure provided by mobile phone operators and it may incur in issues of coverage, high costs of mobile data, and others.

The architecture is implemented in three layers, as depicted in Figure 5:

1) *edge*, usually composed of IoT , mobile computing, and wearable devices;
2) *servers*, providing located computing resources aiming at low latency and quick response for service requests;

3) *cloud*, providing centralised processing and storage.

MEC brings some relevant benefits such as ultra-low latency, high bandwidth, real-time access to radio network information, and location services [51]. For the latter, unlike other models, MEC allows to identify the location of the data source, thus providing additional support for security, locality, and auditing e.g. in case of regulated installations. Moreover, ultra-low latency favours applications that require quick response in decision-making.

The devices located on the edge of the MEC must have components that allow them to access the cellular network, either via *macrocells* i.e. antennas and other classic devices or *smartcells*, which are eager to increase the reach of cellular networks, by expanding their capacity to provide connectivity, specially to o rural areas.

This model is becoming a hot topic with the multiplication of MEC service providers and the arrival 5G technology, in solutions to support communication, computing, control, and content delivery [52]. One the key benefits of this model for IoT solutions is better coverage, specially in urban areas. This will allow for like Smart Cities and Smart Buildings that can directly benefit from MEC and 5G.

The *server layer* brings mobile users close to the benefits of Cloud Computing around elasticity and virtualisation. In the MEC model, this is implemented upon virtualisation platforms like Network Functions Virtualisation (NFV), Information-Centric Networks (ICN) and Software Defined Networks (SDN) [52].

NFV promotes the virtualisation of network functions, making them work like in the Cloud Computing model. This is implemented either through dedicated hardware or off-the-shelf devices [51]. The objective of virtualising network functions is towards the cost benefits of shared infrastructure, preventing e.g. capital costs and operational costs related to site allocation, cooling, maintenance, and others. The functioning is based on three concepts: virtualisation, orchestration, and turning all functions into software. Common examples of virtualised functions include firewall, DHCP, NAT, and others

SDN virtualises the network by decoupling control plane from data plane [51]. As an analogy, NFV visualises network functions, SDN. The goal is to understand the allocation and performance of routes, define new ones, connect physical and virtual services, define policies, allocate IPs, allocate bandwidth, and ensure connectivity. SDN facilities the process of creating NFV by supporting the configuration of the connection of functions in the network.

Ahmed and Rehmani [53] list as challenges the fast development of services at a cost efficient rate, optimised resource utilisation, facilitate the migration of existing application, and security. Vassilakis [54] mentions the need for security and privacy solutions specific to this model and the possible coexistence with unreliable nodes. Beck et al. [55], [56] defines some metrics that need to be met to allow utilisation in some areas, such as energy consumption, delay, bandwidth and scalability. They also mention challenges around scalability, mobility awareness, and utilisation awareness by embedded applications.

Varghese et al. [57] presents a list with five challenges: (i) ability to provide general purpose computing at the edge nodes; (ii) node discovery; (iii) task partitioning and orchestration; (iv) balance demands, processing, and Quality of Service (QoS) and Quality of Experience(QoE); and (v) safety. Roman, Lopes and Mambo [58] list as challenges: infrastructure, virtualisation, resources and tasks, distribution, mobility and programmability.

F. Emerging Models

There are two trendy technologies emerging in the market that are worth mentioning at this point: *Superfluid Cloud* and *Cloud Radio Access Network*. We acknowledge that this list is far from exhaustive and other commercial and research solutions emerge frequently in the market, but included a brief description for the reference.

Superfluid Cloud [59] is a multi-tenant model where virtualised services based on software execute on commodity hardware, being shared and deployed across the network. The idea is to apply low-cost devices with devices with significant computational power, such as System-on-Chip, Cubieboard, Raspberry Pi, and others. The most important characteristics include [51]: recursion; scalability; separation between state and processing; support for very small VMs; support for Extended State Finite Machines (XFSMs), and; on-the-fly monitoring.

Cloud Radio Access Networks virtualise some important functions of modern telecommunications architecture, lowering the cost of deploying and operating mobile networks [60]. Demestichas et al [61] list challenges around multiple perspectives of society, economy, users, and operators. There are also issues on normalisation in order to have a cohesive, inclusive, and sustainable structure. These challenges relate to wireless communications in general and can be mitigated through C-RAN's centralised structures.

