D3.2.5

Smart Lighting System Final Report

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D3.2.5 PU / 1.0
Activity and Work package contributing to the deliverable:	Activity 3 / WP 3.2
Due date:	30th September 2013 – M36
Actual submission date:	4th October 2013

Responsible organisation:	EDP
Editor:	Nuno Pereira
Dissemination level:	Public
Revision:	1.0

Abstract:	This document details the results of smart lighting system's evaluation. It includes an analysis of cloud computing's applicability to Public Lighting and to other Smart Grid systems.
Keywords:	Smart, Grid, Public, Lighting, Evaluation

Editor

Nuno Pereira (EDP)

Contributors

Nuno Pereira (EDP)

Miguel Areias (EDP)

Isabelino Coelho (EDP)

Paulo Santos (EFACEC ENG)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

Executive Summary

"A Smart Grid is an electricity network that can cost-efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety" (EU Commission Task Force for Smart Grids, 2010). It is supported by information and communications technology (ICT) that enables collection and processing of an increasingly high quantity of sensing data and its availability to entitled stakeholders and systems.

Data is collected from everywhere in the smart grid (SG) infrastructure, which includes consumer's homes through smart metering, power plants, substations and lines, and possibly electric vehicles. Collected data is analysed and transformed into useful information for manage and operate the electricity network. It is used as basis to support Human decisions and as input for automated functionalities such as disaster recovery and self-healing. Information is also available to consumers who can be aware of their consumption habits and are able to improve them.

A SG can have thousands up to millions of data collection/ delivery locations by covering city-wide up to country-wide areas. Data collection frequency varies from real-time or near-real-time, in the case of telemetry data, down to 15 minutes, a daily-basis, a monthly-basis or other defined frequencies, in the case of metering data. Therefore, a SG requires substantial computing power to process "big" amounts of complex data.

We perceive cloud computing as a cost-effective solution for a growing SG. It provides services such as on-demand self-service, broad network access and rapid elasticity that can be used to enhance SG's infrastructure, functionalities and services with benefits to clients and to the utility.

However, migrating SG's services to the cloud environment is not a decision to take lightly. A SG is a critical infrastructure. It is a backbone for economy, security and health as it provides ways to monitor and control the power we use in our homes, schools, hospitals, transportation, communication systems, etc. A failure in electricity supply impacts peoples' lives directly and indirectly by affecting other critical and non-infrastructures. A SG must be resilient and secure. In order to comply with these requirements, the cloud environment must ensure confidentiality, integrity and availability of data and services. Migration to an unprotected cloud environment would be unacceptable.

Smart lighting (SL) is a public lighting management system based on a cloud computing environment for a SG. Its purpose is to evaluate cloud computing's applicability to SG systems. A new SL application was developed and integrated in TClouds trustworthy infrastructure cloud which also uses TClouds cloud of clouds feature to provide resiliency to the system. The resulting solution is a scalable, secure and resilient smart lighting system (SLS) compliant with all defined requirements. Chapters 2 and 3 provide a detailed insight into the use case's background, assumptions and evaluation.

We also theoretically analysed cloud computing's application to other SG systems and components based on this results. While most SL requirements apply to other SG systems, the overall SG has more demanding requirements regarding data confidentiality and availability. For instance, consumption data is private information and has higher sensitivity than public lighting schedules. The finding is that a new SG architecture is required in order to take full advantage of cloud computing's features while complying with SG requirements. This analysis is detailed in Chapter 4.

Contents

List of tables

List of figures

Chapter 1

Introduction

1.1 TClouds — Trustworthy Clouds

TClouds aims to develop trustworthy Internet-scale cloud services, providing computing, network, and storage resources over the Internet. Existing cloud computing services today are generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes water, electricity, fuel, food supply chains, and healthcare industry. TClouds focuses on power grids, and electricity management and patient-centric health-care systems as main applications.

The TClouds project identifies and addresses legal implications and business opportunities of using infrastructure clouds, assesses security, privacy, and resilience aspects of cloud computing and contributes to building a regulatory framework enabling resilient and privacy-enhanced cloud infrastructure.

The main body of work in TClouds defines an architecture and prototype systems for securing infrastructure clouds, by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and by assessing the resilience, privacy, and security extensions of existing clouds.

Furthermore, TClouds provides resilient middleware for adaptive security using a cloud-of-clouds, which is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

1.2 Activity 3 — Benchmark Applications & User-centric Evaluation

Activity 3 focuses on the applications and the evaluation of the TClouds platform. The activity's objective is to define and validate cloud applications' architecture and specifications (the medical and the smart grid use case). For this purpose, Activity 3 will specify cloud and application functionalities and requirements, define application prototypes to be implemented on the cloud platform, and validate the application prototypes and the TClouds platform. For this purpose, the requirements defined in Activity 1 will serve as a generic guideline, which will be refined and consolidated in Activity 3. Finally, there is a continuous and close interaction between Activity 3 and Activity 2 in order to make sure that the platform and applications match the specifications and that the TClouds project achieves its overall objectives.

1.3 Workpackage 3.2 — Cloud-middleware and Applications for the Smart Grid Benchmark Scenario

The objective of WP3.2 is to define a sample Smart Grid application architecture and validate it by means of a prototype. We plan to develop a Public Lighting Management System (Smart Lighting) as our sample application that is migrated to the TClouds platform while providing scalable computing and enhancing its resilience and integrity assurance. WP3.2 also investigates how information gathering and response times could be achieved in a cloud-computing environment while achieving real-time timing guarantees. In close relation

with WP2.4, WP3.2 also evaluates, through a prototype in a real world environment, both scalability and availabilities while their resilience and intrusion tolerance increases. This architecture is linked and integrated in general with A2.

