Building a Service Manager For a Smart City Archicture

Towards a service manager in an interoperable environment

Gutemberg Rodrigues Costa Cavalcante[1], Felipe Silva Ferraz[1,2], Guilherme Luiz Mario de Medeiros[1]

[1]CESAR
Recife Center for Advanced Studies and Systems
Recife, Brazil
gutembergrcc@gmail.com
fsf@cesar.org.br
guicaraciolo@gmail.com

[2]Informatics Center
Federal University of Pernambuco
Recife, Brazil
fsf3@cin.ufpe.br

Abstract - **Cities are becoming more and more populous and complex, and this growth is forcing them to better administer their management services. As a result of this growth, and of technological advances, cities are investing in technology so as to become smarter, thereby obtaining quicker results. This technological scenario has not only produced benefits for cities but also fragilities in them. Since the services that a city offers are vital and some of these require confidentiality, the focus has shifted to information security. To ensure their information is covered, cities need specific technologies, such as City Security Layer (CSL), in order to solve security problems arising. This paper focuses on constructing a module that complements CLS. This module is responsible for managing the services available in a network controlled by CSL.**

Keywords- security; smart city; architecture; services.

I. INTRODUCTION

Cities are constantly growing. Nam et al. [1] assert that they are becoming more and more populous and complex. According to Dirks et al. [2], in the 20th century, less than 20 cities around the globe had more than one million citizens. Today, this number has risen to 450 cities. Given this demographic growth, cities are encountering new series of risks, concerns and problems. According to Nam et al. [1], the main problems will be: a deterioration in the quality of the air, in traffic flows and an increase in economic risks, such as greater unemployment and the challenge of ensuring the best use of communication technologies so that it is possible to offer citizens an infrastructure that will become more and more prosperous [3][4].

With regard to the prosperity of cities, according to Sen et al. [5], this could be achieved when the ways that people think about health, security and economic issues are as important as their thinking on tackling uncontrolled urban development. According to Dirks et al. [2], to attend to these matters, the main services that cities offer should become interconnected, thus enabling new intelligence levels to be attained and, therefore, able to meet their own demands and those of their citizens.

In these cities, what is perceived is not only population growth, but also, as Dirks et al. [2] point out, such cities undergo a rise in their economic and technological activities. On the other hand, for Sen et al. [5], it is important to state that revolutionary change in communications is imminent. Such breakthroughs are becoming a reality and arise out of the services being created in cities.

Moreover, according to Sen et al. [5], the option to create services forces and makes software programs even smarter and more and more connected, to such an extent that they can exchange information, thus allowing new solutions to be created. The vision for smart cities is to see them as interconnected urban areas [6][7], which are sustainable and efficient, since all city services are crafted and maintained by focusing on their sharing data with each other. Therefore, it is possible for cities to gather information and take decisions more quickly and reliably. This integration of and between city services is not only a source of benefits, but it also is an imminent point of problems or vulnerabilities when information security is taken into account [8]. This is why Bartoli et al. [8] affirms that one of the biggest challenges when developing smart cities is related to the security of systems.

According to Bartoli et al. [8], Information Security should not only deal with deliberate attacks, such as those by disgruntled employees or for the purposes of industrial espionage, but also vulnerabilities such as that from a malicious entity that has penetrated a network [5][8], and thus has access to how software and data are controlled and, therefore, it can modify and damage the entire system.

This study was prompted after noting the lack of research studies on information security concepts with regard to the peculiarities of urban environments or smart cities. Among the few published papers, CSL stands out in the management of identifiers of entities but there remains the need to extend this solution to include the register of services that a smart city will consist of.

This article is organized as follows: Section 2 addresses how to define a smart city and the different services it may offer. Section 3 defines the security challenges that smart cities need to face up to. Section 4 discusses the CSL security layer, how it is structured, and what challenges it tries to overcome. Section 5 describes the *Service Manager* as a solution for managing services of a smart city. Section 6 sets out a validation of the *Service Manager* module with the CSL layer. Finally, some conclusions are drawn and suggestions made for future research studies in Section 7.

 ISBN: 978-1-61208-438-1

II. SMART CITY AND SERVICE DISTRIBUTION

According to Dirks et al. [2], rapid growth in population creates a new set of challenges for the infrastructure services of cities while, at the same time, creating new economic opportunities and social benefits.