IV. Application Scenarios

In business-critical application that supports decision-making in near real-time based on information from IoT sensors, Quality of Service (QoS) can be measured, between other factors, on aspects of efficiency, accuracy, and security. This sort of solution cannot compromising QoS due to e.g. network latency, intermittent communication, intrusion attacks and things of the sort. It is intuitive that the system will perform better if the decision-making processes are closer to actuators and connected through a reliable communication network, which obviously imply in infrastructure costs. Hence, solution designers juggle to reach a balance between QoS and affordability.

Let us consider an application scenario in the field of Smart Agriculture: a system for monitoring artificial tanks in fish farming. In this solution, sensors information about the fish tanks, such as capture water temperature, oxygenation level, ammonia rates, movement, and other information about fishery. The information is relayed to a processing unit for storage, analysis, and recommendation

generation. The recommendation system controls actuators that act upon mechanisms to control conditions, e.g. turning the oxygenation pumps, releasing food, promoting water circulation, and providing information and insights to oversees through dashboards on mobile devices. The system also provides visualisation through mobile computing devices to support on-spot decision making.

This is a business-critical solution as QoS issues on the monitor-actuator system directly impact farm's production. For instance, taking too long to open oxygenation pumps will lead to high fish mortality; not releasing enough food will lead to malnutrition; providing too much food leads to food poisoning, and others. Scenarios like this present clear challenges in terms of volume, latency, and intermittent access to remote services even by making use of telemetry protocols, such as MQTT. Hence, solution design around distributed Cloud Computing must be considered.

By applying the *Cloud Computing-IoT model*, described in Section III-A, developers have the advantage of having centralised data from multiple points, thus supporting insight models that demand correlation of large volumes of data, creation of dynamic filters, and provide greater computational and storage resources. Nonetheless, this model stress the issues of volume, latency, and intermittent connections around the uploading data links. Hence, this model is useful for specific requirements, such as the creation of models that correlate data from multiple sites, and in specific conditions, e.g. when there is a high-throughput stable data link to support the upload data link.

On the other hand, the *Fog Computing model*, introduced in Section III-B, allows for data being stored in an intermediate node, preventing good part of latency for data uploading. The system's intelligence would be allocated in the FN, closer to the edge. Thus, insights, reports, dashboards, and recommendations would be processed on the Fog Nodes, based on Analytic models trained on the Cloud. The process of synchronisation, maintenance, and model revision and retraining, and retraining, make part of the Orchestration Strategy and must be defined by developers during the system setup. This extra step of complexity is the down side of the model. It requires that developers are familiar of the new demands and toolkits to enable the development at an acceptable cost. Moreover, the data is more expose at the edges, thus highlighting issues of security and privacy.

Mist Computing, presented in Section III-C, is not applicable to this scenario as this model does not provide support to reporting, storing data, and massive data processing. This model, if directly applicable, would provide the best response time in relation to the sensors and actuators, as processing takes place in the same network segment where the sensors are positioned. Due to the limited processing capability, a combination of *Mist Computing* could be adopted in the architecture to provide reactive responses for alarming systems, for instance.

Mobile Cloud Computing, introduced in Section III-D, allows for low-cost sensors to be integrated in the solution. This model requires the implementation of *cloudlet* on the same local wireless network. However, due to extensive data distribution, the compilation and access to reports would depend on an auxiliary system installed on a Cloud Computing system and it would require a synchronisation process to upload data from the cloudlets. This setup implies in higher implementation costs, eventual latency on generating the reports, and maintenance complexity.

Mobile Edge Computing, explained in Section III-E, provides us with a scenario very close to CF. However, it is applicable when there is no possibility of using a cheaper wireless link, with the cellular network option being the only viable one. This can happen due to the sensed tank being remotely distant from a wifi access point but still covered by the mobile network. It is observed that transmission over the mobile network requires greater use of energy and, consequently, shorter battery life.

When considering the utilisation of LP-WAN in the scenario, this technology favors the use of Fog Computing model. That is, when the solution demands higher power networks such as WiFi and wired network, one could not apply the*cloudlets*. If applying a centralised node , such as in the *Cloud Computing-IoT* model, the solution would require a gateway to bridge between the LPWAN segment and the Internet. If the solution involves a number of constrained devices, then any model that require large message exchange, such as Cloud Computing and Mobile Cloud Computing are not the best choice for the scenario.

Hence, we conclude that Fog Computing model is the intermediate solution for this problem scenario. By providing proximity to the edge for the data source, it allows for lower latency and fastest response time suitable in mission critical situations. Mobile Edge Computing also prevents itself as a viable solution in this scenario, due to similarities with Fog Computing. However, the approach implies in higher hardware costs.