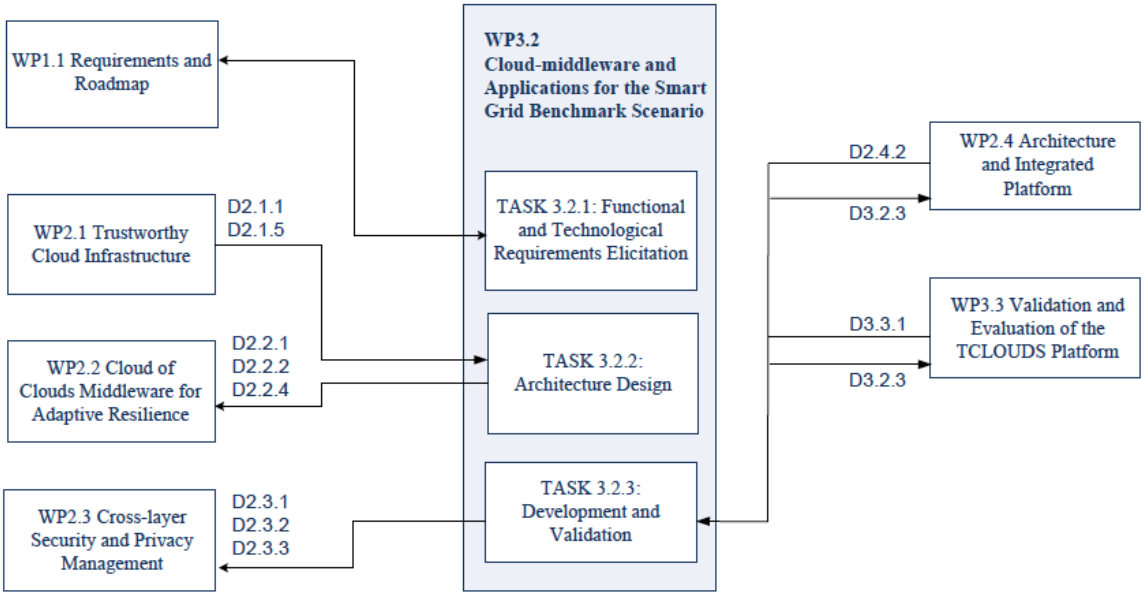

Figure 1: WP3.2 interdependencies

1.4 Deliverable 3.2.5 — Smart Lighting System Final Report

1.4.1 Overview

The smart lighting system (SLS) scenario was defined in D1.1.4. Its specification was delivered in D3.2.1. Its architecture design and functional validation scenarios were delivered in D3.2.2. A first prototype was presented in D3.2.3, including architecture changes for a better adaption of the application to the cloud environment. SLS security requirements were revised in D2.4.2. These requirements were used as criteria for selecting security components to be integrated with SLS. D3.2.4 presents the final version of the prototype, including its integration with trustworthy infrastructure cloud and cloud of clouds security components. A high level SLS validation protocol was presented in D3.3.3. D3.3.4 reports on the results of the validation activities.

Regarding legal, privacy and business issues, D1.2.4 delivers the results of a data privacy impact assessment (DPIA) and D1.3.3 details the results of a business impact analysis that were conducted for SLS.

D3.2.5 is the final report for the smart lighting system (SLS) use case. The purpose is to present use case's evaluation results and also the analysis of cloud computing's applicability to more demanding smart grid systems.

1.4.2 Structure

In Chapter 2 we give an overview of background and objectives for the SLS use case. In Chapter 3 we evaluate SLS based on defined requirements and validation results. In Chapter 4 we broaden the scope of the use case and we analyse the possibility of hosting more

demanding SG systems and components in a cloud computing environment. In Chapter 5 we draw conclusions.

1.4.3 Deviation from Workplan

The contents of this deliverable and related work are fully compliant with the defined workplan.

1.4.4 Target Audience

This deliverable aims at smart grid developers who are searching for new information and communications technology (ICT) solutions for their smart grid systems and that are interested in exploring cloud computing technology. It will help them understand the advantages and constrains of secure and resilient cloud computing for improving smart grid infrastructure and services. This deliverable assumes that the reader possesses background knowledge in smart grids and cloud computing.

1.4.5 Relation to Other Deliverables

D3.2.5 evaluates SLS based on security requirements that were revised in D2.4.2 and on validation results delivered in D3.3.4.

Chapter 2

Smart Lighting Use Case Overview

2.1 Smart Grid challenges

"A Smart Grid is an electricity network that can cost-efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety" (EU Commission Task Force for Smart Grids, 2010). It is supported by information and communications technology (ICT) that enables collection and processing of an increasingly high quantity of sensing data and its availability to entitled stakeholders and systems.

Data is collected from everywhere in the smart grid (SG) infrastructure, which includes consumer's homes through smart metering, power plants, substations and lines, and possibly electric vehicles. Collected data is analysed and transformed into useful information for managing and operating the electricity network. It is used as basis to support Human decisions and as input for automated functionalities such as disaster recovery and self-healing. Information is also available to consumers who can be aware of their consumption habits and are able to improve them.

A SG can have thousands up to millions of data collection/ delivery locations by covering city-wide up to country-wide areas. Data collection frequency varies from real-time or near-real-time, in the case of network telemetry data, down to 15 minutes, a daily-basis, a monthly-basis or other defined frequencies, in the case of metering data. Therefore, a SG requires substantial computing power to process "big" amounts of complex data.

