energies

MDPI

Article

Prototyping a Software Defined Utility

Ramon Martín de Pozuelo *, Agustín Zaballos, Joan Navarro and Guiomar Corral

GRITS—Research Group in Internet Technologies and Storage, La Salle-Ramon Llull University, Barcelona 08022, Spain; zaballos@salleurl.edu (A.Z.); jnavarro@salleurl.edu (J.N.); guiomar@salleurl.edu (G.C.)
* Correspondence: ramonmdp@salleurl.edu; Tel.: +34-93-290-2475

Academic Editor: Antonello Monti
Received: 3 April 2017; Accepted: 13 June 2017; Published: 16 June 2017

Abstract: The smart grid can be seen as a hybrid system composed by many systems. From a large scale point of view, it combines the electric power system itself and a heterogeneous information and communication technology (ICT) infrastructure. Additionally, these systems are composed by many building blocks that are designed and managed as separated systems which are hard to fully integrate between each other. Relying on the experiences arisen and the knowledge gathered from the partners during the development of the FP7 European projects INTEGRIS (intelligent electrical grid sensor communications) and FINESCE (future internet smart utility services), this paper presents the software defined utility (SDU) concept for the management of the smart grid and its security, which advocates for the migration of the utility infrastructure to software systems instead of relying on complex and rigid hardware based systems. Following this approach, SDU proposes the evolution of power systems' ICT and the usage of programmable commodity hardware, low-cost sensors, and reliable high-speed IP-based communications underneath. More concretely, this paper proposes some building blocks for the deployment of the SDU (flexible data management infrastructure, context-aware security and web of things interface) and evaluates their functionalities and benefits for the smart grids of the future.

Keywords: smart grids; ICT; network management; data management; security; internet of things; software defined network

1. Introduction

Power network technologies have been exceptionally stable for a long time, which is in contrast with the fast evolution of current information and communication technologies (ICT) systems. One of the main novelties of the smart grid is the addition of a telecommunications network to the electrical infrastructure in order to transport information such as the state of the grid, real-time power consumption, service fault locations, demand side management, etc. Hence, smart grids are aimed to ensure that the power grid is economically efficient, sustainable and provides high standards of power quality thanks to a lower level of losses and enhanced power management and security [1]. However, smart grid general requirements [2] still present some concerning issues on the integration of telecommunications and electric power networks. In fact, smart grid evolution originates many operational problems that cannot be solved by current systems and technologies, especially if they are used in an isolated way. Fortunately, the evolution and current maturity of ICT systems makes it possible to cope with these problems, especially over the distribution grid where current ICT systems are scarcely deployed.

Indeed, the smart grid can be best seen as a hybrid system composed by many subsystems. From a large-scale point of view, it combines the electric power system domain with a heterogeneous ICT infrastructure [3]. At the same time, these subsystems are composed by a bunch of building blocks that are hard to fully integrate between each other [3] and, thus, some partial solutions that rely on

dedicated and highly expensive devices have been proposed so far [2]. However, these suboptimal solutions committed to address specific and constrained concerns, are no longer feasible given the ever-rising spectrum of services that smart grids aim to offer and the enormous costs associated to their deployment and maintenance [2]. Therefore, there is an increasing need for a standard and broad-range solution able to cover the smart grid demands as a whole—from the electric layer to the services plane—in a cost-effective and scalable way.

Specifically, the main demands of smart grids revolve around: (1) the adaptation of the electrical network infrastructure to new topologies that improves the resilience and self-healing capacity of the grid; (2) new monitoring strategies, based on decentralized service-oriented architectures that can address the huge amount of information collected in the smart grid ecosystem; and (3) the cyber security of the whole smart grid and the associated concerns about the privacy of the obtained energy data [2,4]. Indeed, smart grids, and more concretely electricity distribution networks, suppose a valuable data source that generates a massive amount of data that needs to be collected and processed continuously, which stresses even more the significance of the three aforesaid smart grid challenges.

In recent years, new network models referred to as software defined networks/anything (SDN/SDx) [5] in conjunction with service composition [6,7] have emerged as powerful tools and methodologies for managing future network architectures that propose modularity, adaptability and centralized management of the communication system. During the participation of the authors in the development of the FP7 European projects FINESCE (future internet smart utility services) [8] and INTEGRIS (intelligent electrical grid sensor communications) [9], it has been shown that the characteristics featured by these novel network models match with the aforesaid smart grid demands, not only in terms of scalability, standardization and maintenance, but also in cyber security. Therefore, the authors advocate for the adoption of the software defined utility (SDU) concept [4] to address the management of the smart grid and its security.

The objective of this paper is to propose a new way of managing the smart grid based on the SDU paradigm coined by the authors, that aims at enabling a more flexible operation of the power infrastructure and, thus, sharing the on-field experiences and knowledge collected in [8,9]. As it is further discussed in this work, the benefits of using this software-based approach are manifold. First, many of those smart functions [10] that are currently undertaken by expensive dedicated devices will rely on programmable commodity hardware, low-cost sensors, and a reliable high-speed communications network. Next, SDUs can adapt themselves to the intrinsic heterogeneity of the smart grid in order to effectively conduct monitoring duties by collecting and processing real-time data, taking advantage of service-oriented decentralized architectures, and properly configuring each specific internet of things (IoT) device and its communication services separately. In addition, SDUs can handle the variable privacy requirements and the security threads arisen from the interconnection of the power grid to an IED-based (intelligent electronic devices) communication network by providing security functionalities on-demand and, only if necessary, adapting their operation to each specific area and function of the smart grid. Finally, distribution system operators (DSOs) aim at self-adapted and context-aware applications deployed that efficiently adapt to the highly dynamic and heterogeneous environment of the smart grid [11]. These features provided by SDUs contribute to the autonomic behavior of the smart grid by actively reacting against possible isolation of some parts from the main network. Overall, this paper discusses the relevance of the SDU concept in the smart grid domain and prototypes an architecture to exhibit the feasibility of this alternative approach. The contributions of this paper are the following:

- A definition of an SDU-based distributed storage architecture for the smart grid data.
- A state-of-the-art review of the security mechanisms to obtain high reliability in the smart grid.
- A proposal of an SDU that meets the cyber security requirements of data in a smart grid.
- A secure web of things based interface to manage the smart grid assets and data.

The remainder of the paper is organized as follows. Section 2 introduces the concept of SDU and proposes its building blocks. Subsequent sections detail the advances in the design and development of the SDU architecture: hybrid cloud data management (Section 3), context-aware security (Section 4) and web of energy (Section 5). Section 6 exposes the impact that SDU approach can bring to the smart grid operation efficiency and automation. Section 7 presents an experimental evaluation made from the ICT and electrical power network management perspectives. Finally, Section 8 presents some conclusions and further work to be done continuing the development of the SDU prototype.

2. A Flexible and Context-Aware Smart Grid Infrastructure

All of the functionalities proposed by a smart grid require a high degree of network control that increases the complexity in its management [11]. The boost on distributing and virtualizing electrical resources requires new methodologies that simplify the tasks of the administrators in electrical distribution networks [8]. In this sense, the advances on computer network architectures and their management could give a hint about how it could be done. Thus far, there are two emerging trends in computer networks that present capabilities completely aligned with the specific needs of the smart grid.

On the one hand, the appearance of SDN/SDx presents a way to manage highly distributed resources in a more autonomous and centralized way. For instance, they can program certain type of resources to be adapted on the fly by themselves (self-configuration). In fact, SDN/SDx aim to decouple the network control plane from the data plane [12]. Therefore, one of the main advantages of SDN/SDx is the network abstraction to unify and centralize the network management. Abstraction gives network administrators a simplified global vision of the whole network infrastructure. In addition, it allows system architects to achieve greater scalability and an easy integration with different middleware, even on demand (i.e., using a cognitive system able to learn, react and configure the network according to certain parameters [13]). This will make the network act like a living organism that adapts itself to certain situations boosting its versatility and ease of operation.

On the other hand, service-oriented architectures and service composition for smart grids have evolved dramatically, which has brought several advantages [3,10,14]. Specifically, this technology is widely spread in the world of web-services. It presents a way of modularizing the system functionalities as small independent services that can be published, placed, invoked and combined together with other services, to run them remotely and on demand.

The authors claim that the combination of both information and operational technologies (i.e., IT and OT), by means of SDN/SDx and service composition, could make a great impact in the development of smart grids in the following years. Moreover, this paper takes into account the mandatory low latency required in smart grid communications and that the resources of the distribution electrical grid such as generators, storage devices or actuators are increasingly becoming more spread [15]. First steps in this direction have been already made when considering the necessity of total protection against failures in smart grids, which has driven practitioners to research different solutions and propose an orchestrator for handling redundancy in different types of networks. This strategy has shown to be efficient at tackling the stringent requirements when recovering services from a failure in the system, even though an overload is introduced on it [1,13]. Therefore, it has been shown that the performance depends on the status and characteristics of the underlying communications network.

This paper revolves around the forthcoming smart grid digital transformation towards an intelligent programmable network based on SDUs. Actually, SDUs can be implemented by translating the philosophy, concepts and technologies from the SDN/SDx and service composition to smart grids IT and OT requirements. In this regard, three different architectural pieces of this SDU concept (Figure 1) have been considered as a first step for its prototyping [4] by conforming a functional pretotype [16].

