Procedure for the Deployment of Fog Computing Use Cases

Liz Gámez Picó and Caridad Anías Calderón

Faculty of Informatics, GTEC, University of A Coruña, 15071 A Coruña, Spain
Technological University of Havana. "José Antonio Echevarría", CUJAE, 19390, Havana, Cuba
Correspondence: liz.gamez@udc.es

DOI: *https://doi.org/10.17979/spu.23.c18*

Abstract: Fog Computing (FC) emerges in response to the demands of the Internet of Things, which requires lower latency, greater security, and the capacity to manage multiple devices. Its implementation poses challenges due to the diversity, mobility, scalability, and interoperability of the elements involved. This work aimed to define the key elements for designing and deploying fog computing systems. A study of the state of the art was conducted, and a procedure composed of six stages was proposed, with technical aspects and recommendations in each. The procedure was validated through its application to a video surveillance use case, with satisfactory results.

1 Introduction

The emergence of the Internet of Things (IoT) facilitated the development of new technologies due to its versatility and location in varied scenarios, performing tasks automatically and working with information in real time. This created an avalanche of data on the network, and the emergence of new applications for this technology, which conditioned the appearance of new paradigms that attempted to solve the needs of storing and processing large amounts of information, in the shortest possible time. The cloud-centric execution of IoT applications fails to fully meet these needs, as cloud data centers are generally distant from IoT devices. Due to this, the idea of a cloud extension at the network edge, introduced the fog computing (FC) approach, allowing these applications to run closer to the data sources. In this way, fog computing can improve the service delivery time of IoT applications and decrease network congestion Mann (2021). Although the OpenFog Consortium was created in 2015, a consortium of high-tech industry companies and academic institutions from around the world whose objective is the standardization and promotion of fog computing in various capacities and fields, it is important to note that within the scope of standardizing this technology, much remains to be defined Pinzón Castellanos (2020). The main objective of this work is to design a guide that considers the elements to take into account for the design and deployment of an FC system, based on recent research and best practices, in which each of the layers of the OpenFog architecture and solutions that enable the design of heterogeneous and interoperable systems are present.

2 Theoretical Framework

The growing interest in the topic of fog computing networks made it necessary to create a referential architecture, which would serve as a standard for the deployment of this technology, meeting the existing requirements and expectations surrounding the paradigm. To this end, the OpenFog consortium was created, formed by the main institutions in the industry IoT Futura

(2018). In 2017, a reference architecture for FC was published by the aforementioned consortium with the objective of helping engineers and developers understand the needs and particularities of FC systems. Later, the IEEE would announce the use of this architecture by the IEEE 1934-2018 standard IEEE Communications Society (2018), and this standard is what was used for the development of the present research. The Fog Computing architecture defined by OpenFog is based on a set of basic principles called pillars, which represent the key attributes that a system needs to incorporate to be defined as an FC system Adnan Mahmood (2018).

3 Guide for the Deployment of Fog Computing

The guide for the design and deployment of FC that is proposed consists of a set of well-defined stages, which guide all the aspects that have been considered important for implementing a project or deploying a fog computing application case from scratch. A Top-Down approach is followed, with the objective of achieving a final deployment that fully responds to the needs and objectives of the project to be implemented, and security aspects must be considered in each of the stages, due to their importance in FC.

3.1 First Stage

In the first stage, "Characterization and definition of objectives" see Figure 1, a general description of the project and its objectives is made, and the functional, non-functional, and security requirements of the system are specified, based on the needs of the use case. Furthermore, the FC applications intended to be implemented must be specified in detail, and a characterization of the pre-existing infrastructure and environmental parameters is performed. Finally, it is defined what type of data Sinaeepourfard et al. (2017) will be handled and how and where it will be processed. Also, the security measures that must be taken throughout the entire solution are analyzed. Within the functional requirements are the functions or services expected to be resolved by the project, as well as the most detailed possible definition of the set of inputs, behaviors, and outputs. It is important to define: necessary capabilities related to computation, storage, and connectivity of IoT devices; bandwidth and latency parameters required in the area network; types of metrics to be obtained; expected data processing; alerts and report periodicity; where the historical analysis and storage of data will be performed; among others. For the definition of non-functional requirements, the eight pillars of FC must be taken into account: Security, Scalability, Openness, Autonomy, Programmability, RAS, Agility, and Hierarchy. Specify security requirements, keeping in mind that the main security problems in FC implementations are: access control, authentication, data protection, intrusion detection, privacy, and reliability. Data classification must be based on five fundamental aspects: type of data; volume of data; latency requirements; bandwidth requirements; and privacy requirements. Once the main characteristics of the project are detailed, it is important to define whether a fog computing approach is really needed or if a traditional cloud computing architecture would be sufficient Chakraborty (2019).