As illustrative example, EDP's systems are already able to collect SCADA/DMS telemetry data in real-time from over 8,000 Km of high voltage (HV) lines, more than 400 HV/MV primary substations and 80,000 km medium voltage (MV) network feeding more than 60.000 MV/LV secondary substations, and also management data from the supporting communications network and server equipment, frontend locations and datacentres. LV consumption data, registered every 15 minutes, is currently being collected from more than 31,000 smart meters at consumers' homes on a daily basis. This number will grow up by 100,000 until 2014 and then up to six million until 2020 in the event of a possible roll out of smart metering technology.

EDP's smart grid architecture, depicted in Figure 2, is composed and operates in three main layers. The bottom layer (right on the figure) encompasses devices that can measure and monitor grid behavior through sensors on the grid or meters installed at homes. The middle layer is comprised of information technology systems that gather all the data being captured by the previous layer and deliver them to where they are needed. The top layer is responsible for analysing all the data gathered, translating and presenting it to stakeholders.

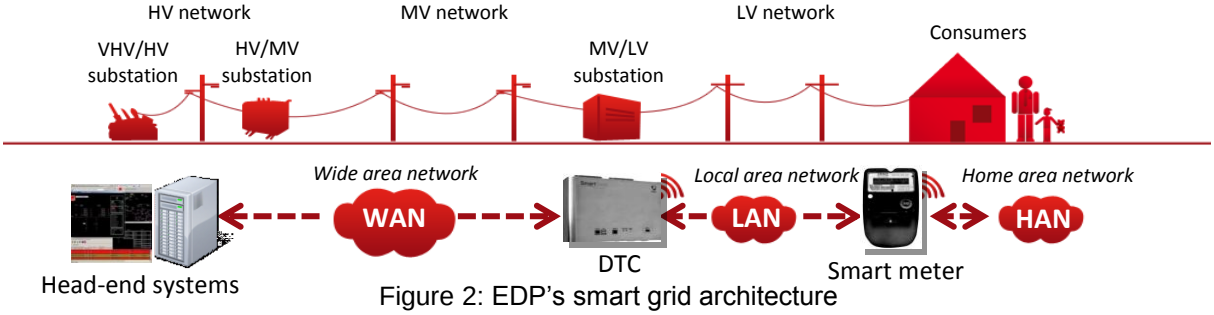

Figure 2: EDP's smart grid architecture

2.2 Cloud Computing Solution

We perceive cloud computing as a cost-effective solution for a growing SG. It provides services such as on-demand self-service, broad network access and rapid elasticity that can be used to enhance SG's infrastructure, functionalities and services with benefits to clients and to the utility. For example: 1) clients can have access to consumption data in real-time through the cloud and 2) a utility can increase data centres' management and operation efficiency; it is able to get computational power on demand, increased server efficiency, lower power supply and cooling systems all through an efficient and integrated resource management.

However, migrating SG's services to the cloud environment is not a decision to take naively. A SG is a critical infrastructure. It is a backbone for economy, security and health as it provides ways to monitor and control the power we use in our homes, schools, hospitals, transportation, communication systems, etc. A failure in electricity supply impacts peoples' lives directly and indirectly by affecting other critical and non-critical infrastructures. A SG must be resilient and secure. In order to comply with these requirements, the cloud environment must ensure confidentiality, integrity and availability of data and services. Migration to an unprotected cloud environment would be unacceptable.

2.3 Public Lighting Management Today

We selected public lighting management as a SG use case for this project with the purpose to evaluate cloud computing's applicability to SG systems. It is an important subject of concern to municipalities and to the utility in terms of personal welfare, security and cost efficiency. Public lighting costs have a great impact on municipality budgets once they are translated directly into the electrical bill that needs to be paid; on the other hand, public lighting is considered a factor that contributes to the safety of persons, property and the society in general. For this reason, effective monitoring and management can contribute to avoid overspending and to contribute to people's safety.

The designed use case scenario is based on the Portuguese reality where all public lighting concessions were granted to the only distribution system operator (DSO), which relates with strategic decisions made by the Portuguese government. However, there are countries in which public lighting is managed by a company that is not the DSO. The Portuguese situation may also change in the near future; between 2014 and 2020 most public lighting concessions will end and it is expected that municipalities will grant new concessions in an open market. In this context, the role of EDP is to manage the Portuguese public lighting system in line with the municipalities' requirements.

Figure 3: Portugal from space (NASA Earth Observatory, 2011) (left); Lisbon in the evening (right)

Nowadays, public lighting control is divided by two geographical groups: urban area (Porto and Lisbon), and remaining country. Porto's and Lisbon's public lighting is centrally controlled by two dispatch centres located in these two cities through a Centralized Remote System (CRS), which is able to control public lighting by sending signals through the electrical grid.

On the other hand, the remaining country has a completely different way to control public lighting, based on local equipment, such as astronomic clocks, light sensors or defined thresholds, and manually operated.

EDP's public lighting management systems are similar to other cases in Europe and, therefore, use case results will be useful to other utilities and vendors.

2.4 Smart Lighting – A new cloud-based solution

Smart Lighting is a public lighting management system for a Smart Grid (see D3.2.1, D3.2.2, D3.2.3). It was designed to address the cloud computing paradigm and, as such, it is quite different when compared with a traditional architecture. It consists of a web application (see Figure 4) hosted in a computing cloud that lets authorized users interact with the underlying Smart Grid infrastructure (see Figure 5 and Figure 6) in order to operate and extract information from the public lighting sub-system, thus enabling a more efficient management over the public lighting service.