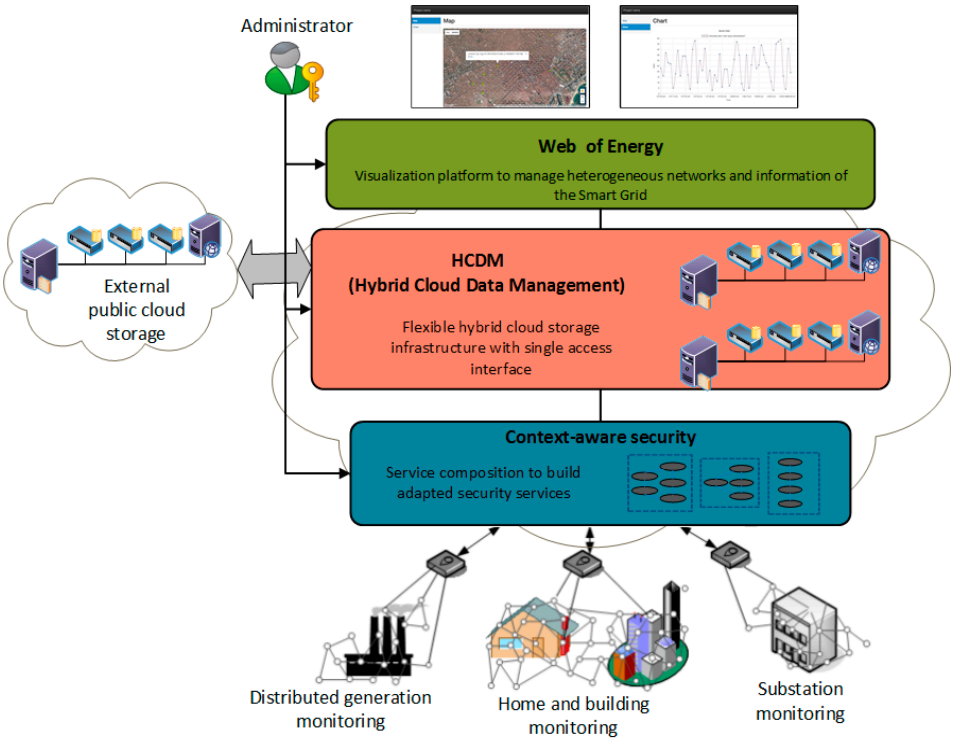

Figure 1. Developed components of the SDU architecture.

- Hybrid cloud data management (HCDM) (Section 3). A flexible and scalable data management system for the smart grid. It is a distributed storage system based on a dynamic configuration of the nodes that collect and store data from the smart grid at distribution level. Additionally, it includes a data orchestrator for hybrid cloud storage in smart grid environments, which is a system that decides in which data storage system the resources and data collected by the smart grid should be placed [13].
- Context-aware security (Section 4). A system able to analyze the different security levels that each smart grid function might need, and apply different policies that translate into different services and different service compositions, providing a framework for flexible and on-demand deployment of security services.
- Web of energy (Section 5). A monitoring and management system that relies on an IoT-based infrastructure and enables machine-to-machine (M2M) interactions between small and resource-constrained devices on the smart grid domain based on HTTP protocol. It extends the IoT concept by providing a bidirectional human-to-machine interface inspired by the web of things (WoT), which results in a ubiquitous energy control and management system (i.e., uniform access to all devices of the smart grid) coined as web of energy (WoE) [17]. The main objective with the design and implementation of this block is to carry out a proof-of-concept of an open API that isolates the electricity grid domain from its utility functions, relying on the aforesaid distributed storage layer to support the massive amount of data generated by the smart grid.

3. The SDU Data Management

A first step towards the validation and evaluation of the SDU concept in the smart grid has been proposed in the scope of the abovementioned European projects. In this regard, a distributed data storage system has been defined to provide high-availability and reduce the latency in acquiring data from the local sites of the utility while offering a secure solution to share data information with external stakeholders (see Figure 1). The following subsections detail the design and implementation of this subsystem based on the proposed SDU paradigm.

3.1. Hybrid Cloud Based Distributed Storage System

The considered scenario stresses the flexible data management concept. Hence, it takes into account a novel ICT infrastructure for smart distribution grids that allows flexibly moving smart grid data and applications from local systems to an external cloud service and protecting them by using security mechanisms that can be added on demand.

There can be several reasons for the mobility of applications and information from the public cloud to local sites and vice versa. They range from application latency improvement, placing smart grid functions closer to data when necessary, to the confidentiality of the data when the data is too sensitive to be stored in the public cloud, or the low capacity of local resources (i.e., using the public cloud when more storage resources and more flexible and dynamic ones are required). However, it will make the DSO infrastructure ready to interact with the cloud in a very gradual incorporation of the novel functionalities even from the fog computing.

The stringent communication requirements lead to define a hybrid solution in which the smart grid manager can configure where is the best place to store the information collected at different points of the network (e.g., substation information, smart metering, etc.). The system offers two possibilities: to store it locally in the own infrastructure of the utility company or by means of external public cloud services.

Furthermore, dividing the smart grid into logical layers presents some critical difficulties arisen from the fact that, typical IEDs are closed devices that do not allow implementing custom developments (e.g., security or information-exchange protocols) as novel experimental devices do. Therefore, a new device coined as FIDEV (Finesce devices) [4,8,9] was proposed. This device behaves as a frontier between these two layers and implements: (1) a communications subsystem that allows heterogeneous network coexistence; (2) a security subsystem that provides a reliable and secure low layer communications infrastructure; and (3) a cloud-based distributed storage subsystem that smartly stores all data generated by IEDs.

FIDEVs are a set of fog computing elements that have been defined as single, yet distributable and interconnected devices, which integrate the needed functions: scalable data storage system, identity management and access control, high-speed and reliable communication interfaces, remote terminal units (RTUs), smart meter data collectors and support for smart grid functions [4]. Those FIDEVs are designed to be placed at different electrical distribution network points (e.g., secondary substation) and interconnected, considering the potential applications to be developed over them, such as remote electrical fault information recovery and remote access control, self-healing network functions, or distribute energy resources (DER) monitoring and control.

For the sake of testing this approach, two trials were deployed in Ireland and Barcelona (Figure 2). They present a flexible data management system that allows maintaining the data generated by ESB (the Electricity Supply Board is a state owned electricity company operating in the Republic of Ireland) locally replicated and in the hybrid cloud as well (through FIWARE Lab when needed). It shows a novel ICT infrastructure for DSOs, providing automatic data collection at substations, critical data exchange and redundancy among substations, and flexible but secure movement of smart grid data and applications from local systems to the cloud. To test these features, different regions (Ireland, Barcelona, and Public Cloud) and several zones inside each of those regions have been defined. The data replication scheme of the data storage distributed system [13] can be configured by the DSO network administrator to automatically distribute the data among regions and zones and assure its high availability and low latency access, in a dynamic cloud or fog computing services deployment basis.

The SDU data management module (Figure 3) works over the FIDEV machines. It includes a RESTful API, which provides users with transparent access to the hybrid cloud infrastructure (distributed private storage or public cloud storage system) for the data management of the SDU. It also combines and integrates functionalities from object storage management, identity management and encryption functionalities of local instances and in a public cloud service. Following service

composition premises, the definition of the SDU data management is modular, which allows to dynamically plug security services or to change the replication policies on demand.

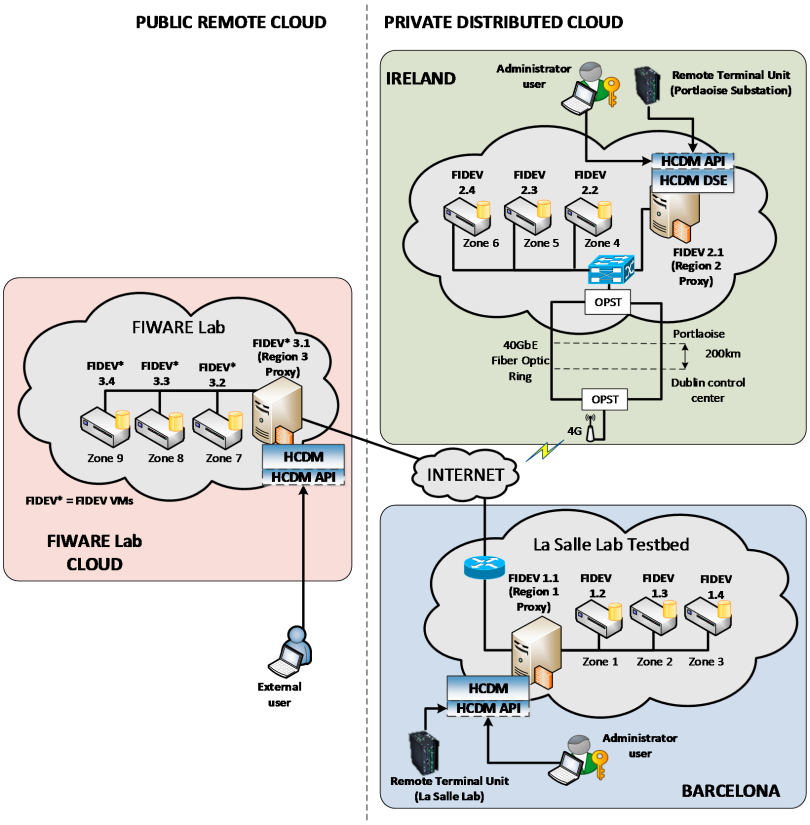

Figure 2. SDU data management trial scenario in FINESCE project where several RTUs were also configured to collect data from electric devices in different regions and directly inject them to the deployed SDU data management system by means of the hybrid cloud data management API.

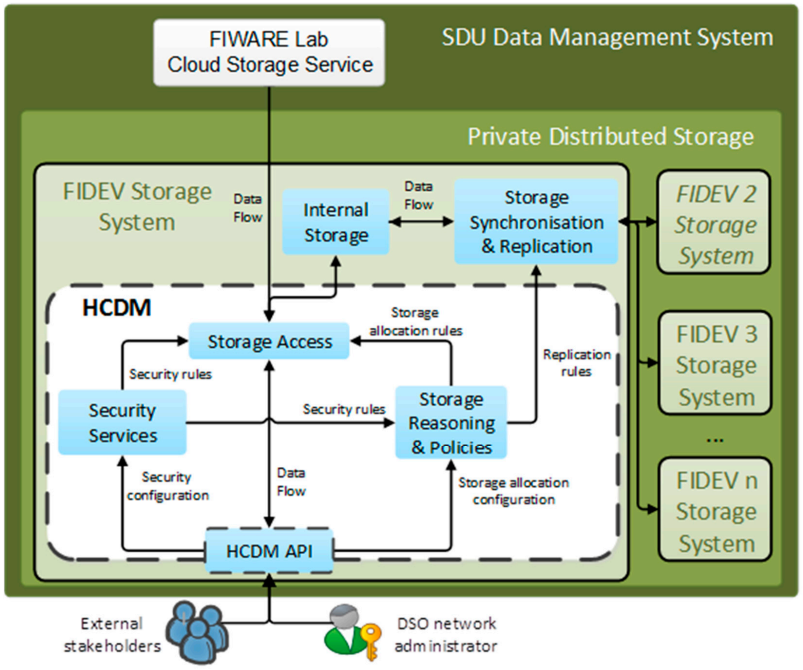

Figure 3. Hybrid cloud data management (HCDM) functional blocks diagram.