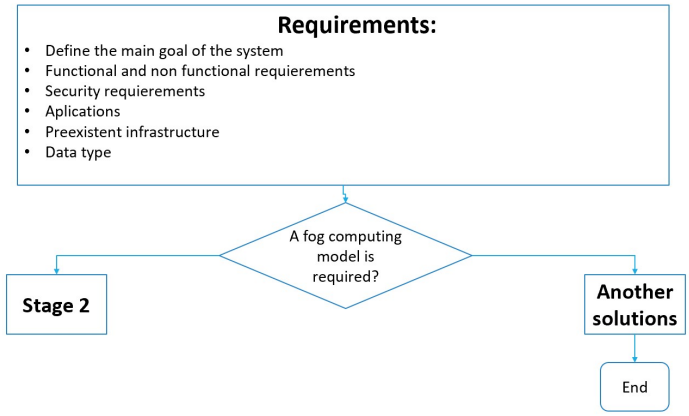

Figure 1: Stage 1. Characterization and definition of objectives.

3.2 Second Stage

Based on the objectives set, a logical design must be carried out, which defines the hierarchical deployment model, the generic elements required by the fog network and its topology, the interconnection technology to be used, the types of software needed, the characteristics that the management systems must have, the communication protocols, among others. Each fog node must be autonomous to guarantee the uninterrupted operation of the infrastructure it manages. One of the elements that conditions this decision is the definition of where the analysis and storage will be performed, and it is closely related to the volume of data generated by the sensors and the immediacy of their processing. Most scenarios fall into cases two and three described in the reference architecture. Partiendo de la selección del modelo jerárquico de despliegue de la FC y habiendo definido la cantidad de dispositivos IoT, así como un estimado del volumen de datos a generar por cada uno de ellos, es importante definir el número de niveles niebla que demanda el caso de uso y la cantidad de nodos nieblas en cada nivel. Para poder aplicar el análisis se debe partir de conocer la cantidad de datos generados por cada sensor, la cantidad de datos a almacenar, la capacidad de almacenamiento del nodo niebla y su capacidad de procesamiento. El aspecto clave para decidir la implementación o migración de funcionalidades entre los niveles niebla más bajos y los niveles medios, según lo requiera el escenario, es principalmente la latencia que soporte la aplicación y la capacidad de procesamiento de los nodos. Los nodos niebla se pueden agrupar de acuerdo a la distribución geográfica, tipos de datos, aplicaciones niebla que implementen, entre otros. Cada uno de los niveles niebla realizan funciones específicas: monitoreo y control, soporte a la operación o soporte al negocio. Starting from the selection of the hierarchical FC deployment model and having defined the number of IoT devices, as well as an estimate of the data volume to be generated by each, it is important to define the number of fog levels demanded by the use case and the number of fog nodes at each level. To apply the analysis, one must know the amount of data generated by each sensor, the amount of data to be stored, the storage capacity of the fog node, and its processing capacity. The key aspect in deciding the implementation or migration of functionalities between the lower fog levels and the middle levels, as required by the scenario, is mainly the latency supported by the application and the processing capacity of the nodes. Fog nodes can be grouped according to geographical distribution, data types, fog applications they implement, among others. Each of the fog levels performs specific functions: monitoring and control, operational support, or business support.

3.3 Third Stage

In this stage, the elements that make up the fog network must be selected, that is, the sensors and actuators, the fog nodes, the cloud platform, and the management system, see Figure 2. The selection of sensors and actuators will depend on factors such as power consumption, protocols used, measurement range, processing capabilities, product reliability, costs, environmental conditions, among others. Although all devices can function perfectly independently, in many projects, it is necessary to integrate their operation into what is called a sensor network, so that conditions in different locations can be monitored. To choose the sensors, one must take into account the type of sensor (temperature, humidity, pressure, etc.), its detection range, the type of power supply, the security and management options it presents, as well as the communication protocol it uses. Regarding the actuators, one must consider the method they use to execute an action (pneumatic, hydraulic, or electronic), the time it takes to execute said action, the communication protocol it uses, and the management and security options it presents. In Toledo B. and Martínez Hernandez (2017) comparative tables of different types of sensors and actuators can be found. For the selection of fog nodes, three elements must be considered: hardware, virtualization (optional), and software.

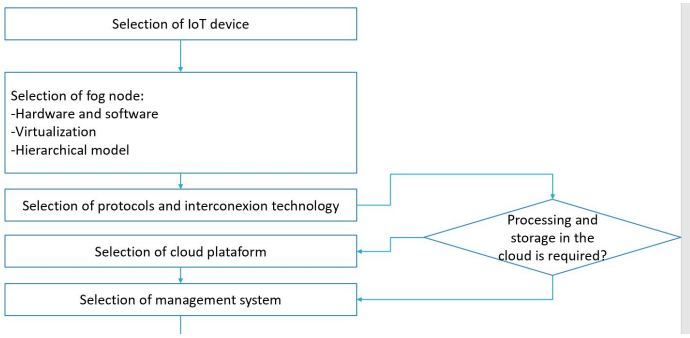

Figure 2: Stage 3. Selection.