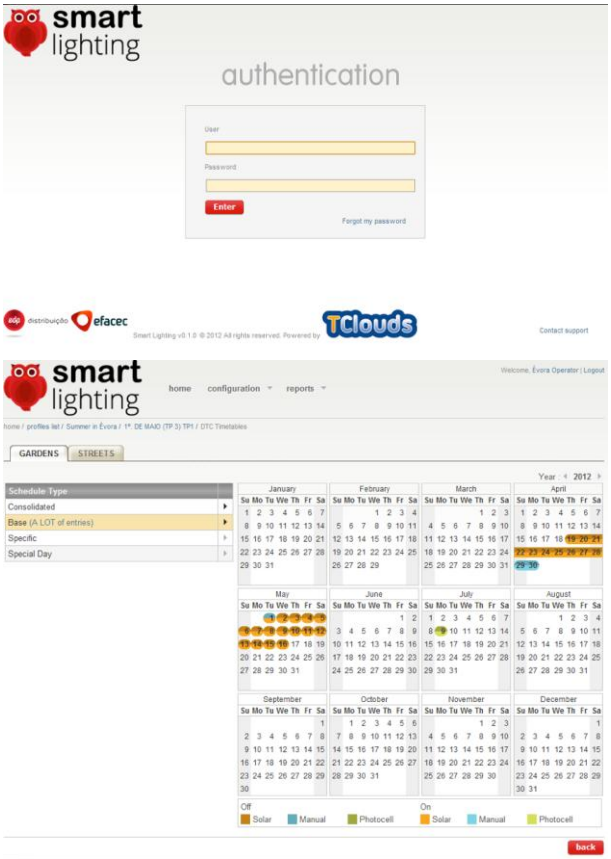

Figure 4: Smart lighting application interface

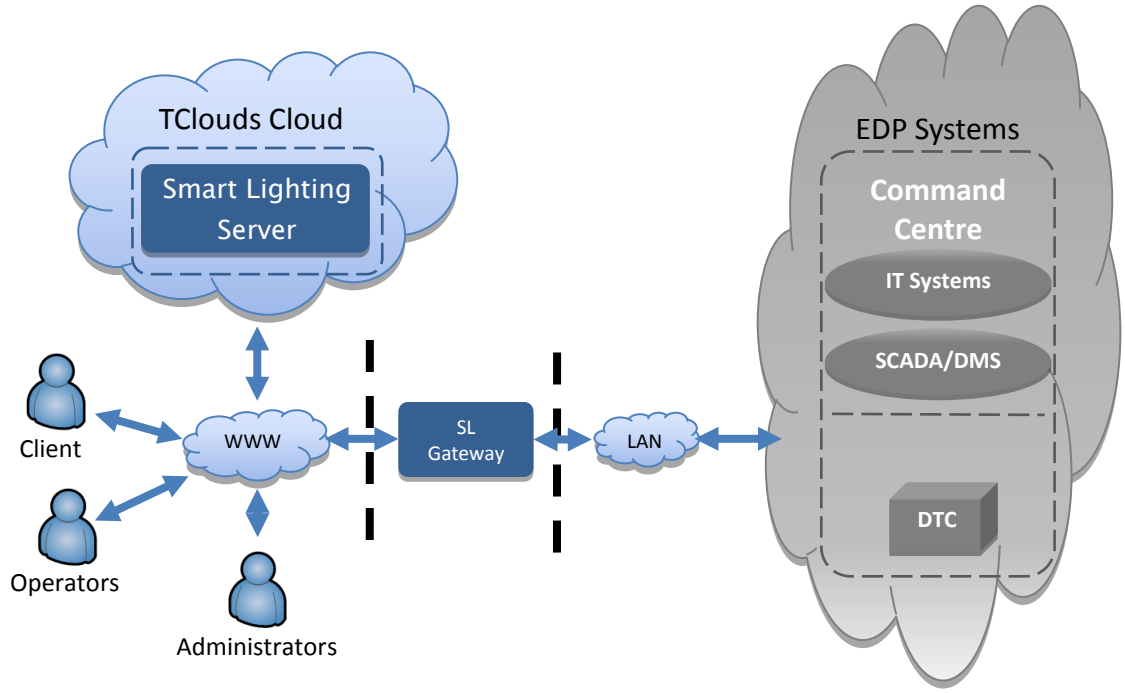

Figure 5: Smart lighting system architecture

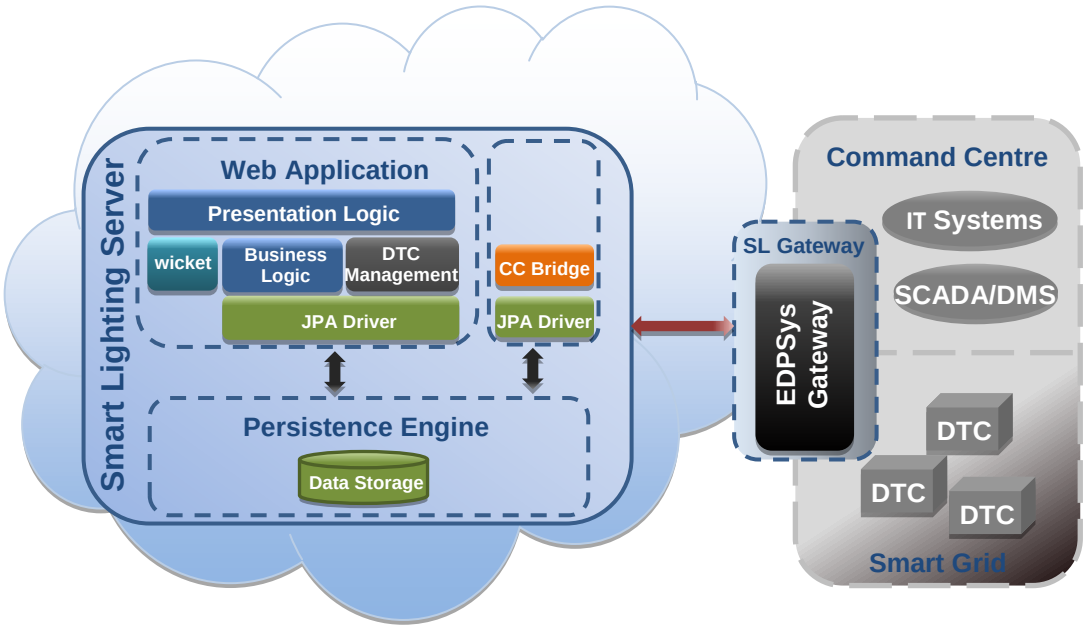

Figure 6: Smart lighting system component model

SLS provides functionalities such as on/off commands, real-time status, energy consumption and schedules update to client municipalities and to the operator utility. These functionalities rely on integrity and availability of the collected information. Grid operators are allowed to act upon public lighting with more information, ensuring the most efficient control. Also, municipalities are able to directly monitor the system, which allows them to make more specific and strategic decisions.

Users, including clients and operators, are allowed to generate reports about many operational aspects. It is possible to segregate access to information by defining what kind of data each user can access.

The cloud environment brings to the utility the scalability and computational power needed to manage a system with high level of geographic expansion and constant integration of new assets. Smart Grid components in general and public lighting in particular involve many different kinds