3.2. Deployment and Management Tools

In order to assist on the configuration and deployment of the distributed storage system over the smart utility facilities, a web-based graphical interface has been developed as depicted in Figure 4. Through this intuitive interface, it is possible to: (1) configure the distributed storage architecture (i.e., define the number of replication layers [18], regions and servers that will be taken into account for the replication logic); (2) deploy the configured system to the smart grid facilities; and (3) monitor the status of the replication process and servers. The nodes collect data from different energy resources and are in charge of replicating these data among them in order to provide data redundancy and spread the information over the smart grid, so it can become rapidly available at different points of the network. Replication layers [18] define the different levels of replication, being the servers on the top layer the ones that have the freshest data since they are updated more frequently [1,18]. Additionally, in order to determine the scope of the data replication process, different regions can be defined inside any layer. Hence, each server can be associated to any of the defined regions. Therefore, depending on the layer that the region is placed, different data refresh times can be configured. Note that using this epidemic replication approach [18] the system scalability is improved and the data availability can be adjusted according to the application demands.

For example, as shown in Figure 4, two replication layers can be created and one region can be placed on layer 1 and two regions on layer 2. Then, the manager can bind them and define a main server in each region, which will be the one that contains the original data that will be replicated among the servers of its region, and afterwards among the servers from other linked regions if any [18].

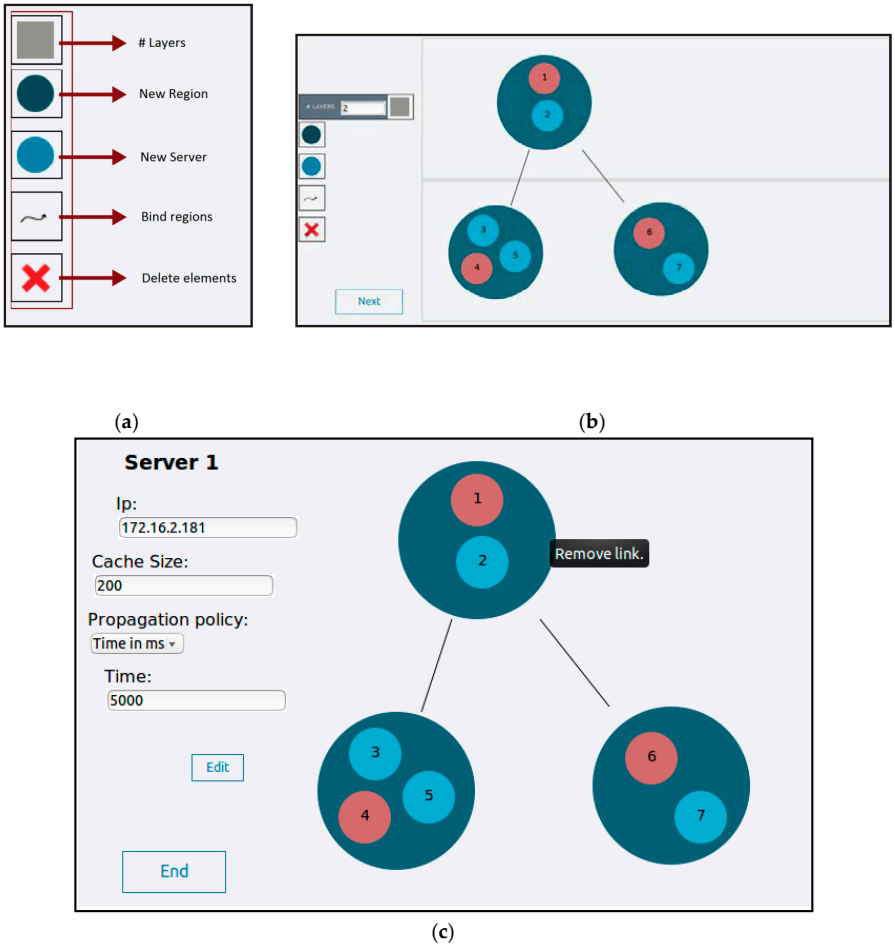

Figure 4. Deployment configuration tool: (**a**) main command tools; (**b**) scenario deployment example with two replication layers; and (**c**) servers configuration process example.

Once the entire distributed system is deployed and operative, other mechanisms and tools are needed to interact with it in order to manage the stored data. In this regard, a RESTful API is used to interact with the HCDM modules and store data in the closest FIDEV. That can be directly configured to work with some sensors or basic software systems to store sequentially any piece of information collected. In addition, a java-based front-end application has been also developed to upload new datasets to the system, access and download them, or easily migrate them to a public cloud when they want to offer them to external stakeholders.

Overall, a low-cost and simple "software" tool was built to manage the smart grid data infrastructure that enables collecting and managing information in a straightforward way. From the experience of the authors, it was identified that this approach is aligned with what DSO network administrators seek. Actually, involved industrial partners to these projects have endorsed the system and tools herein presented, which envisages that they can be useful and convenient for the management of all the data generated by future electrical power networks.

3.3. Hybrid Cloud Allocation Reasoner

The SDU trial specifies the policies to gather data from utilities and replicates these data in several nodes located in two different environments: the public and the private cloud, thus creating a hybrid cloud. As a result, information is stored in several locations, which makes it available from anywhere—considering the cyber-security concerns—and allows users with the corresponding permissions to access the system. Nonetheless, it is worth discussing the efficient usage of this hybrid-cloud-based infrastructure for managing the data generated by the smart distribution grid.

For the sake of this work, it was considered to store the most recent generated data (substation monitoring, smart meter data, electric vehicle charging stations, etc.) in the hybrid cloud and it was found that there is not always enough storage capacity to keep all this historical information. Therefore, a public cloud was used to respond less restrictive queries and handle peak demands using the outsourcing burst model (i.e., when the private cloud cannot provide all the requested services additional resources are offered by the public cloud) [19], which results in an additional on-demand expense [20].

As shown in [20], the crucial factor for economic savings in IT when using a hybrid cloud is the optimal allocation of storage resources. Considering a scenario with different services to be allocated in more than one cloud, the distribution of these services is not trivial. An inappropriate placement of data and services might increase the response time and, thus, limit the quality of service (QoS) offered by the cloud [21]. Therefore choosing a particular location without a defined strategy may entail not to the best choice for a resource distribution, which leads to failing to fulfill the predefined requirements and can represent a much higher cost than the optimum one [22]. Hence, the authors conclude that it is necessary to design a set of rules that mark preferences; priorities; and limits of cost, time, etc., to obtain the best possible location for services or data in a particular scenario [23].

4. SDU Context-Aware Security

Access and protection of generated data is another fundamental piece of the architecture to be built. Opening the huge amount of sensitive data from the smart grid would envisage new business opportunities [11] but also would lead to several new security concerns. This section analyzes the cyber security threads for the digital evolution of smart grid and explains the deployment of another module of the SDU: a flexible and context-aware security access. It explains an intuitive use case of securing smart metering data acquisition by means of dynamic service composition and configuration of different security mechanisms, in order to exemplify the potential of the proposed solution and compare it with current operation.

Although the main parameters to consider regarding cyber security are integrity and confidentiality, reliability and latency should also be taken into account. Table 1 summarizes the requirements of

the functional classes in terms of cyber security. It is important to highlight the low latency and very high reliability needed for some smart functions such as active protection functions (APF) (see Table 1).

Table 1. Functional classes and requirements [2].

Function	Latency	Reliability	Integrity	Confidentiality
Active protection functions	<20 ms	Very High (99.999%)	High	Low
Command and regulations	<2 s	High (99.99%)	High	Low
Monitoring and analysis	<2 s	High (99.99%)	High	Low
Advanced meter and supply	<5 min <10 s	Low (99%)	High	High
Demand response	<5 min <5 s	Medium (99.9%)	High	Low

Note that this reliability degree is difficult to achieve in practice with current technologies in a distribution grid environment. These requirements imply that special care has to be taken to minimize denial of service (DoS) attacks to the minimum [2]. In what follows, a brief review of the state-of-the-art about the high degree of reliability needed in the smart grid and possible mechanisms and protocols to achieve it are presented.

Security in smart grids is essential for the survival and feasibility of the global electricity distribution concept [24] but for its achievement it is necessary to phase out the big challenges posed by the vulnerabilities inherited from internet plus the new ones coming from the different applications, requirements and actors interacting together in a smart grid. Therefore, the smart grid has its own specificities concerning security that need to be considered. In fact, the strongest requirement of a smart grid is the need to continue securely, operating even upon temporary communication disconnections due to communication network partitions.

4.1. The Security Thread

The evolution on the remote control of the electrical distribution grids could give back undesirable vulnerabilities if the architecture is not correctly secured. Smart grid network control and monitoring are very important features for providing distributed energy generation and storage, QoS and security. Smart grids link many distinct types of devices (IEDs) demanding very different QoS levels over different physical media. Obviously, this kind of data network is not exempt from the growing needs of cyber security. In addition, availability and secured communications are also crucial for the proper network operation [25], which drives practitioners to consider active network management (ANM) techniques to coordinate the whole communication network.

In addition to this, the smart grid relies on sensors, actuators and a management network, usually controlled by supervisory control and data acquisition systems (SCADA), which are used to control and supervise industrial processes from a computer. That is to say, SCADA systems control items in the physical world through computer systems. This is one of the points in which the main security concern of smart grids relies. Some recent cases have demonstrated the critical relevance of it.

- One of the most famous cases in this matter is Stuxnet [26], a very complex worm and Trojan discovered in June 2010 that attacked the Iranian nuclear enrichment program. Its code used seven different mechanisms to expand itself, mainly exploiting 0-day vulnerabilities. It achieved the destruction of about a thousand nuclear centrifuges by changing the behavior of the actuators while telling the sensors that everything was good.
- A year later, in September 2011, a new Trojan called DuQu was discovered presenting a very similar behavior to Stuxnet so it is believed that the two worms were related [27].
- In 2013, Iran hacked US Energy Companies (oil, gas and power) and was able to gain access to control-system software and was also accused of launching DDoS (distributed denial of service) to US banks [28].

- On 23 December 2015, hundreds of thousands of homes in the Ivano-Frankivsk region of Ukraine were left without electricity as a result of an attack [29]. Hackers were able to successfully compromise information systems of three energy distribution companies of the country and temporarily disrupt electricity supply to the end consumers.

Cyberspace is defined as "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected ICT-based systems and their associated infrastructures" [30]. Thus, cyber warfare is the kind of war that happens in that space in contrast with the traditional kinetic warfare where physical weapons are used. Smart grids have become a clear potential target of cyber warfare considering that nowadays almost everything runs on electrical power and therefore potentially causing outages or, even worse, causing damage especially in some kinds of power plants (e.g., hydroelectric, nuclear, etc.).