The main elements recommended to take into account for the selection of the fog node hardware are: the type of device (router, switch, access point, or general-purpose hardware, such as a Raspberry Pi), whether they support the selected fog software, the communication protocols they use, whether they are designed to withstand the environmental conditions defined in stage 1 of the project, the resources they possess, as well as the management and security options they present. Furthermore, it is very important to consider their computing characteristics such as their processing capacity, storage capacity, and RAM capacity. Hardware-based virtualization mechanisms are available in almost all hardware used to implement fog software. It is recommended that processing, acceleration, storage, and networking functions be virtualized in the fog nodes, in order to maximize the efficiency and flexibility of the system. The selection of fog system software to implement a specific use case is also very important. The fog software will be installed on the hardware devices deployed in the fog layer, providing it with possibilities for interoperability with sensors and the cloud platform; resource and data management; programmability and processing agility; among others. Said software must comply with the eight pillars described in the reference architecture for FC, and especially those defined as most important in Stage 1. For the selection of fog software, it is recommended to analyze the following requirements: scalability, free/open-source software solution, communication protocols, interoperability, usability, and security/privacy. Security considerations For the service security layer, the following are recommended: deep packet inspection, application layer proxy, legal message interception, intrusion detection and protection systems, monitoring of system and network events and status. For the protection of the fog system software, it is

recommended to deploy the following security measures: Secure, periodic, and authenticated software updates, perform backups of equipment configurations, change default passwords on devices, and establish access control mechanisms for the use of the system software. For the selection of the cloud platform, it is recommended to consider: whether it is free or paid, the security options it has, such as: access control, data encryption, etc.; the databases it works with; the possibilities for virtual servers, container management, and selection of general-purpose computing instances it has, which offer a balance of compute, memory, and network resources; if it has support service for distributed applications; if it allows resource configuration tracking; if it has tools for alert monitoring; if it enables integration with existing infrastructure; and if it contains tools for data analysis. For the protection of applications deployed on the cloud platform, it is recommended to deploy the following security measures: establish access control mechanisms for the use of applications; login monitoring; critical file monitoring; perform vulnerability scanning tests on applications and take protective actions; encryption of the data being handled; among others.

3.4 Fourth Stage

This "Simulation" stage is very necessary as it allows for testing and verifying, to a certain extent, that the FC system design effectively achieves the proposed objectives, see Figure 3. The use of the iFogSim simulator and the application of the simulation procedure described in Gámez et al. (2020) is proposed, which generalizes the main elements to consider for evaluating diverse and comprehensive FC application scenarios.

3.5 Fifth Stage

Once the simulation results have been successful, we move to the fifth stage, "Physical Design", where the network documentation is prepared and the corresponding configurations are defined in each of the software tools. To complete the design of the FC system, it is essential to document it, for which a physical design is required to define details that may be missing from the logical design, such as addressing. The following aspects must be defined and included in the network management system: physical diagrams of the FC system; types of cables used; the length of each cable; the termination type of each cable; the geographical location in the physical structure; labeling scheme for easy identification; addressing; among others. A detailed description of the complete inventory of all devices used must also be included, for example, for the organization of inventory sheets, the following information should be available: device serial number; physical location; full memory description; connection interfaces; supported protocols; peripherals in general (Brand, model, type); general comments about the device; installed software; software license. Regarding security requirements, in this stage, all user policies must be well described, meaning all user permissions and how they interact with the FC system must be established.

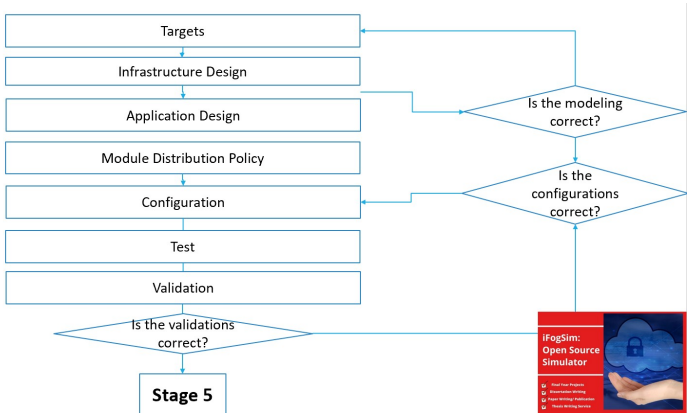

Figure 3: Stage 4. Simulation.