of technical devices which, in many cases, are vulnerable to failures or damage. With a cloud based solution using TClouds' security components this impact is reduced, bringing a higher reliability to the system.

From the utility point of view, cloud computing ads flexibility to hardware investment plans. It allows lower startup investments and also the possibility to evolve the solution to follow changing requirements.

2.5 Smart Lighting Security and Resilience

SLS takes advantage of TClouds' Trusted Infrastructure Cloud (see D2.1.5, Chapter 3) and Cloud of Clouds (see D2.2.4) concepts in order to acquire security and resilience properties. The final integration architecture is depicted in Figure 7 as it was presented in D3.2.4.

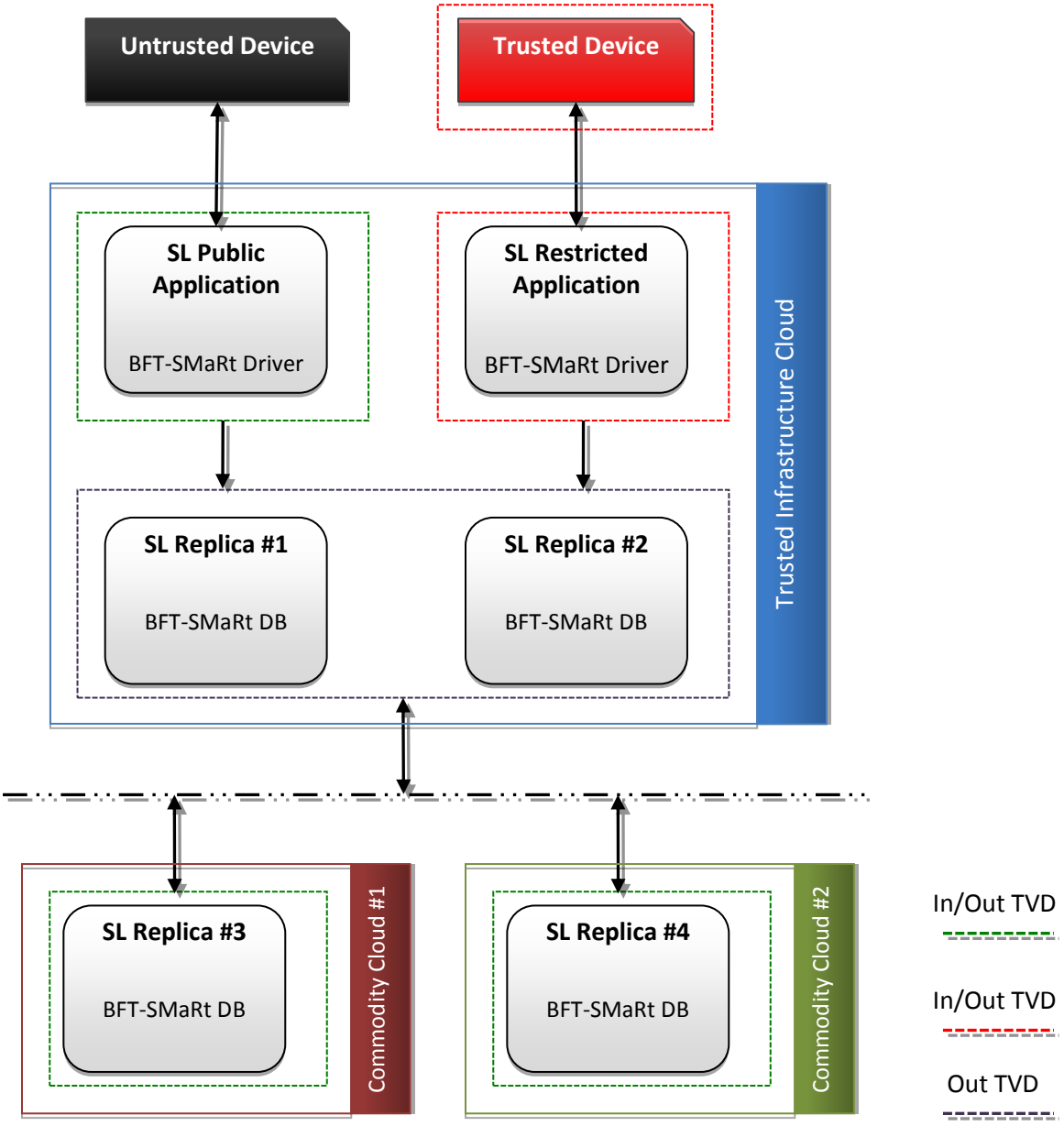

Figure 7: Smart lighting system integration architecture

The final SLS integration architecture environment is composed by two Smart Lighting Web application instances and several BFT-SMaRt nodes. Each BFT-SMaRt node is composed of a database instance and a BFT-SMaRt component that is responsible for communication between nodes and their local database. Communication between nodes uses the BFT-SMaRt protocol (see D2.2.4, Chapter 2) in order to ensure data integrity.