Regarding cyber security standards, many of the existing ones have to be taken into account in the smart grid as is highlighted in NISTIR 7628 [31], where they are listed and commented. A relevant one among them is ISO-IEC62351-6 [24] because it is the cyber security standard of reference for IEC 61850 and, thus, for the smart grid. NISTIR 7628 gives guidelines for cyber security implementation in the smart grid and provides a logical security architecture of general nature. Significantly, it contains interesting considerations regarding the use of authentication certificates and secret keys management.

The state of the art regarding security in the smart grid is in fact defined in the mentioned IEC 62351-6 standard, which basically applies security at transport layer (TLS1.0 [32] with some restrictions) and upper layer communication protocols. It could be argued that protecting the transport layer could be enough since this may provide confidentiality, integrity and device authentication for user data and because many commercial systems rely on protecting systems just like this. However, protecting the smart grid only at the transport layer leaves the network and its links open to cyber security attacks such as DoS, which can produce an eavesdropping of network management messages and ban the users from accessing the service. This fact is not aligned with the high reliability feature that is required in the smart grid [33]. For this reason, the smart grid really urges multilevel security, even above the transport layer [1,2]. Moreover, some smart grid applications (e.g., smart metering data management) can also require additional data anonymization and data encryption services at the edges that could be added when needed, for preserving consumers' privacy. A table summarizing the most important security issues that can affect the proposed data storage infrastructure for the smart grid was previously published in [8]. It was developed by gathering this information from several sources and putting together the experience of academia and industry experts from utilities and telco operators' managers.

To face this challenge and secure the smart grid, the proposed security system is designed in a way that it is really deployable and operative, that balances the many and sometimes conflicting security goals of the different actors and subsystems and accommodates a large and dynamic set of security mechanisms. This is done by creating an entity in which to concentrate the distributed agents that provide service to the smart grid among which the security server and repository (Figure 1).

As it can be seen, all the concerns revolve around the efficient adaptation of the security mechanisms to the specific requirements of the smart grid function to be deployed. Therefore, a context-aware smart grid management broker has to be placed in different locations of the SDU and work coordinately in order to provide the adapted security mechanisms when and where needed. As an example of this dynamic security configuration, a use case focused on flexible smart metering security is shown in the following section.

4.2. Securing Smart Metering Through Service Composition

This section summarizes the extension of service composition techniques in order to manage flexible smart grid applications. More concretely, it develops the methodology around a proof-of-concept use case that focuses on the securitization of the advanced metering infrastructure of the smart

grid. The obtained results can be extended to the whole smart grid and are showcased in real and modern applications.

As stated before, the smart metering represents only a set of the smart grid solutions, but it is the part that has already been more regulated, deployed and tested around the world. Advanced metering infrastructure (AMI) consists of smart meters, data management, communication network and applications. AMI is one of the three main anchors of smart grids along with distributed energy resources (DER) and advanced distributed automation (ADA). Smart metering is usually implemented using automatic meter reading (AMR), a technology that automatically gathers data from energy, gas and water metering devices and transfers it to the central office in order to analyze it for billing or demand side management purposes. Data is read remotely, without the need to physically access the meter. AMR systems are made up of three basic components to be secured end to end: the meter, the central office and the communication systems. AMR includes mobile technologies, based on radio frequency, transmission over the electric cables (power line), or telephonic platforms (wired or wireless) [3,15].

The deployed prototype is focused on collecting smart meter and RTU data, encrypting them and saving them in some place (the cloud, a concentrator, the IEDs, etc.) in a way that the authorized actors can work with the data without having access to user specific data, preserving their customers' anonymity and protecting them from malicious attacks.

First of all, in order to determine the security requirements of the smart metering function, it has been of great importance to follow the guidelines for smart grid cyber security [31] developed by the National Institute of Standards and Technology (NIST), because of its high detailed description of requirements and elements that must be taken into account when deploying a smart grid. Since this research targets to secure smart metering as a first approach, a limited set of requirements have been selected from among over 200 entries in [31], considering those that affect directly or indirectly to the smart metering use case. Once the requirements have been set up, a chart (Table 2) has been developed with the cybersecurity requirements [34] on one axis and the technologies that can be used to meet the requirements on the other axis. The different technologies are graded (from 5 when it totally applies, to 0 when it does not apply), depending on the level of support to the requirement. They were also selected based on the authors experience from [8,9], besides an exhaustive review of the literature about smart grid security and specify which secured-ICT technology can meet more accurately the requirements.

In addition, the conclusions extracted from the experience acquired in those projects that have guided this work have helped us to define the following rules in the design of cyber security solutions for smart grid:

- To rely as much as possible on proven existing standards, only complementing them when strictly necessary. This comes from the evidence that the first versions of most standards contained serious vulnerabilities.
- To choose the most adequate option from these standards for the specific smart grid case (see Table 2).
- To place cyber security services as close as needed to the sensing and actuation points to improve latency and reliability of applications. In fact, these capabilities aligned to fog computing trend can be based on service composition paradigm by placing them in the cyber security server and repository contained in the IEDs.
- To use a common coordinated cyber security data repository for all the involved technologies.
- To distribute this repository, either as a whole or partially, in the cloud, although having also a central repository located elsewhere. The central cyber security repository is replicated so that, in case of disconnection, the system continues to work for some time even allowing the inclusion of new devices and functions.
- To define cyber security metrics to feed the context-aware system to enable improved system management.

- To use, whenever feasible, authentication based on certificates.

Table 2. Smart grid cybersecurity service requirements and technologies analysis.

Service Requirements	PKI	Encryption + Decryption (AES)	NAC	Checksum SHA	DoS Defense System	ACL (Different Layers)	IDS	IPS	NMS	Supervised Cognitive System	Unsupervised Cognitive System	Logging	Segmentation (VLAN) VRF, MPLS)	SSH	QoS	Format Check	Homomorphism
SG.SC-3 Security function isolation	4	3	4	0	0	2	1	1	0	0	0	0	5	0	0	0	0
SG.SC-4 Information remnants	5	0	5	0	0	0	4	4	3	0	0	2	1	0	0	0	0
SG.SC-5 DoS protection	0	0	0	0	5	3	4	4	0	0	2	2	0	0	0	0	0
SG.SC-6 Resource priority	0	0	2	0	0	0	0	0	0	0	3	0	1	0	5	0	0
SG.SC-7 Boundary protection	5	1	4	0	0	4	3	3	1	0	0	1	5	0	0	0	0
SG.SC-8 Communication integrity	5	3	0	5	0	0	0	0	0	0	1	0	0	0	0	5	4
SG.SC-9 Communication confidentiality	5	5	2	0	0	2	2	2	0	0	0	0	0	1	0	0	5
SG.SC-10 Trusted path	5	0	0	0	0	1	1	1	4	1	3	0	0	0	0	0	1
SG.SC-11 Crypto key establishment	5	5	4	0	0	0	1	1	1	0	0	1	0	0	0	0	5
SG.SC-12 Use of validated cryptography	5	5	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
SG.SC-15 PKI certificates	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SG.SC-19 Security roles	5	0	4	0	0	3	1	1	1	0	0	1	2	0	0	0	0
SG.SC-20 Message authenticity	5	4	1	4	0	0	0	0	0	0	0	0	0	1	0	5	3
SG.SC-26 Confidentiality at rest	0	5	0	3	0	0	0	0	0	0	0	0	0	0	0	0	4
SG.SC-29 Application partitioning	5	0	5	0	0	2	1	1	0	0	0	0	3	0	0	0	0
SG.SI-2 Flaw remediation	0	0	0	0	0	0	0	0	4	5	5	2	0	0	0	0	0
SG.SI-3 Malicious code/spam protection	0	2	0	0	0	5	5	5	5	0	0	0	0	0	0	0	5
SG.SI-4 Information system monitoring	0	0	0	0	0	0	4	4	5	2	3	4	0	0	0	0	0
SG.SI-7 Software and info integrity	5	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	5
SG.SI-8 Information input validation	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0
SG.AC-3 Account management	5	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SG.AC-8 Unsuccessful login attempts	5	0	5	0	0	0	3	3	4	2	4	4	0	0	0	0	0
SG.AC-11 Concurrent session control	0	0	5	0	0	0	1	1	5	2	4	3	0	0	0	0	0
SG.AC-13 Remote session termination	5	0	5	0	0	0	0	0	3	2	2	0	0	0	0	0	0
SG.AC-16 Wireless access restrictions	5	4	5	0	0	0	0	0	0	0	0	0	0	0	0	0	1
SG.AC-17 Access control mobile devices	5	0	5	0	0	0	1	1	1	0	0	2	0	0	0	0	0
SG.AU-X Auditability	2	0	0	0	0	0	0	5	0	0	5	5	0	3	2	0	0
SG.AU-16 Non repudiation	5	0	0	0	0	0	0	0	4	0	5	0	0	0	0	0	0
SG.CM-x Configuration changes	5	0	5	4	0	1	1	1	3	3	0	5	0	4	2	5	4
SG.IA-5 Device identification and auth.	5	0	5	0	0	0	3	3	2	0	0	2	0	0	0	0	0
SG.MA-x Remote maintenance	5	4	5	1	0	2	2	0	3	3	2	4	1	5	2	1	1

Notes: 0 means does not apply; 1 means somewhat applies; 2 means applies; 3 means mostly applies; 4 means applies a lot; 5 means totally applies.

Many examples of smart metering use cases that should fulfill the security requirements of Table 2 can be defined, such as the installation process of a smart meter, reading the power consumption, firmware updating, system monitoring, maintenance processes, fraud avoiding, etc. Aiming at just giving a proof-of-concept demonstration of some of these benefits that service composition and SDN could bring into smart grid, a basic use case was designed on securing the smart metering in a software defined utility environment [8].

Combining SDN and service composition becomes especially powerful for the secure self-maintenance of networks, which represents a very important characteristic for the development of smart grids. They could be applied at different segments of the electrical distribution grid implementing easy and fast-to-deploy intelligent solutions.

The focus on the service composition interoperable standalone modules, which can be invoked or dropped on demand, leads to considerable cheap solutions in the field of smart grids and presents a solution that could be integrated incrementally. Moreover, it allows system architects to create flexible solutions that could be modified and evolved according to eventual new needs. Furthermore, the modularization of smart grid functionalities and encapsulation into self-contained services facilitate the distribution of the smart grid intelligence, approaching the reasoning and decision process and helping to handle its critical constraints of latency on fault reaction.