Washburn et al. [9] is of the opinion that as people migrate to urban areas, resources become limited and badly managed. As a result of this, Dirks et al. [2] point out that problems will arise to do with high costs of living. For example, as to fresh water, it is expected that it will increase 25% in price by the mid-2030s. The high cost of living in some cities can already be observed in terms of people looking to the private sector due to the lack of some basic provisions in health and education services by government.

For Dirks et al. [2], cities that are already facing these challenges need to act by making using of new technologies so as to transform their systems and, in so doing, they will be better able to manage their resources and thus become more competitive. In order to achieve this, Ferraz et al. [7] and Kanter et al. [10] state that, when the tools and services of cities are integrated into a network, they will contribute to higher efficiency, since they will be able to use an enormous range of information, thereby enabling them to be creative and to make assertive decisions that are well-founded.

A city has different systems and distributed services. What we understand as services and systems is the combination of the complete range of resources for a specific function. Such services may be represented as being part of a set, which according to Ferraz et al. [7] can be separated and organized into several categories: education, public safety, transport, energy and water, health and governmental bodies.

According to Dirks et al. [2], we should note that what these services comprise, may vary from city to city, and in the number of citizens, since each city has its own characteristics, but nevertheless within the groups presented and defined. Dirks et al. [2] and Ferraz et al. [7], go on to state and demonstrate that the effectiveness and efficiency of these services will determine how successful the city that provides them will be. In the next section, each category of service in a smart city will be analyzed.

A. Types of Service

A city can offer different types of services. According to Ferraz et al. [7], services can be in the following areas: education, public safety, forms of transport, government services, health, energy and water.

Education: This represents the services that are directly and indirectly related to all educational services, such as, for example, setting standards for student's grades or educational shills.

Public Safety: This represents the services that help cities to respond quickly responds to emergencies, thus guaranteeing safety in a city. With the help of these services, for example, we are able to identify the rate of theft in certain areas.

Transport: Transport services include the state of roads, seaports, and airports. For example, controlling the volume and flow of traffic on city roads.

Government: This represents each system which works within governmental frameworks. For example, the control of a city's budget and expenditure.

Health: This represents services that help improve public health. By using these services, users will be able to have a shared medical record, that is always available, and which will lead to quicker and more precise diagnoses.

The smart integration of those services in a smart city will not only deliver benefits. One example is the evolution of the health services, where paramedics or even patients can be advised at a distance how to store and apply drugs. For Verbauwhede [11], this evolution will only be possible when there are strong privacy and user authentication policies. This privacy and authentication can be supplied by providing artefacts with protocols and cryptographed application software, as will be seen in the following section.

III. SECURITY IN SMART CITIES

According to Bodei et al. [12], studies showed the need for a new set of research studies focusing on improving information security, when dealing with smart cities [5][8].

In the midst of the problems related to information security, a subset of security questions is present in the backdrop to smart cities, amongst which worthy of special mention are access to information, tracking items of information and citizens, loss of data and unauthorized access to datacenters.

The issues above are dealt with in a broader study undertaken by Ferraz et al. [7], and are presented here as a way to illustrate points that smart cities will need to address.

These three issues are discussed in the following subsections.

1) Issues related to access to information

The interaction between software and the network involves data sharing. According to Sen et al. [5], this interaction can represent a threat since the data from different entities can become accessible. The traffic of packets from a device to the network, and from the network to other devices is a concern, since these packets can be intercepted when they are being transferred.

2) Issues related to data tracking

One important characteristic in an interconnected environment is the fact that a set of information used by one system cannot be traced back to the originator of the data. This kind of problem can destroy the anonymity that the services supply.

3) Issue related to entity tracking related issues

Each smart city may have many distributed sensors to capture data and facilitate the integration of systems. For Sen

 ISBN: 978-1-61208-438-1

et al. [5], information from these sensors must not be used to track entities. More information can be found in [13][14].

All problems here described are related to access and security matters. For Bartoli et al. [8], an alternative for solving some of those problems is by using key management. This means providing secure management of data encryption. The author states such management will ensure users are authenticated and authorized. According to Bartoli et al. [8] and Li et al. [15], for effective protection in a smart city, a series of security related problems needs to be addressed, and a predefined plan or goal should be adhered to.