The SLS Web application instances and BFT-SMaRt nodes run inside virtual machines (VM) provided by TClouds' Trusted Infrastructure Cloud (see D2.1.5, Chapter 3), which consists of Trusted Server (TS), Trusted Channel (TC) and Trusted Object Manager (TOM) components. One of the web applications is protected by a Trusted Virtual Domain (TVD) and is the entry point for users with operation/ administration privileges (Operator and Administrator users). The other is outside the TVD in order to enable access from a normal computer to users with read only privileges (Client users). Therefore, integrity and confidentiality are enhanced.

In this architecture, while all elements can run locally inside the Trusted Infrastructure Cloud, replica nodes can also be distributed through other clouds in order to enhance resilience and, therefore, availability.

It would also be beneficial to integrate TClouds' Tailored Memcached component in a more demanding Smart Grid use case. However, in SLS use case environment, due to its small dimension, these benefits would not be visible. Therefore, although it would be integrated in a future development of the system, we decided not to integrate it in the final prototype in order to focus our efforts in the components mentioned above. As such we used a standard Memcached in the final prototype.

Chapter 3

Smart Lighting System Evaluation

3.1 Requirements

We have identified functional, design, security and economic requirements for SLS.

3.1.1 Functional requirements

Functional requirements define functions of SLS and its components (see Table 1). A complete set of functional validation scenarios were defined D3.2.2. However, in WP3.3 it was decided that the focus of validation regarding use case applications, including smart lighting, would be privacy, security and resilience. Therefore, these scenarios were not executed.

Table 1: Functional requirements table

Requirement name	Requirement #	Description
Monitor consumptions	ASFUNREQ1	The system must record all consumptions registered by EBs.
Monitor state and anomaly events (alarms)	ASFUNREQ2	The system must monitor the state and alarms triggered by the DTCs.
Manage lighting Services and Schedules	ASFUNREQ3	The system must have an interface to manage the lighting services and also to create/edit/remove schedules.
Manage public lighting settings	ASFUNREQ4	The system must have an interface to manage lighting preferences.
Actuate over control circuits	ASFUNREQ5	The system must have an interface through which users with the right privileges are able to actuate over lighting control circuits and receive the feedback of their actions.
Manage settings of public lighting intelligent devices (DTC & EB)	ASFUNREQ6	The system must enable users with the right privileges to manage the settings of public lighting devices.
User access control	ASFUNREQ7	The application must restrict user access based on specified user profiles.

3.1.2 Design requirements

Design requirements are guidelines for the architecture design process (see Table 2). The only defined design requirement for SLS is the usage of cloud environment, which allows us to evaluate cloud computing applicability to public lighting management.

Table 2: Design requirements table

Requirement name	Requirement #	Description
Usage of clouds environment	ASDESREQ1	The Smart Lighting system must be hosted in a cloud environment.

3.1.3 Security requirements

Security and resilience requirements (see Table 3) assure confidentiality, integrity and availability of data and services. These requirements are validated and prioritized in D3.3.4. The results of this analysis are summarized in Section 3.2.

Table 3: Security requirements table

Requirement name	Requirement #	Description
Trustworthy Audit	ASSECREQ1	Smart Lighting actions (application access; create, update and delete data) must be fully audited, and accessible only to privileged users.
Trustworthy Infrastructure	ASSECREQ2	The hosting infrastructure must prevent intrusions.
Trustworthy Persistence Engine	ASSECREQ3	The persistence engine must prevent intrusions and ensure confidentiality, integrity and availability
Resilient	ASSECREQ4	The Smart Lighting System must be fault-tolerant at infrastructure and persistence level.
Trustworthy communications	ASSECREQ5	Communications between a client and the Smart Lighting System must prevent data from being altered by using adequate security mechanisms.
High performance & Scalable	ASSECREQ6	The Smart Lighting System must have near-realtime performance, and able to scale on increased load.

3.1.3.1 Confidentiality

The SL system must prevent unauthorised access to the application, overall infrastructure and system configurations. However, public lighting schedules are public information; therefore there are no legal or privacy concerns.

3.1.3.2 Integrity

Communication between a client and SLS must be completely secure, e.g. there is no possibility to corrupt data.

3.1.3.3 Availability

Smart lighting is a near real-time system; therefore, data must be available when needed in the overall system.

3.1.4 Economic requirements

The only defined economic requirement is cost effectiveness (see Table 4). A cost effective smart lighting solution will contribute to the adoption of cloud computing to other smart grid systems and to other critical infrastructures. In WP1.3 and WP3.3 it was decided that an economic analysis of smart light (and healthcare platform) would be out of scope of TClouds.

Table 4: Economic requirements table

Requirement name	Requirement #	Description
Cost effective	ASECOREQ1	A cloudified-trustworthy Smart Lighting System must be cost effective when compared to a traditional in-house hosting approach.