V. Conclusions

This work brought an overview of emerging paradigms of distribute cloud computing, describing their architecture, applicability and models. We focused on solutions around LPWAN and constrained devices and related the restrictions and characteristics of both models.

We concluded that Fog Computing is the most adequate paradigm for the proposed scenario, providing the desired features of distribution, orchestration, and normalised interfaces. However, the Mobile Edge Computing model provides similar characteristics with appealing cost structure. Thus, both models must be considered when designing IoT solutions that demand low latency, local processing, high throughput and other related characteristics.

Moreover, we assessed that aspects of security are fundamental in distributed Cloud Computing. We highlight the often overseen issues of *intrusion attacks*. As any other distributed environment, Fog Computing, Mist Computing, MEC, and others are prone to intrusion attacks due to their distribution and heterogeneity nature. It requires methods for distributed intrusion detection and reaction

allowing for real-time security and intrusion prevention [23], [24]. Vieira et al [25] introduces a method to apply Big Data for fast intrusion detection and reaction, claiming that the longer it takes to react to intrusion attacks, the more likely are them to succeed. We believe that these solutions will become increasingly more relevant with the widespread of IoT and distributed Cloud Computing.

As future work, we propose the use of network simulators to evaluate the protocols to be used together with the paradigms. Simulations could also be applied to evaluate message protocols and security issues. This will allow you to assess what network protocol is most suitable for LPWAN and CD in the proposed scene. In addition, there are potential advancements in distributed processing and swarm computing to be considered and integrated in the models. For example, in Assuncao et al [62] we introduced a view of *grids of agents* as a implementations were very distributed and interconnected acting elements would implement required services. The raise of Fog Computing and Mist Computing catalyse the need for that kind of infrastructure, creating an opportunity for future research and development. Finally, situation aware solutions such as presented in [63], a context-aware content delivery implementation, will demand for extended coordination and orchestration in Fog Computing and Mobile Edge Computing, calling for research and development in context-aware orchestration in distributed cloud computing environments.

Referências

[1] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)*, IEEE, 2014, pp. 16–23.

[2] P. Mell, T. Grance, *et al.*, "The nist definition of cloud computing," 2011.

[3] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *2014 International Conference on Future Internet of Things and Cloud*, IEEE, 2014, pp. 464–470.

[4] *OWASP top 10 internet of things*, https://www.owasp.org/, 2018.

[5] S. Deep, X. Zheng, and L. Hamey, "A survey of security and privacy issues in the internet of things from the layered context," *arXiv preprint arXiv:1903.00846*, 2019.

[6] E. Bertin, D. Hussein, C. Sengul, and V. Frey, "Access control in the internet of things: A survey of existing approaches and open research questions," *Annals of Telecommunications*, pp. 1–14, 2019.

[7] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, IEEE, 2015, pp. 73–78.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[9] R. Buyya, J. Broberg, and A. M. Goscinski, *Cloud computing: Principles and paradigms*. John Wiley & Sons, 2010, vol. 87.

[10] C. Matt, T. Hess, and A. Benlian, "Digital transformation strategies," *Business & Information Systems Engineering*, vol. 57, no. 5, pp. 339–343, 2015.

[11] S. J. Berman, "Digital transformation: Opportunities to create new business models," *Strategy & Leadership*, 2012.

[12] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in internet of things," *Future Generation Computer Systems*, vol. 83, pp. 326–337, 2018.

[13] M. R. Ramli, S. Bhardwaj, and D.-S. Kim, "Toward reliable fog computing architecture for industrial internet of things," 2019.

[14] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: Taxonomy and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 369–392, 2013.

[15] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 5, pp. 27–32, 2014.

[16] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, "Fog computing: A platform for internet of things and analytics," in *Big data and internet of things: A roadmap for smart environments*, Springer, 2014, pp. 169–186.

[17] O. Standard, "Mqtt version 3.1. 1," *URL http://docs. oasis-open. org/mqtt/mqtt/v3*, vol. 1, 2014.

[18] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," 2014.

[19] G. Pardo-Castellote, B. Farabaugh, and R. Warren, "An introduction to dds and data-centric communications," *RTI, Aug*, vol. 26, 2005.

[20] O. Standard, "Oasis advanced message queuing protocol (amqp) version 1.0," *International Journal of Aerospace Engineering Hindawi www. hindawi. com*, vol. 2018, 2012.

[21] P. Saint-Andre, "Extensible messaging and presence protocol (xmpp): Core," 2011.

[22] *STOMP Protocol Specification version 1.2*, http://stomp.github.io/stomp-specification-1.2.html.