In this regard, the authors have extended the work conducted in [6] and present a new taxonomy of services (Figure 5) for AMI security in this paper. This taxonomy classifies services into six different generic parameters: "Granularity", "Execution", "Scope" (application/network), "Purpose", "Usage" (mandatory/optional) and "Order" (dependent/independent), following the criteria selected in [6] and defining new sub-criteria based on the general and security requirements of a smart metering management [2,9,31,35]. All these criteria can be applied generically to any smart grid service, although the options shown in Figure 5 for "Purpose" criteria are limited to smart metering. Afterwards, the selected modules for smart metering are classified according to this taxonomy (Table 3).

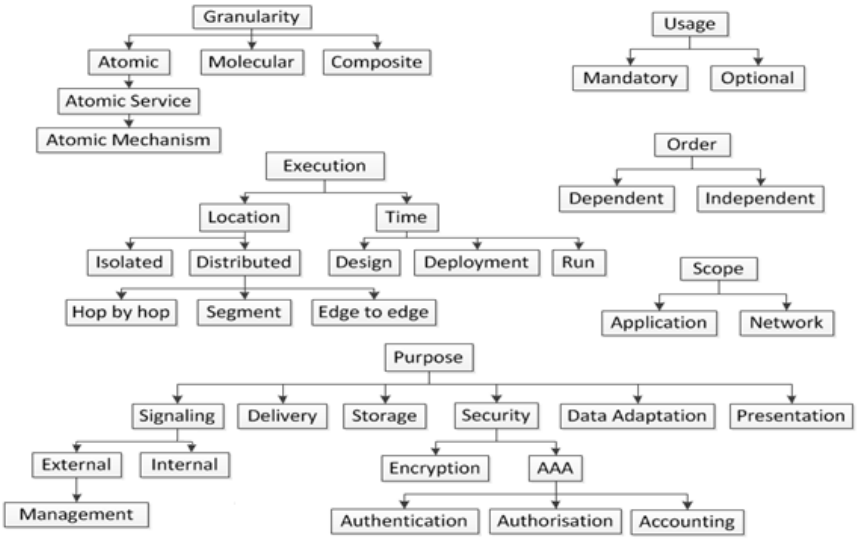

Figure 5. Extended taxonomy for secure smart metering.

Table 3. Secure smart metering composition modules classification.

Parameter	Consumption Increasing	Consumption Decreasing	Consumption Checking	Consumption Initializing	USB Authentication	User & Password Validation	User & Password Login	USB ID Login	Digital Certificate Login	Cypher key Obtaining	Digital Certificate	Data Encryption	Data Decryption
Granularity	Atomic												
Scope	Application												
Execution location	Isolated/Segment/E2E					Segment/E2E						Isolated	
Execution time	Run		Deployment			Run							
Purpose	Signaling external management			Signaling internal management		AAA			Delivery			Encryption/Decryption	

The one by one definition and classification of the modules can guide the service composition design process done of composite services and the placement of the different modules in specific physical or logical locations of the smart grid. For example, considering the description of some security modules such as AAA (authentication, authorization and accounting) module, its execution location could be in a specific segment or end-to-end, while encryption or decryption modules are isolated modules that could be placed in a specific location of the network. This fact can help the reasoning of the administrator or the specification of automation processes for building and deploying composite services automatically in a multilayered scheme. However, some characteristics are intrinsically related to the functionality offered by the composite service to the end-user, such as the atomic service usage (optional or mandatory) or the order of them inside the workflow (dependent or independent) and, thus, they can only be completely defined when building the composition.

4.3. Atomic Services Definition

The first and foremost important task that should be accomplished in the definition of the use cases is to define which functionalities are required to achieve the goal of the use case and which service modules are necessary to cover each of these functionalities. After an in-depth analysis of the security requirements and the technologies available on the smart grid, it is time to discuss which functionalities are required and which modules could be useful to accomplish the objective of the final workflow. A correct process modularization must present services as loose-coupled as possible in order to help to reuse the services in different use cases avoiding their reimplementation and facilitate the adaptability of the workflow to context changes (i.e., changes on the security level may allow some services to be added or removed at will to improve the process performance). In the following, some examples of these most important atomic service modules defined for these use cases are presented.

- USB keychain authentication: This service encapsulates the functionality of using an USB token dongle for authentication purposes. It contains a unique ID, which converts it to more than a common password since the USB device cannot be easily replicated.
- USB ID validation: In order to carry out the USB dongle verification and to assess whether it is valid or not, a module has been defined. It checks a list (AES (advanced encryption standard) encrypted) of revoked IDs to accept or deny the device.
- AES decryption: This atomic service performs the AES decryption (advanced encryption standard) needed for the ID validation module. Another different service will be in charge of generating and providing the required key.
- Key-distribution: This service provides the key needed to encrypt/decrypt using a symmetrical algorithm. Usually it uses either a pre-shared key or a public key infrastructure system. Although both modules can be used, for this example the pre-shared key system is selected.
- Certificate download with user + password: It allows downloading the asymmetrical certificates that will be used for the final enrollment of the smart meter to the smart grid system. This can be done in several ways but, in this case, a module that allows doing so by entering the username and password of the technician has been selected. If both are correct and the USB ID has been validated, the certificate will be downloaded.
- Login with certificate: This service is required to use the certificate previously downloaded and checking a certificate revocation list. Finally, the smart meter will be enrolled to the smart grid if everything is correct.

4.4. Workflow Example

Finally, the modules have to be joined to create the whole workflow. As it has been described before, this process allows the smart meter function to be enrolled into the smart grid system. In order to do so, the whole process is being carried out in some steps (Figure 6). A request to the USB device is made, then both the signal saying that the USB is still connected and the ID of the USB itself is sent to

the next module that checks whether the ID is valid or not, using the information in plain text received from the AES decryption module. At the same time, this module receives the decryption key from another module. Then, if this step is completed successfully, the technician must insert his username and password. Then, the certificate is downloaded and once checked with the certificate revocation List, the smart meter can successfully login to the smart grid network.

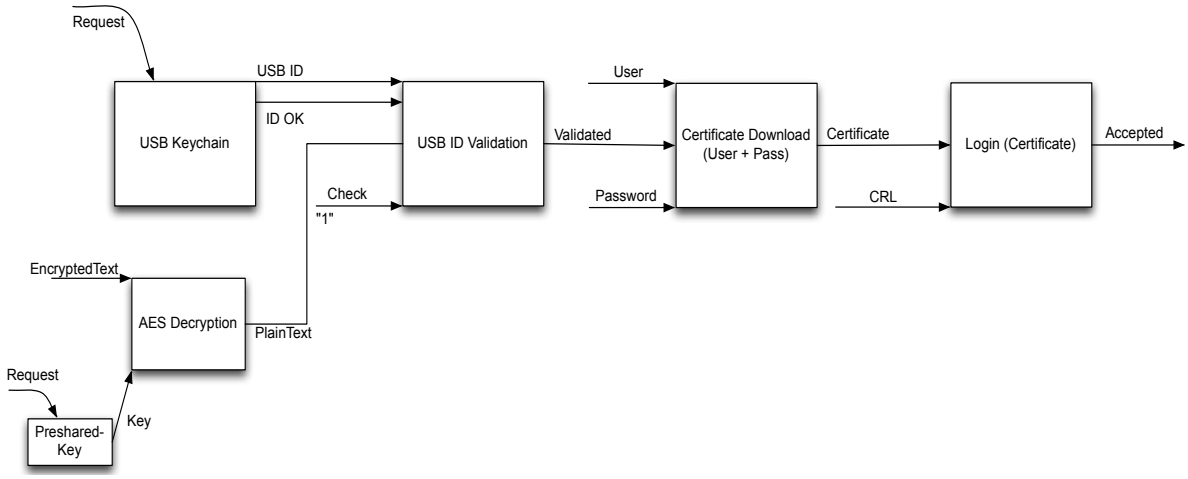

Figure 6. Complete workflow approach for "sign up with a non-validated USB" service.

However, the importance of this process is not the process itself but its modularized design based on service composition, development and deployment. That is to say, the main importance is the great flexibility provided by this way of working. It is very different to current-day straightforward deployments by procuring to the system architect a reusable design, a function virtualization and a chance to cloud computing deployment. If this process does not suit the utility's needs it can be easily changed, modules can be quickly swapped for others or even removed to simplify the process. The greatness comes when this technique is combined with some kind of intelligent middleware that set the policies and build the workflows autonomously (orchestrator) [36]. The orchestrator could even learn and make decisions based on the status of the network [1]. Another interesting characteristic is that it does not depend on how the modules are implemented. As long as the input and output interfaces are well-defined, the module interoperability is fixed. Thus, it should also help to avoid any vendor lock-in and to foster the interoperability and reusability of the systems.

4.5. Interfaces Definition

Usually, service modules like the ones presented in this work are expressed by means of well-defined interfaces that hide their implementation (in order to maintain them loose-coupled in the service composition process) that could be coded in different logic or development languages. In this case, the option of using web services description language (WSDL) [37] was selected to exemplify and deploy this use case. WSDL is the most extended language used by web-services description, and offered a good solution for an easy and fast definition of the services' interfaces, besides bringing a standardized and well-known language easy to integrate with other service frameworks like OSGi [38]. Definition of services used in [6,7] was adapted for network services. However, it was defined generic to be adapted to application cases as well, as this one. Therefore, specific or more complex definitions can be used in the future, to completely define and deploy the services on demand, placing and invoking or dropping them on one device or another. The following list enumerates the basic interfaces that each one of the services defined in Section 4.3 can include:

- Types: In this field, the variables are defined using a simple name and type nomenclature.
- Interface name: Contains the name of the interface.

- Fault_name: Name of the attribute generated when an error appears.
- Operation_name: Indicates the name of the operation. It must be unique per interface. It also contains the pattern that usually is "in-out" or "in-only" and defines how the data is exchanged and style (non-mandatory).
- In_msgLabel: Defines the name and format of inputs.
- Out_msgLabel: Defines the name and format of outputs.
- Out_fault: Associates the output error with the operation.

At the end, the number and quality of the resulting workflows are limited by the compatibility and exchangeability of the individual service modules. Therefore, the adequate planning of the interfaces is highly relevant since it will define how the modules can communicate between each other.