3.2 Survey results

An external stakeholder survey was conducted in WP3.3 in order to validate and prioritize smart lighting system security and resilience requirements. This process is further detailed in D3.3.4. The final results of the survey are presented in Table 5.

Table 5: Smart lighting prioritization table

Requirement name	Requirement #	Value to municipalities	Value to utility	Value to vendor	Priority rating
Trustworthy Audit	ASSECREQ1	5	10	10	8
Trustworthy infrastructure	ASSECREQ2	6	9	10	8
Trustworthy persistence engine	ASSECREQ3	5	8	10	8
Resilient	ASSECREQ4	8	10	10	9
Trustworthy communications	ASSECREQ5	9	10	10	10
High performance & scalable	ASSECREQ6	4	9	10	8

3.3 Validation results

In D3.3.4 we presented a set of validation activities focusing on the validation of SLS security properties. There were defined six integration validation activities and also specific activities to validate each integrated TClouds' component: five for BFT-SMaRt, three for TOM, three for TS and two for TC. Details of performed execution steps are detailed in D3.3.4. All validation activities were performed with success.

3.4 Evaluation and Conclusions

The SLS use case allowed us to assess the feasibility of hosting a part of our SG – the public lighting management service including related systems - in a cloud computing environment. There was defined a set of requirements regarding the three pillars of cyber security, namely confidentiality, integrity and availability.

Soon it was identified by TClouds' legal team that SLS does not present major confidentiality issues, which is mainly due to the fact that it does not collect, process neither store personal customer data. In fact, SLS only deals with lighting schedules, which are public information, and schedule related equipment configurations, which are considered reserved information. On the other hand it was necessary to ensure that the SLS considers different types of users in order to allow the right access privileges to the right type of users, which include administrators, operators and clients. Therefore, the definition of security requirements targets also confidentiality issues. Although access control mechanisms were implemented at application level, the Trusted Cloud Infrastructure implements also security mechanisms regarding confidentiality protection. Administration and operation read-write required privileges are only allowed when accessing SLS through the use of a Trusted Device (TD) that connects to a restricted instance of the application that is inside a TVD. Client read-only required privileges are allowed from a common computer which will connect to a public application instance inside the TI. The TVD concept allows that the two application instances are isolated from each other, which was successfully validated. VPN connections are used in communications between internal TI components: TC, TOM and TS. Also, machines' hard disks are encrypted. Furthermore, IPSec is used to ensure confidentiality in communications between all replicas on public clouds (untrusted part of the system) and the VMs that are hosted in the Trusted Infrastructure (TI).

On the other hand, integrity and availability are linked with the requirements that were higher rated by SLS stakeholders in the validation survey. When asked to choose between the two, stakeholders chose integrity. As it was already discussed in D3.3.4, it is important that information is available but, if it does not maintain its integrity, it might lead to wrong and potentially dangerous decisions with impact in society (e.g. a street blackout due to wrong scheduling hour). Integrity at infrastructure level is ensured by the trusted infrastructure cloud. BFT-SMaRt is used to ensure the integrity of communications between replicas and between replicas and clients. As it is explained in D2.2.4, Chapter 2, it relies on the answers given by all replicas, and not just one entity, in order to verify the data integrity. In communications between replicas, BFT-SMaRt uses Message Authentication Codes (MACs) based on the SHA-1 algorithm as it was validated. Therefore, any modification on the messages will be detected and modified messages are discarded.

Regarding availability, BFT-SMaRt enhances the resilience of the system with the use of several replicas in order to keep the system working in the case of a fault occurrence. As it is explained in D2.2.4, Chapter 2, BFT-SMaRt tolerates the occurrence of "f" faults with "3f+1" replicas, which means that with four replicas it will tolerate one fault. Also, by using the concept of cloud of clouds, we rely on the assumption that a security issue that affects two different clouds (different technologies and configurations) is low in a short time frame is very unlikely to occur. We also performed validation activities where we stressed the resilience of

BFT-SMaRt in this environment and we obtained results that are compliant with specified security requirements. Also in these tests we saw that response times are not compatible with near-real-time Smart Grid systems. Note that near-real-time performance is a functional requirement of SLS. However, we recognized that this is rather due to network latencies between clouds than due to the BFT-SMaRt implementation itself. Nevertheless, we are certain that all these limitations can be overcome with continued investment into the component development.

In the SLS use case, TClouds' cloud computing solution meets all specified security requirements and it is therefore a secure and resilient solution for public lighting management in a SG. Although, there is still investment to be made in the development of a future solution in order to improve system performance in a cloud of clouds environment.

Chapter 4

Smart Grid in the Cloud Analysis

In this chapter we analyze the possibility of exploiting cloud computing to more demanding SG areas beyond public lighting management.

4.1 Smart Grid Requirements

The power system always needs to be available. Therefore, it is imperative that any security countermeasures implemented in the Smart Grid do not impact power availability or safety. Lack or omission of information in the system, for example, during an emergency situation, could cause safety issues.

In most Industries, confidentiality and Integrity have higher precedence over availability. However, in the electrical power systems there is a slight difference once electricity must always be available. In these specific systems the more important security attribute is availability followed by integrity and finally by confidentiality.

4.1.1 Availability

Availability, as already mentioned, is the major security attribute of the electrical power system. These systems continuously monitor the state of the grid, in an estimated maximum latency of 8.3 milliseconds (Wright, Kinast, & McCarty, 2004) (for a typical SCADA configuration of 1200 baud, 8 data bits, 1 start bit, and 1 stop bit, transmitting one character), and a disruption in the information update can cause a loss of power. The righteousness, despite availability, of the electrical power will be dependent on the quality of the current state estimation in the power system and can be translated in integrity of input data.