3.6 Sixth Stage

Finally, it culminates with the "Implementation" stage, where the hardware and software are configured and tests are performed to validate their correct functioning, thus implementing the FC system and the guidelines for its constant management. It is divided into three phases: field tests, FC system deployment, and continuous management. The testing stage is extremely important since it verifies if all elements of the FC system function correctly, before moving on to the project's deployment with the certainty that the proposed objectives will be met. Subsequently, and on an ongoing basis, it is recommended to manage the implemented fog computing solution, enabling corrective actions to be taken in order to maintain and improve the performance of the deployed system. Among the metrics to monitor are: amount of time the service is available, delays, bandwidth, throughput, and response speeds; reliability and availability in message exchange; error percentages in message exchange, among others.

4 Application of the Guide for Fog Computing Deployment to a Use Case

The research results were applied to a video surveillance use case; the implementation stage was carried out on a small scale using lower-performance devices that allowed verifying the functionality of the designed FC system. This implementation was developed as part of collaborative projects with the Faculty of Telecommunications and Electronics at CUJAE and a company in the ICT sector, within the framework of University-Enterprise agreements.

By applying the proposed guide, it was possible to adapt the use case solution to the pre-existing infrastructure elements of the Video Surveillance Systems (CCTV) for Control, Security, and Protection of the company. iSPY was proposed as software for camera management and video processing in the fog nodes. The simulation of the scenario using the iFogSim tool demonstrated the feasibility of using the fog computing system and its scalability. The last stage, implementation, could only be carried out in a reduced scenario. In light of the results obtained, it is considered that the objectives and requirements of the use case were met and that it is feasible for the company Tecnomática to migrate its CCTV system to the designed FC system, without loss of reliability and providing benefits such as increased scalability, decreased bandwidth consumption, and reduced latency.

5 Conclusions

In this article, the proposed guide for the deployment of fog computing was presented, which consists of six well-defined stages, in each of which aspects of interest to consider and recommendations were detailed. In stage 1, all requirements and general characteristics of the project must be clearly and precisely described, to later analyze if an FC approach is required. In stage 2, the hierarchical deployment model is defined, as well as other aspects of interest. In stage 3, the selection of the basic elements that make up the fog network is carried out, which is decisive for the rest of the stages. The procedure does not select the elements that make up the FC system, but rather provides criteria for the selection of sensors and actuators, fog nodes, the cloud platform, communication protocols, access and interconnection technologies, and the management system. Security is a fundamental pillar within an FC system; it is an aspect that must be given special attention during the project implementation, which is why it is an element that must be considered in each of the procedure's stages. In stage 4, the use of the iFogSim simulator is proposed, and three phases are highlighted: formulation, design, and simulation. In stage 5, the network documentation is carried out, and the corresponding configurations are defined in each of the tools, which will be used later in the deployment of the FC system. Network documentation is very important to complete the design of an FC system. In stage 6, conducting field tests is extremely important to verify the correct functioning of the proposed design before its total deployment. The FC system must be managed and monitored continuously to ensure its correct functioning. The proposed procedure can be used in various FC use cases.

Bibliography

H. Z. Adnan Mahmood. Toward edge-based caching in software-defined heterogeneous vehicular networks. In *International Conference on Smart Cities*, 2018.

M. Chakraborty. Fog computing vs. cloud computing, 2019.

L. Gámez, C. Calderón, Y. Rollón, and D. Frómeta. Procedimiento de simulación de redes de computación en la niebla. *Revista Tono*, 16, 2020.

IEEE Communications Society. IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing. Technical report, IEEE, 2018. [En línea; consultado en la fecha en la que se accede].

IoT Futura. OpenFog, la arquitectura de referencia para el Fog Computing. *https://iotfutura.com/2018/07/openfog/*, 2018. [En línea; consultado en la fecha en la que se accede].

Z. Mann. Notions of architecture in fog computing. *Computing*, 103:1–23, jan 2021.

J. Pinzón Castellanos. *Implementación de una arquitectura fog computing*. PhD thesis, Universidad autónoma de Bucaramanga – UNAB Facultad de ingeniería, Maestría en gestión, aplicación y desarrollo de software, Bucaramanga, 2020.

A. Sinaeepourfard, J. Garcia, X. Masip-Bruin, and E. Marin-Tordera. A novel architecture for efficient fog to cloud data management in smart cities. In *IEEE International Conference on Smart Cities*. IEEE, 2017.

A. Toledo B. and A. Martínez Hernandez. Procedimiento para ofrecer servicios m2m por parte de una empresa de telecomunicaciones, 2017. Disponible en la base de datos del Centro de estudios para las Telecomunicaciones y la Informática (CETI).