5. A Web of Energy

The last but not least fundamental piece of the SDU comes from the necessity of a graphical remote management of the communication network, data and devices from a single interface, as previously depicted in Figure 1. The authors have specified and developed an IoT-based infrastructure coined as web of energy (WoE) [17] in order to define a single management tool for monitoring and controlling several distinct smart devices or IEDs from different vendors often using proprietary protocols and running at different layers. This infrastructure must allow to interact with those IEDs with the aim to effectively deliver energy and to provide a set of enhanced services and features (also referred to as smart functions) to both consumers and producers (prosumers) such as network self-healing, real-time consumption monitoring and asset management [3].

Day by day, the number of connected things is growing exponentially. The latest data shared by Cisco estimates that IoT connections will grow from 780 million in 2016 to 3.3 billion by 2021 [39]. The way to access these devices from a single platform is undoubtedly one of the biggest headaches for researchers. In this regard, standardized solutions provided by the rapid evolution of the Internet have laid the foundation of the web of things (WoT) [40]. Although the latest developments on the IoT field have definitely contributed to the physical connection of such an overwhelming amount of smart devices [40], several issues have arisen when attempting to provide a common management and monitoring interface for the whole smart grid [41,42].

Indeed, WoE, which takes the pioneering new form of the WoT, is targeted at providing a context-aware and uniform web-based novel environment to effectively manage, monitor, and configure the whole smart grid. WoE also integrates the heterogeneous data generated by every device on the smart grid (i.e., wired and wireless sensors, smart meters, distributed generators, dispersed loads, synchrophasors, wind turbines, solar panels and communication network devices) into a single interface.

The open IoT-based infrastructure previously presented by the authors in [17], provided the definition of new tools to manage energy infrastructures at different levels, from IoT-based infrastructure enabled M2M interactions between small and resource-constrained devices on the smart grid domain. Thus, the IoT concept has been extended by providing a bidirectional human-to-machine interface—inspired by the WoT—that results in a ubiquitous energy control and management system. WoE combined the web-based visualization and tracking tools with the Internet protocols, which enables a uniform access to all devices of the smart grid. Extended details of WoE design and development can be found in [17].

6. Impact on the Smart Grid Operation

One of the main benefits that SDU approach provides is the fast response to changeable conditions and its flexibility towards data management variations. In a smart grid environment that is increasingly integrating electric power and ICT systems, SDN provides novel mechanisms that change the way data networks are managed. The impact on the operation of the networks and the own data from

advanced metering infrastructure (AMI), distributed energy resources (DER), network management system (NMS), etc. During trial validation in FINESCE, numerous examples of potential applications of SDU architecture have been identified:

- Remote electrical fault information (oscillography) recovery;
- Remote access from substation to central servers;
- NMS and management of communications network;
- AMI/AMM (advanced metering management) data access and management;
- DER monitoring and control;
- Secondary substations distributed SCADA;
- Decentralized FLISR (fault location, isolation and supply restoration) solution;
- Self-healing network functions: current, voltage and environmental asset conditions monitoring and alarm setting;
- Electrical vehicle supply equipment (EVSE) control;
- VoIP substation intercommunication;
- Substation surveillance (video storage and communication for physical security and surveillance equipment control); and
- Physical access security (i.e., including centralized identity management and ID card reader control).

Locating FIDEVs in the household or managing the information provided by a set of households, could also provide smart metering related applications, collecting the data and generating almost real-time patterns of the neighborhood and providing abstracted data to control centres. Other examples proposed to integrate FIDEV functionality with EVSE control, providing advanced control applications, such as switching off/on the EV charging depending on the levels of current and voltage monitored in the household, or the energy available.

SDU could represent an opportunity for utilities to have more flexible devices (based on software, upgradable, configurable, able to deploy new applications above them), enabling a lower-cost distribution grid management, and reducing a 75% the reconfiguration times as detailed in Section 7. In addition, SDU systems can provide the means to share data from devices such as electric vehicle charging points, smart metering or substation monitoring, with third party users. It can foster new business models, such as selling region specific smart metering data to an Energy Service Company (ESCO) or retailer, providing them high-value energy information, or electric vehicle mobility information.

For the specific case of DER monitoring and control, SDU can minimize the impact of DER new connections in the electric power network. Moreover, there exist several limitations of legacy electric grid that can be mitigated, such as the dependability of the size of the grid in the hardware and software requirements, or the performance variation (it may differ in networks of 10 or 100 nodes). SDU can simplify the DER operation, permitting the DSOs (or even third parties such as aggregators) to monitor DER and apply dynamic policies of energy curtailment.

Virtual IEDs over FIDEV machines, may work together or as alternatives to commercial IEDs to provide SDU data management system with network information and to apply control actions on simulation environments in real-time.

7. Experimental Evaluation

In order to test the SDU potential features, the trial shown in Figure 2 was deployed connecting a set of FIDEVs placed at different locations inside the DSO infrastructure (secondary substations in Ireland) and outside their facilities (La Salle communications laboratory in Barcelona and some virtualized FIDEVs in the FIWARE Lab Cloud). This trial allowed us to have first results about data management, smart grid operation timing, and feasibility using SDU system. In this section,

two of these experimentation tests are presented, one focused on data management of the system and another one on the flexibility provided by the SDU approach for AMI security management or other of the potential smart grid functions mentioned in Section 6.

7.1. On-Demand Logical Topology Reconfiguration of the Hybrid Cloud Data Management System

As the amount of data increases in a distributed storage architecture, moving data to computation units becomes unfeasible due to the overhead associated to the communications network and its limited available bandwidth compared to the volume of data [43,44]. Therefore, latest trends on the management of big data volumes aim to "move" the computation facilities to data (also referred to as computational portability [45]) rather than flooding the whole communications system every time a data computation task needs to be conducted. Smart grids are a good example of this situation where a heterogeneous communications network [3] is used to link several sources that are continuously generating data which need to be efficiently stored.

In this regard, the SDU proposed in this paper implements a hierarchical distributed storage architecture able to reconfigure its topology—with little overhead—according to the needed computation and storage load patterns [18]. The purpose of this experiment is to assess the capabilities of the SDU on adapting to new storage and computation scenarios. Specifically, for the sake of this experiment an eventually consistent full-replication scheme was assumed [46] (i.e., all the nodes have the same data objects, which boosts data availability and system fault tolerance [18]) and defined two extreme scenarios on top of the physical topology detailed in Figure 2: (1) an update-intensive situation (modeling an automatic meter reading smart function operation that encompasses a high number of devices generating new data) with 80% of write operations and 20% of read operations; and (2) a read-intensive situation (modeling a decentralized FLISR function) with 80% of read operations and 20% of write operations. It is worth noting that read operations require no synchronization with other replicas, while write operations need to be applied everywhere.

Figure 7 describes the evolution of the experiment. Initially, at Stage I the system is configured in a neutral setup: nodes from the substation in Ireland act as the core replication layer (i.e., all updates are directed to them), nodes from Barcelona Laboratory act as the second level of the replication hierarchy and nodes from FIWARE Lab cloud act as the third level of the replication hierarchy. In this situation, the replication process is as follows. First, all data generated anywhere are initially sent to a node of the Ireland cloud. This node will eagerly replicate these data to all the nodes of its cloud. Subsequently, the primary master of this core layer will lazily replicate new data to the pseudo-primary node [18] of the second level of the replication hierarchy. At this point, the pseudo-primary will replicate these data to all the nodes of this second level. Next, the pseudo-primary of the Barcelona cloud will lazily replicate these data to the pseudo-primary of the FIWARE Lab cloud. Finally, the pseudo-primary of the FIWARE Lab cloud will replicate new data to its surrounding nodes and the full-replication status will be achieved. This situation can be best seen as a particular case of primary copy replication [18] where the maximum update load that the storage system can handle is limited to the size of the Ireland substation (i.e., primary). In addition, it is worth noting that data generated from other locations (i.e., Barcelona or FIWARE Lab) will suffer from a significant communication delay due to the cost of moving data to the core layer (i.e., Ireland). This situation is convenient for moderate storage loads with no delay constraints.

At Stage II, all the nodes of the scenario collecting AMI data are forced to generate a massive update load. That is, each one generating 80% of update operations. Therefore, a trigger is generated on the web interface detailed in Section 5 and a logical topology reconfiguration command is issued to all the nodes. To handle this new load, all the nodes of the system are promoted to the core layer, and, thus, all of them accept update operations (i.e., updates from Barcelona and FIWARE Lab no longer needed to be eagerly forwarded to Ireland). To reach the full replication status, data are lazily replicated to all nodes as in update everywhere replication scheme [18]. As shown in Figure 7, the number of

served operations per second decreases while the system is undertaking the reconfiguration process but rapidly increases once the system is set up to address this new type of load.

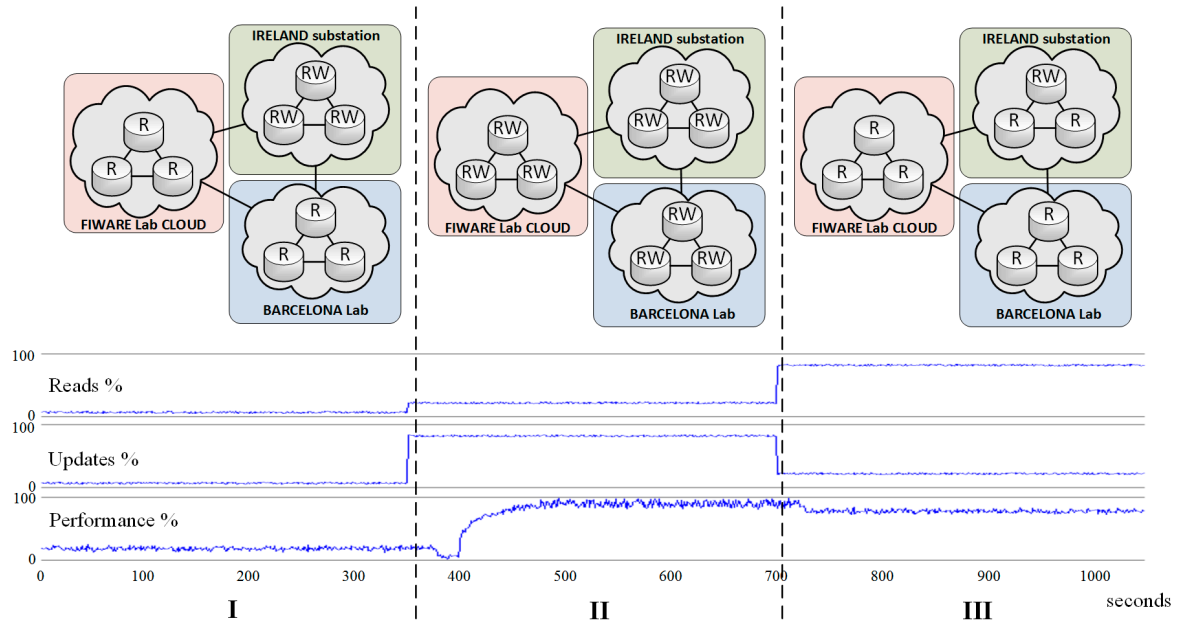

Figure 7. Dynamic system reconfiguration process. The logical topology of the hybrid cloud data management system adapts to changes in input data access patterns (i.e., overall data reads and data updates ratios).