4.1.1.1 Reliability and Fault Tolerance

The SCADA system relies on fault tolerance mechanisms based on hot-standby functionalities. Upon a computer failure, identified by the loss of communication, the system automatically transfers the functionality to the secondary (stand-by) computer. It is important to note that the failure determination is done independently from either computer, so a failure of either computer alone does not jeopardize the monitoring/control process. If the primary computer fails, the transfer to the hot standby is automatic. If the secondary computer fails, the primary continues all of the monitoring/control functions.

This approach has the ability to tolerate faults and it is normally used in the most critical systems that may need to operate even while under attack by intruders, viruses, or even malfunctioning servers.

4.1.2 Integrity

Data integrity in the critical infrastructures is one of the most worrying characteristic to address considering the main CIA (Confidentiality, Integrity and Availability) security

attributes. SCADA systems are traditionally prepared to operate while some servers are malfunctioning. This is achieved, as mentioned before, by a hot standby[1] system that ensures extreme reliability through data replication mechanisms. Loss of data integrity, in a SCADA system, can result in failures in the power supply or even blackouts. This is because all the system updates are centralized on a dashboard and shown to the operator. A malicious change on that information can induce or influence the operator to perform actions based on wrong information or influencing wrong decisions.

4.1.3 Confidentiality

The underlying challenges about data confidentiality on a Critical Infrastructure environment are similar to any other system and rely on ensuring that only authorized entities can gain access to that information. When unauthorized individuals or systems can have access information then, confidentiality is breached. Usually the value of confidentiality is high when it concerns personal information about people and their behaviour. Considering this last paragraph and in the context of our work, problems arise when the SCADA system become border and, through the Smart Grid, starts to deal with personal and private information.

4.2 Smart Lighting Requirements versus Smart Grid

D1.3.3 presents a risk analysis focusing on the operational criticality of major categories of services in SGs, concerning loss of Availability, Integrity and Confidentiality. It is also assessed the impact of identified risks regarding financial, business continuity and reputation impact.

SL is a subsystem of the SG. There are some issues and concerns that are similar to those of other systems and there are others that are completely different. If we map SL to the SG services that are listed in the risk analysis, it fits inside Grid Control and Operation. As it was stated before, its criticality is very high when considering availability and integrity, although regarding confidentiality its criticality is moderate. Loss of availability has moderate financial, business continuity and reputation impact. Loss of integrity has moderate financial impact but high business continuity and reputation impact. Loss of confidentiality has moderate financial and business continuity impact but low reputation impact.

When comparing SL with other SG services there are two relevant differences. First, notice that confidentiality has moderate criticality while other services such as energy metering management have very high criticality. The reason for this difference is that while smart lighting stores and processes public lighting scheduling information, energy metering management services deal with customer information, which raises data privacy issues. The second difference is not visible directly. Grid control and operation services include also collection, processing and presentation of grid telemetry data to grid operators, which requires real-time performance, instead of near-real-time as required by SL. This means that although the SL use case results are very promising for services with similar or lower requirements, it set requirements too low when considering more demanding Smart Grid use cases, namely regarding availability and confidentiality.

[1] Hot standby is a method by which a redundant standby server is ready to run at any moment, when the primary fails, without requiring further setup configurations.

4.3 Conclusions

What we learned from TClouds tells us that it is feasible to use cloud computing inside a Smart Grid as long as security and resilience requirements are met. This depends on the specific Smart Grid part in which cloud computing will be used and it also depends on the type of cloud environment that is considered (public, private or hybrid). Security requirements for a public cloud might be different than those that would be specified for a private cloud, thus reducing solution complexity. In fact, companies such as EDP are already starting to create their own private clouds by using virtualization technologies in their data centres.

Chapter 5

Conclusion

With TClouds we were able to understand, test and validate the added value of a resilient and trustworthy cloud environment when used in a critical infrastructure. Technically we were able to design a smart grid cloud-based solution and to assess its benefits and drawbacks through a thorough validation process.

These results are the cornerstone to a future decision regarding migration of our systems to a cloud computing environment based on the developed risk analysis. We now know which smart grid components can be migrated to a cloud computing environment and we understand the corresponding risk at financial, business continuity and reputation levels.

A new smart grid architecture based on cloud computing can emerge in following years, not only considering hosting of data centre components in a cloud environment, but also to take advantage of the cloud environment for remote devices such as smart meters and data concentrators. This evolution will require the development of new privacy and security solutions in order to address new challenges in this area.

Chapter 6

List of Abbreviations

Table 6: List of Abbreviations

DPIA	Data Privacy Impact Assessment
DSO	Distribution System Operator
DTC	Distribution Transformer Controller
EC	European Commission
EU	European Union
HV	High Voltage
LV	Low Voltage
SCADA/ DMS	Supervisory Control and Data Acquisition / Distribution Management System
SL	Smart Lighting
SLS	Smart Lighting System
SG	Smart Grid
SM	Smart Metering
TC	Trusted Channel
TI	Trusted Infrastructure
TD	Trusted Device
TOM	Trusted Objects Manager
TS	Trusted Server
TVD	Trusted Virtual Domain
VM	Virtual Machine

References

EU Commission Task Force for Smart Grids. (2010). *Expert Group 1: Functionalities of smart grids and smart meters - Final Deliverable.*

NASA Earth Observatory. (2011). *Iberian Peninsula at Night.* Retrieved August 23, 2013, from http://earthobservatory.nasa.gov/IOTD/view.php?id=76777

Wright, A., Kinast, J., & McCarty, J. (2004). *Low-Latency Cryptographic Protection for SCADA Communications.*