[23] A. Schulter, J. A. Reis, F. Koch, and C. B. Westphall, "A grid-based intrusion detection system," in *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learn-*

ing Technologies (ICNICONSMCL'06), IEEE, 2006, pp. 187–187.

[24] A. Schulter, F. Navarro, F. Koch, and C. B. Westphall, "Towards grid-based intrusion detection," in *2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006*, IEEE, 2006, pp. 1–4.

[25] K. Vieira, F. L. Koch, J. B. M. Sobral, C. B. Westphall, and J. L. de Souza Leão, "Autonomic intrusion detection and response using big data," *IEEE Systems Journal*, 2019.

[26] M. R. Chowdhury, S. Tripathi, and S. De, "Adaptive multivariate data compression in smart metering internet of things," *IEEE Transactions on Industrial Informatics*, 2020.

[27] K. Muhammad, T. Hussain, M. Tanveer, G. Sannino, and V. H. C. de Albuquerque, "Cost-effective video summarization using deep cnn with hierarchical weighted fusion for iot surveillance networks," *IEEE Internet of Things Journal*, 2019.

[28] B. Girgenti, P. Perazzo, C. Vallati, F. Righetti, G. Dini, and G. Anastasi, "On the feasibility of attribute-based encryption on constrained iot devices for smart systems," in *2019 IEEE International Conference on Smart Computing (SMARTCOMP)*, IEEE, 2019, pp. 225–232.

[29] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 4–6, 2018.

[30] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," *arXiv preprint arXiv:1502.01815*, 2015.

[31] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, "Cloud computing security challenges & solutions-a survey," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2018, pp. 347–356.

[32] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 71, pp. 28–42, 2018.

[33] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & iot," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[34] R. Buyya and S. N. Srirama, *Fog and edge computing: principles and paradigms*. John Wiley & Sons, 2019.

[35] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. S. Goren, and C. Mahmoudi, "Fog computing conceptual model," Tech. Rep., 2018.

[36] M. Liyanage, C. Chang, and S. N. Srirama, "Mepaas: Mobile-embedded platform as a service for distributing fog computing to edge nodes," in *2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, IEEE, 2016, pp. 73–80.

[37] D. Vasconcelos, R. Andrade, V. Severino, and J. D. Souza, "Cloud, fog, or mist in iot? that is the question," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 2, pp. 1–20, 2019.

[38] B. R. Swain, J. J. Sahoo, A. Prasad, and D. T. Selvam, "Rise of fluid computing: A collective effort of mist, fog and cloud," 2019.

[39] J. S. Preden, K. Tammemäe, A. Jantsch, M. Leier, A. Riid, and E. Calis, "The benefits of self-awareness and attention in fog and mist computing," *Computer*, vol. 48, no. 7, pp. 37–45, 2015.

[40] M. K. Yogi, K. Chandrasekhar, and G. V. Kumar, "Mist computing: Principles, trends and future direction," *arXiv preprint arXiv:1709.06927*, 2017.

[41] D. Vasconcelos, V. Severino, J. Neuman, R. Andrade, and M. Maia, "Bio-inspired model for data distribution in fog and mist computing," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, vol. 2, 2018, pp. 777–782.

[42] M. Suárez-Albela, P. Fraga-Lamas, and T. M. Fernández-Caramés, "A practical evaluation on rsa and ecc-based cipher suites for iot high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, 2018.

[43] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," in *2014 Australasian telecommunication networks and applications conference (ATNAC)*, IEEE, 2014, pp. 117–122.

[44] Y. Zhang, D. Niyato, and P. Wang, "Offloading in mobile cloudlet systems with intermittent connectivity," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2516–2529, 2015.

[45] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless communications and mobile computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[46] M. H. Au, K. Liang, J. K. Liu, R. Lu, and J. Ning, "Privacy-preserving personal data operation on mobile cloud—chances and challenges over advanced persistent threat," *Future Generation Computer Systems*, vol. 79, pp. 337–349, 2018.

[47] T. Leppänen and J. Riekki, "Energy efficient opportunistic edge computing for the internet of things," in *Web Intelligence*, IOS Press, vol. 17, 2019, pp. 209–227.

[48] K. Sekaran, G. R. Vikram, and B. Chowdary, "Design of effective security architecture for mobile cloud computing to prevent ddos attacks," 2019.

[49] T. H. Noor, S. Zeadally, A. Alfazi, and Q. Z. Sheng, "Mobile cloud computing: Challenges and future research directions," *Journal of Network and Computer Applications*, vol. 115, pp. 70–85, 2018.

[50] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the internet of things," in

2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), IEEE, 2015, pp. 603–608.