Finally, at Stage III all the nodes of the scenario are forced to generate a massive read load. That is, each one generating 80% of read operations. As read operations do not need any synchronization with other nodes, the network traffic decreases. Once again, another trigger is generated on the web interface and another reconfiguration command is issued to all the nodes. In this situation, a pure primary backup scheme is selected (i.e., a single node handles all update operations while read operations are equally handled by all the nodes). Thus, in this situation the core layer is composed of a single node of the Ireland cloud and the second replication layer is composed by the rest of the nodes. As shown in Figure 7 there is no significant performance degradation during the reconfiguration process due to the fact that the new load (i.e., read intensive) generates far less overhead than the previous load (i.e., update intensive).

Overall, this experiment has described the behavior of the proposed SDU unit when switching from two extreme scenarios regarding the HCDM system. Specifically, the ability of the system on adapting to new data loads that require a concrete topology and how this reconfiguration process temporally affects the system performance have been seen.

7.2. SDU Reconfiguration for AMI Operation

In the trial proposed in Figure 2, the migration from one configuration to another in different smart grid applications, such as AMI, was evaluated. Although the test is provided in a limited environment connecting only nine FIDEVs over two different substations, La Salle laboratory testbed in Barcelona and the FIWARE Lab cloud, it gives some results about plausible reconfiguration latency (as shown in Tables 4 and 5 and Figure 7).

Table 4. Scenario definitions.

Security Level Workflow	Dongle	By Design	AAA	Best Effort
Scenario 1	No	No	No	Yes
Scenario 2	No	No	Yes	Yes
Scenario 3	No	Yes	Yes	Yes
Scenario 4	Yes	Yes	Yes	Yes

Table 5. AMI security system reconfiguration times.

Initial Scenario	Final Scenario	Network Reconfig.	HCDM Reconfig.	Overall
Scenario 1	Scenario 2	Milliseconds	Milliseconds	1 s
Scenario 1	Scenario 3	1–2 s	3 s	4–5 s
Scenario 1	Scenario 4	1–2 s	4 s	5–6 s

Over this trial, some qualitative experiments have been made migrating the SDU configuration for providing different security level mechanisms in the automatic meter reading. Four different scenarios have been defined (Table 4) using the building blocks defined in Section 4.3, from non-security mechanisms (Scenario 1) to the one specified in Figure 6 (Scenario 4).

The testbed experimentations demonstrate the feasibility of the solution and a ratio of time reduction of one forth in smart grid function reconfiguration at distribution level. However, when scaling up the scenarios provided in Table 5, some other parameters should be considered, such as the provisioned network bandwidth between FIDEVs, memory dirtying rate of the FIDEVs and round trip time (RTT) between the SDU manager entry point and the FIDEVs. Times presented in Table 5 are extracted taking into account that FIDEVs have previously installed all selected services. For other use cases, in which the smart grid configuration changes can require the installation and invocation of a novel service not previously installed in the FIDEVs the order of magnitude of the reconfiguration time may vary, including the transmission time and deployment time of the new applications or FIDEV images.

Furthermore, a benchmark analysis has been made considering different protocols used in the smart grid environment and evaluating their potential integration in the SDU solution for AMM applications (Table 6). The characteristics examined are: (1) the protocol architecture, whether they have already defined their compatibility with TCP/IP protocol stack or its communication needs to be built directly over network access layer; (2) the level of security provided by the own protocol; (3) if it was originally designed for AMI communications; and (4) the potential integration in the proposed SDU system for the complete digitalization of the AMM operation. DLMS/COSEM and IEC 61850 were the protocols identified as more feasible to be integrated because of the compatibility with TCP/IP protocol stack provided by FIDEVs, their higher security features and their AMI-compliant original design, although other options that can work over TCP/IP are also considered as potential solutions to be completely integrated in the SDU system, when needed.

Table 6. AMM protocols evaluation in the SDU context.

AMM	Protocol Architecture	Security Intrinsic Level	AMI-Compliant	Bumpless SDU Integration
DLMS/COSEM	TCP/IP	Medium	Yes	Totally
IEC 61334	Access layer	Low	No	Partially
IEC 61850	TCP/IP	Medium/High	Yes	Totally
PLC-based	TCP/IP	Medium	Yes	Totally
PLC-based	Access layer	Low	No	Partially
CEA 701.1B	TCP/IP	Low	No	Totally
IEC 60870-102	Access layer	Low	No	No
IEC 60870-104	TCP/IP	Low	No	Totally

7.3. Smart Grid Functions Qualitative Benchmarking

On the other hand, based on the smart grid functions identified during FINESCE project, a qualitative benchmarking has been built considering the grade of feasibility of them over the SDU system in a short term (Table 7).

For their evaluation, several factors have been taking into account, such as the current grade of integration of the ICT and electric power networks, the dependability on data management, the required operation latency, regulatory handicaps and the scores provided by different DSO managers and technicians. Although at this stage is difficult to evaluate objectively the potential migration of Table 7 functions into a SDU model, this qualitative analysis helps to identify functions that are hard to be migrated to a SDU environment in a short period of time, due to the lack of integration with ICT network or the DSOs reluctance to change the current operation (e.g., self-healing network functions).

Table 7. Smart grid functions qualitative benchmarking.

New Smart Grids Function	Feasibility
Remote electrical fault information recovery	High
Remote access from substation to central servers	High
NMS and communications network management	High
AMI/AMM	High
VoIP substation intercommunication	High
DER monitoring and control	Medium
EVSE control	Medium
Secondary substations distributed SCADA	Medium
Substation surveillance and phisical access security	Medium
Decentralized FLISR solution	Medium
Self-healing network functions	Low

8. Conclusions and Results

This article concentrates the solutions developed in the context of FINESCE and INTEGRIS European research projects that focus on the protection of data while being transmitted, stored and used in the context of the distribution smart grid. These advances have been made with the objective of proposing a software defined utility (SDU) that meets the data cyber security requirements of smart grid. In those projects, several issues were tackled such as access control, key management and context-aware security design in the case of the electrical distribution smart grid in the cloud. More concretely, three different research lines have been studied and subsequent research outputs have been given towards the development of the SDU concept, which advocates for the migration of the utility infrastructure to software systems instead of relying on complex and rigid hardware based devices.

The design and implementation of the distributed storage system covers the three main priorities demanded by utilities:

- To provide a scalable distributed storage solution that handles the large amount of data that could be generated in the distribution grid, and, indeed, be the basis of a SDU.
- To provide a management tool that can be easily adopted by DSO administrators. Graphical interfaces must offer simplicity and usability.
- To assure that the solution provides the level of security required for managing the communications and data of the critical infrastructure for what it is designed.

First, an in-depth analysis of a flexible storage systems for the smart grid based on a combination of cloud storage systems with distributed storage located in the utility facilities (e.g., at secondary substations) has been conducted. The SDU data management trial has been presented and details about

the different deployment and management tools that were developed to enable the fast deployment of distributed storage services for a SDU data storage infrastructure have been outlined.

Second, context-aware security for the SDU is presented and the relevance of the security aspects in a critical infrastructure such as the smart grid has been reviewed. It has been found that the diversity of contexts and security requirements within the smart grid makes it difficult to decide which is the appropriate level of security needed in each case. It usually means an overloading of the cyber security mechanisms or leaving unprotected elements of the electric power network. Therefore, a way to offer adapted security solutions on demand based on the service composition methodology and mechanisms has been proposed and discussed. In this regard, a large set of smart grid services has been analyzed together with the collaboration of telco operators and DSOs. From this analysis, the required level of security for those services has been evaluated and matched them with different protection mechanisms. To further exemplify the way to undertake this methodology in a specific smart grid use case, this paper also presents a smart metering context-aware security selection, providing a set of basic services and how they can be combined to offer different levels of cyber security.

Third, the WoE development has been exposed from the previous work of the authors. Definitely, the WoE is another complementary piece of the SDU already developed. To extend the conducted work, this paper provides details on a proof-of-concept deployment of the WoE.

The three developments presented in this paper represent a first approach towards a flexible, context-aware and low-cost design for the future smart grids based on SDUs. This proposal aims at meeting the stringent cyber security requirements of the smart grid and is open to forthcoming mechanisms, protocols and architectures.

Those three developments and the integral SDU solution presented have been analyzed from the perspective of potential impact in the TSO/DSO infrastructures management. Taking into account the knowledge and experience, not only of the authors but other experts from utilities and telco operators, many smart grid applications (such as AMM, DER, FLISR control and management) have been identified as specific targets to which the SDU. It can be considered as a tool that can change the way that these applications are managed nowadays and provide a solution that simplify and speed up the infrastructure operations. Furthermore, some of the applications have been tested in a limited but real scenario connecting secondary substations and managing smart metering and DER data. The tests mainly focused on the operational changes times in order to illustrate how the SDU approach can foster the innovation and make utility infrastructures more agile for dynamically introducing new elements and reducing up to 75% of the reconfiguration time of the analyzed smart grid functions.

At the end, the SDU prototype is not only a product, rather a methodology or a tool. It is better shown as a strategy to perform certain tasks autonomously depending on the requirements that apply for each certain case. Further, the implementations presented in this article provide a specific realization of this methodology, and SDU would allow programming the smart grid operation, enabling a more agile view of the electric power and ICT infrastructures of the utilities and reducing its operational costs and time.

Acknowledgments: Part of the work of this article was carried out within the framework of FINESCE project, funded by the Future Internet Public Private Partnership Programme (FI-PPP) of the European Commission's 7th Framework Programme (ICT-2011, grant number 604677); and ENVISERA project, funded by Spanish Ministerio de Economía y Competitividad (Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016, grant reference CTM2015-68902-R).

