Ramon Martin de Pozuelo

Researcher
FUNITEC - La Salle R&D
http://lasallerd.salleurl.edu/

Bilateral Meetings

- Wednesday (2:00pm - 4:00pm)
- Wednesday (4:00pm - 6:00pm)
- Thursday (10:00am - 12:00pm)
- Thursday (12:00pm - 2:00pm)
- Thursday (2:00pm - 4:00pm)
- Thursday (4:00pm - 6:00pm)

Description
Research Group on Internet Technologies and Storage (GRITS) (http://lasallerd.salleurl.edu/Redes) of the centre
FUNITEC - La Salle, of Ramon Llull University. We are active in many R&D projects in the area of Computer Networking
and Cybersecurity especially in the fields of Smart Grids and Smart Cities. Most recent European projects: FP7
INTEGRIS, FI-PPP FINESCE.
Organization Type
University
Organization Size
Yes, I need an Exhibition Visitor Pass Discount Code
Areas of Activities

TECHNOLOGY

1. city platform
2. sensors
3. Internet of things cloud
4. big data
5. networks
6. high technology
7. standardization
8. security

ENERGY

1. renewables

2. grid architecture
3. efficiency
4. management
5. ICT
6. electricity
7. metering

Offer

Software Defined Utility - Security

La Salle proposal is to continue developing a complete framework for a Software Defined Utility (SDU) approach, which we started in FINESCE project (FI-PPP Smart Energy use case) together with other industrial (utilities, telcos, hardware vendors, etc.) and academic partners.

In the case of the Smart Grid and more concretely in the electricity distribution network a huge amount of data collected is processed continuously. Nowadays it is treated usually by dedicated and highly expensive devices. Relying on our own expertise and experience from a long-term collaboration with utilities, and the complementary knowledge of the other FINESCE partners, we advocated for the SDU concept where many of the functions that those devices do will rely on programmable commodity hardware, low-cost sensors, and high-speed and reliable IP-based communications underneath.

As fundamental pieces of this approach, we defined single, yet distributable, devices (called FIDEVs, FInesce DEVices), which will integrate the needed functions for it:

i. Hybrid Cloud data storage system (FIDEV distributed storage system and external cloud storage connection).

ii. Identity management and access control system.

iii. High-speed and reliable communication interfaces and management.

iv. Special functions to improve latency, reliability and QoS.

v. RTUs and Smart Meters data collectors.

vi. Support for Smart Grid functions.

Those FIDEVs are targeted to be placed at different electrical distribution network points (e.g. secondary substation) and interconnected, considering the following list of potential applications to be developed over FIDEVs architecture:

• Remote electrical fault information (oscillography) recovery;

• Remote access from substation to central servers;

• NMS (Network Management System) and management of communications network;

• Secondary substations distributed SCADA (Supervisory Control And Data Acquisition);

• Substation surveillance (video storage and communication for physical security and surveillance equipment control);

• Physical access security (e.g. including centralized identity management and ID card reader control);

• Self-healing network functions: current, voltage and environmental asset conditions monitoring and alarm setting;

• DER monitoring and control.

• VoIP substation intercommunication;

Given the criticality of most of those applications, the level of security that those devices should provide must achieve

really high standards. The required cybersecurity assessment of the data storage infrastructure was done during the FINESCE project, starting from a general study of the security requirements in Cloud Computing environments, and then extracting the concrete threads, and potential vulnerabilities found in the proposed storage platform for FINESCE. La Salle proposed to continue developing the security framework to protect those devices, while searching for partners to collaborate in new projects, helping in the development of some of those potential abovementioned applications. FIDEV platforms could derive in a product in the future. However, FIDEVs are not mature enough yet to be the elemental management piece for the "Software Defined Utility" approach. They represent an opportunity for utilities to have more flexible devices (based on software, upgradable, configurable, able to deploy new applications above them), allowing them a lower-cost distribution grid management, as well as providing them means to share their data (from electric vehicle (EV) charging points, smart metering or substation monitoring) to third parties. It can foster new business models, such as selling specific region smart metering data to ESCOs or retailers, providing them high-value information, or EV information to mobility.

Cooperation Offered

1. Outsourcing co-operation
2. Technical co-operation

Cooperation Requested

1. Outsourcing co-operation
2. Technical co-operation
3. Investment/Financing

Offer

Software Defined Utility

Based on the developments made in previous European projects -INTEGRIS (FP7) and FINESCE (FP7 FIWARE)- we provide a Hybrid Cloud solution that was initially designed to overcome the reluctance of utilities and the energy sector in general to rely on cloud platforms, public or private. However, the results from those projects are not strictly tied to the Smart Grids and Smart Energy field, and could become valuable assets to be applied for managing data in other Smart Cities' scenarios (Smart Districts, Smart Buildings, Smart Campus, etc.) or enterprises.
In the case of the Smart Grid and more concretely in the electricity distribution network a huge amount of data collected is processed continuously. Nowadays it is treated usually by dedicated and highly expensive devices. In FINESCE project we advocated for a Software Defined Utility (SDU) concept where many of the functions that those devices do will rely on programmable commodity hardware, low-cost sensors, and high-speed and reliable IP-based communications underneath. For building up this concept we started to develop a storage system adapted to the requirements of the Smart Distribution Grid (e.g. very low latency, high-availability, data processed in spread locations, etc.), and can handle properly the data generated at the costumer (smart meter), aggregator or substation level. We consider it a fundamental piece of the SDU, so it will allow to sustain the data of Smart Grid applications that can be centralized but also easily distributed and residing in different points of the distribution grid and in the cloud. At the end, we aimed at establishing a distributed storage system that provides high-availability and reduces the latency in

acquiring data from the local sites of the utility while offering a secure solution to share data information with external stakeholders.

It resulted on a hybrid cloud storage platform based on Openstack and FIWARE tools and services. On the one hand, a distributed storage system has been deployed among several interconnected devices (that we called FIDEVs -FInesce DEVices-) located in different substations, shaping all together a spread in-house private cloud storage service for the utility. On the other hand, additional cloud storage functionalities were configured over the FIWARE Lab, emulating a commercial public cloud service.

Some assets are provided to complete the solution, such a single API that allows interaction with both storage systems and a graphical interface that allows data managers to easily manage the data and select where to store it, in the private or public cloud, migrating the data when necessary. It also includes also another GUI that helps the fast configuration of the platform, the data replication time, triggers and different levels of locations.

Besides all of that, an extensive knowledge of the group was acquired on cloud metrics analysis in generic and in the Smart Distribution Grid scenarios, designing a methodology to build resource allocation recommendation system, an orchestrator that can select or recommend the optimal place of a specific cloud service, in the private or in the public cloud infrastructures.

Last but not least, security aspects are specially taken into account by the group, and they provided their expertise and experience in the past to make exhaustive security analysis, such as the one undertaken to the cloud platform as a whole that was designed for FINESCE, and the different FIWARE Generic Enablers used.