[51] G.-a. Zhang, J.-y. Gu, Z.-h. Bao, C. Xu, and S.-b. Zhang, "Joint routing and channel assignment algorithms in cognitive wireless mesh networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 3, pp. 294–307, 2014.

[52] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[53] E. Ahmed and M. H. Rehmani, *Mobile edge computing: Opportunities, solutions, and challenges*, 2017.

[54] V. Vassilakis, I. P. Chochliouros, A. S. Spiliopoulou, E. Sfakianakis, M. Belesioti, N. Bompetsis, M. Wilson, C. Turyagyenda, and A. Dardamanis, "Security analysis of mobile edge computing in virtualized small cell networks," in *IFIP International Conference on Artificial Intelligence Applications and Innovations*, Springer, 2016, pp. 653–665.

[55] M. T. Beck, M. Werner, S. Feld, and S. Schimper, "Mobile edge computing: A taxonomy," in *Proc. of the Sixth International Conference on Advances in Future Internet*, Citeseer, 2014, pp. 48–55.

[56] M. T. Beck and M. Maier, "Mobile edge computing: Challenges for future virtual network embedding algorithms," in *Proc. The Eighth International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2014)*, Citeseer, vol. 1, 2014, p. 3.

[57] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, IEEE, 2016, pp. 20–26.

[58] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[59] F. Manco, J. Martins, K. Yasukata, J. Mendes, S. Kuenzer, and F. Huici, "The case for the superfluid cloud," in *7th {USENIX} Workshop on Hot Topics in Cloud Computing (HotCloud 15)*, 2015.

[60] M. Peng, C. Wang, V. Lau, and H. V. Poor, "Fronthaul-constrained cloud radio access networks: Insights and challenges," *IEEE Wireless Communications*, vol. 22, no. 2, pp. 152–160, 2015.

[61] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5g on the horizon: Key challenges for the radio-access network," *IEEE vehicular technology magazine*, vol. 8, no. 3, pp. 47–53, 2013.

[62] M. D. Assuncao, F. L. Koch, and C. B. Westphall, "Grids of agents for computer and telecommunication network management," *Concurrency and Computation: Practice and Experience*, vol. 16, no. 5, pp. 413–424, 2004.

[63] M. D. De Assuncao, F. L. Koch, and M. A. S. Netto, *Content delivery infrastructure with non-intentional feedback parameter provisioning*, US Patent 9,590,875, 2017.

Wesley dos Reis Bezerra is a Professor at the Federal Institute of Santa Catarina, Campus Rio do Sul, and PhD candidate at PPGCC, UFSC. He obtained his Master in Engineering and Knowledge Management from EGC, UFSC. He holds a Bachelor of Information System from INE, UFSC, and a Bachelor in Business Administration from Estácio de Sá University.

Fernando Luiz Koch is a Visiting Researcher at PPGCC, UFSC, and Data & AI Solution Architect with IBM. He dedicated the past 25 years of his career in advancing Data & AI and Cloud Computing. He holds a PhD in Computer Sciences (2009) from the Utrecht University, with a thesis about the use of AI to improve Mobile Services; M.Sc. and B.Sc. in Computer Sciences from INE, UFSC. He published 6 co-edited books, 35+ patents and 70+ papers.

Carlos Becker Westphall Carlos Becker Westphall is Full Professor at the Federal University of Santa Catarina since 1993, acting as leader of the Network and Management Group, founder and supervisor of the Network and Management Laboratory. PhD in Informatics, specializing in "Network and Service Management" at the Université de Toulose (Paul Sabatier), France in 1991. Master in Computer Science in 1988 and Electrical Engineer in 1985, both from UFRGS. He is the author and / or co-author of more than 470 publications. In 2011 he received the "Awarded IARIA Fellow". He is (and was) a member of the Editorial Board of more than a dozen journals. Serves (and has served) as a member of the organizing and / or program committee for hundreds of conferences. Has experience in Computer Science and Telecommunications, with emphasis on Administration and Management of Networks and Services, acting mainly on the following themes: security, autonomic computing, cloud computing and Internet of Things. He founded the LANOMS conference (Latin American Network Operations and Management Symposium). He also provided services: for IEEE acting on CNOM (Committe on Network Operation and Management); for IFIP acting in "WG6.6 - Management of Networks and Distributed Systems"; to Elsevier as editor of COMNET (Computer Networks Journal); to Springer as senior editor at JNSM (Journal of Network and Systems Management) and to IARIA (International Academy, Research, and Industry Association) as Latin America - IARIA Liaison Board Chair.