Author Contributions: Ramon Martín de Pozuelo developed the overall concept of the SDU and the required building blocks. He also led the execution of the trial deployment during FINESCE and the experimental evaluation of the system for different smart grid functions. Agustín Zaballos participated in the SDU conceptualization, supported the design of the WoE and context-aware security parts and participated in the writing and reviewing of the entire paper. Joan Navarro was in charge of the design, development and experimental evaluation of the HCDM system. Guiomar Corral provides her knowledge and expertise in security, participating in the design and development of the security modules and writing and reviewing the smart grid security aspects presented in the paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

API	Application Programming Interface
ACL	Access Control List
COSEM	Companion Specification for Energy Metering
DLMS	Device Language Message Specification
E2E	End to End
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
PKI	Public Key Infrastructure
RESTful	Representational State Transfer
SHA	Secure Hash Algorithm
SSH	Secure SHell
TCP	Transmission Control Protocol
TSO	Transmission System Operator
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VoIP	Voice over Internet Protocol

References

1. Navarro, J.; Zaballos, A.; Sancho-Asensio, A.; Ravera, G.; Armendáriz-Iñigo, J.E. The information system of INTEGRIS: Intelligent electrical grid sensor communications. *IEEE Trans. Ind. Inform.* **2013**, *9*, 1548–1560. [CrossRef]
2. Selga, J.M.; Corral, G.; Zaballos, A.; Martín de Pozuelo, R. Smart grid ICT research lines out of the European project INTEGRIS. *Netw. Protoc. Algorithms* **2014**, *6*, 93–122. [CrossRef]
3. Zaballos, A.; Vallejo, A.; Selga, J.M. Heterogeneous communication architecture for the Smart Grid. *IEEE Netw.* **2011**, *25*, 30–37. [CrossRef]
4. Martin de Pozuelo, R.; Ponce de Leon, M.; Howard, J.; Briones, A.; Horgan, J. Software defined utility: A step towards a flexible, reliable and low-cost smart grid. In Proceedings of the 5th International Conference on Smart Grid Systems, Barcelona, Spain, 7–9 September 2016.
5. Nunes, B.A.A.; Mendonca, M.; Nguyen, X.N.; Obraczka, K.; Turletti, T. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1617–1634. [CrossRef]
6. Gonzalez, A.J.; Martin de Pozuelo, R.; German, M.; Alcober, J.; Pinyol, F. New framework and mechanisms of context-aware service composition in the future internet. *ETRI J.* **2013**, *35*, 7–17. [CrossRef]
7. Khondoker, R.; Reuther, B.; Schwerdel, D.; Siddiqui, A.; Müller, P. Describing and selecting communication services in a service oriented network architecture. In Proceedings of the Kaleidoscope: Beyond the Internet?—Innovations for Future Networks and Services, Pune, India, 13–15 December 2010; pp. 1–8.
8. FP7 FI-PPP FINESCE Project Website. Available online: http://www.finesce.eu/ (accessed on 2 February 2017).
9. FP7 INTEGRIS Project Website. Available online: http://fp7integris.eu/ (accessed on 2 February 2017).
10. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid and smart homes: Key players and pilot projects. *IEEE Ind. Electron. Mag.* **2012**, *6*, 18–34. [CrossRef]
11. Rodríguez-Molina, J.; Martínez-Núñez, M.; Martínez, J.F.; Pérez-Aguiar, W. Business models in the smart grid: Challenges, opportunities and proposals for prosumer profitability. *Energies* **2014**, *7*, 6142–6171. [CrossRef]

12. Giorgetti, A.; Cugini, F.; Paolucci, F.; Valcarenghi, L.; Pistone, A.; Castoldi, P. Performance analysis of media redundancy protocol (MRP). *IEEE Trans. Ind. Inform.* **2013**, *9*, 218–227. [CrossRef]
13. Sancho-Asensio, A.; Navarro, J.; Arrieta-Salinas, I.; Armendáriz-Íñigo, J.E.; Jiménez-Ruano, V.; Zaballos, A.; Golobardes, E. Improving data partition schemes in smart grids via clustering data streams. *Expert Syst. Appl.* **2014**, *41*, 5832–5842. [CrossRef]
14. Spanò, E.; Niccolini, L.; Di Pascoli, S.; Iannacconeluca, G. Last-meter smart grid embedded in an Internet-of-Things platform. *IEEE Trans. Smart Grid* **2015**, *6*, 468–476. [CrossRef]
15. Selga, J.M.; Zaballos, A.; Navarro, J. Solutions to the computer networking challenges of the distribution smart grid. *IEEE Commun. Lett.* **2013**, *17*, 588–591. [CrossRef]
16. Savoia, A. Make Sure You Are Building the Right it before You Build it Right. Available online: www.pretotyping.org (accessed on 6 March 2017).
17. Vernet, D.; Zaballos, A.; Martin de Pozuelo, R.; Caballero, V. High performance web of things architecture for the smart grid domain. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, 1–13. [CrossRef]
18. Arrieta-Salinas, I.; Armendáriz-Iñigo, J.E.; Navarro, J. Epidemia: Variable consistency for transactional cloud databases. *J. Univ. Comput. Sci.* **2014**, *20*, 1876–1902.
19. Genez, T.A.; Bittencourt, L.F.; Madeira, E.R. On the performance-cost tradeoff for workflow scheduling in hybrid clouds. In Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, Dresden, Germany, 9–12 December 2013; pp. 411–416.
20. Briones, A.; Martin de Pozuelo, R.; Navarro, J.; Zaballos, A. Resource allocation on a hybrid cloud for smart grids. *Netw. Protoc. Algorithms* **2015**, *8*, 7–25. [CrossRef]
21. Li, S.; Zhou, Y.; Jiao, L.; Yan, X.; Wang, X.; Lyu, M.R. Delay-aware cost optimization for dynamic resource provisioning in hybrid clouds. In Proceedings of the IEEE International Conference on Web Services (ICWS), Anchorage, AK, USA, 27 June–2 July 2014; pp. 169–176.
22. Chu, H.Y.; Simmhan, Y. Resource allocation strategies on hybrid cloud for resilient jobs. *Small* **2013**, *1005*, 65.
23. Shifrin, M.; Atar, R.; Cidon, I. Optimal scheduling in the hybrid-cloud. In Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, Belgium, 27–31 May 2013; pp. 51–59.
24. International Electrotechnical Commission IEC 62351. Power Systems Management and Associated Information Exchange—Data and Communications Security—Part 6: Security for IEC 61850. Available online: https://pdfs.semanticscholar.org/9936/dc232462ae78004040a857463abd7e202b83.pdf (accessed on 24 May 2017).
25. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
26. Virvilis, N.; Gritzalis, D. The big four-what we did wrong in advanced persistent threat detection? In Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), Regensburg, Germany, 2–6 September 2013; pp. 248–254.
27. He, D.; Chan, S.; Zhang, Y.; Guizani, M.; Chen, C.; Bu, J. An enhanced public key infrastructure to secure smart grid wireless communication networks. *IEEE Netw.* **2014**, *28*, 10–16. [CrossRef]
28. The Associated Press. Iranian Hackers Infiltrated U.S. Power Grid, Dam Computers, Reports Say. Available online: http://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342/ (accessed on 18 May 2017).
29. Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Available online: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed on 6 March 2017).
30. Parks, R.C.; Duggan, D.P. Principles of cyberwarfare. *IEEE Secur. Priv. Mag.* **2011**, *9*, 30–35. [CrossRef]
31. Lee, A.; Brewer, T. Guidelines for Smart Grid Cyber security, Volume 1, Smart Grid Cybersecurity Strategy, Architecture, and High Level Requirements. Available online: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 24 May 2017).
32. Dierks, T.; Allen, C. RFC 2246: The TLS protocol. Available online: https://www.ietf.org/rfc/rfc2246.txt (accessed on 24 May 2017).
33. Ghafoor, I.; Jattala, I.; Durrani, S.; Tahir, C.M. Analysis of OpenSSL heartbleed vulnerability for embedded systems. In Proceedings of the IEEE 17th International Multi-Topic Conference (INMIC), Karachi, Pakistan, 8–10 December 2014; pp. 314–319.

34. Sánchez, J.; Corral, G.; Martin de Pozuelo, R.; Zaballos, A. Security issues and threats that may affect the hybrid cloud of FINESCE. *Netw. Protoc. Algorithms* **2016**, *8*, 26–57. [CrossRef]
35. Cleveland, F.M. Cyber security issues for advanced metering infrasttructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–5.
36. Goransson, P.; Black, C.; Culver, T. *Software Defined Networks: A Comprehensive Approach*; Morgan Kaufmann, Elsevier: Boston, MA, USA, 2014.
37. Chinnici, R.; Moreau, J.J.; Ryman, A.; Weerawarana, S. Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language. Available online: https://www.w3.org/TR/2006/CR-wsdl20-20060327/wsdl20-z.pdf (accessed on 24 May 2017).
38. Gu, T.; Pung, H.K.; Zhang, D.Q. Toward an OSGi-based infrastructure for context-aware applications. *IEEE Pervasive Comput.* **2004**, *3*, 66–74.
39. CISCO. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper. Available online: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html (accessed on 3 May 2017).
40. Guinard, D.; Trifa, V.; Mattern, F.; Wilde, E. From the internet of things to the web of things: Resource-oriented architecture and best practices. In *Architecting the Internet of Things*; Springer: Heidelberg, Germay, 2011; pp. 97–129.
41. Bo, C.; Xin, C.; Zhongyi, Z.; Chengwen, Z.; Junliang, C. Web of things-based remote monitoring system for coal mine safety using wireless sensor network. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 1–14. [CrossRef]
42. Aman, S.; Simmhan, Y.; Prasanna, V.K. Energy management systems: State of the art and emerging trends. *IEEE Commun. Mag.* **2013**, *51*, 114–119. [CrossRef]
43. Navarro, J.; Sancho-Asensio, A.; Zaballos, A.; Jiménez-Ruano, V.; Vernet, D.; Armendáriz-Iñigo, J.E. The management system of INTEGRIS. In Proceedings of the 4th International Conference on Cloud Computing and Services Science, Barcelona, Spain, 3–5 April 2014; pp. 329–336.
44. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58.
45. NIST Big Data Public Working Group (NBD-PWG). NIST Big data interoperability framework: Volume 1, definitions. *Natl. Inst. Stand. Technol.* **2015**, *23*, 132.
46. Werner, V. Eventually consistent. *Commun. ACM* **2009**, *52*, 40–44.