What this consists of will be discussed in the next section. Similar solutions will be analyzed and a new layer will be put forward that aims to solve the problem of controlling entities and ensuring authenticity in smart cities.

IV. CSL

This section will discuss the CSL approach, as a solution to identity security in a smart city. In the first topic, a brief description of the problem will be given. The second topic will present similar solutions and the third and final topic will discuss the CSL.

A. Problem

In Section 2, the concept of a smart city was described as comprising different services. Given the growing number of such services and related entities, the complexity of security problems has also kept growing.

Among the problems detected, attention is drawn to the situation when the information service requests the service provider to supply it with confidential personal information on third parties.

According to Ferraz et al. [14], exchanging information via a network is considered to be unreliable because messages are subject to losses and interception when they are transmitted, as set out under security in Section 3. In short, the problem identified is based on guaranteeing the anonymity of an entity within the environment of a smart city.

There are already some solutions on the market that address these problems but none of them focuses on smart cities, as will be shown in the next topic.

B. Similar solutions

Some of the problems mentioned in Section 3 can be mitigated by some of the existing security solutions. According to Ferraz et al. [17] approaches such as using Open Authorization (OAuth), Security Assertion Markup Language (SAML) and OpenID may help the process of giving cover to some security flaws.

OAuth (Open Authorization), according to Yang et al. [18], is an authentication protocol used for storing secure data, whereby the owner of the storage does not need to provide his access credentials. The Security Assertion Markup Language (SAML), according to Saklikar et al. [19], is an XML-based framework for exchanging authentications, authorizations and data. By using SAML, a relationship of trust between entities in a network environment can be created. On the other hand, OpenID is an open technology in which, according to Ferraz et al. [17], users are identified by a URL. In systems using OpenID, users do not need to create a new account to access them. Users only need to be authenticated by an identity provider.

For Ferraz et al. [17], solutions like OpenID, SAML and OAuth, are fundamental to ensure users' security. However, these protocols cannot cover all existing security problems. Most of these concerns are related to the fact those solutions are focused on authentication and authorization, which, in an environment full of sensitive data, is not sufficient. CSL arose with a view to having a solution for dealing with anonymity between entities in a smart city and will be described in the next topic.

C. CSL Solution

CSL represents a layer that should be placed on the external border of a service, or a set of services, in smart cities.

According to Ferraz et al. [20], the main objective of CSL is to be the layer responsible for modifying the identifiers of services when messages are exchanged. The new identifier will be generated based on combining the previous identifier with the service to be accessed.

For Ferraz et al. [20], by means of this process, it is possible to ensure that an entity keeps itself anonymous within the entire smart city environment, even when this entity accesses multiple services, since the creation of the identifier consists of combining two other identifiers. The final access identifier will be different for each of the services.

By using CSL, it is expected that there will be an increase in security, since there will now be a layer which will provide a unique identifier for each service. With this approach, the real identity of the entity is preserved. On the other hand, Ferraz et al. [20] stresses that CSL does not provide resources to ensure authentication and authorization, which OAuth, SAML and OpenID do. Therefore, making use of an extra layer or solution to address vulnerabilities on this matter is required.

Despite the limitations mentioned, the security problems shown in Section 3 are partially covered by CSL. Table 1 illustrates the coverage of each item.

TABLE I. CSL COVERAGE

Risks	Coverage
1. Data Access	✓
2. Data tracking	✓
3. Entity tracking	✓

According to Ferraz et al. [20], if any packets shared between entities which go through CSL are intercepted, it will be hard to identify and understand who is who, since the interceptor will not know what the identifiers of these entities are. This covers the first issue, described in Section 3.

 ISBN: 978-1-61208-438-1

When there is anonymity of the entities during communication, the second issue is covered as well, since the difficulty of identifying which information is associated with which entity makes it hard to map the relationships. This characteristic also covers the third issue, since the entities are isolated.

The proposed approach has presented an efficient solution for some of the issues mentioned. Also, another set of issues is partially addressed by **C**ity **S**ecurity Layer (CSL).

During the development of CSL, as presented in The First International Conference on Advances and Trends in Software Engineering in Barcelona – Spain, the need for a service manager to manage connected services was raised. The next section describes the specification and definition of that component.

V. SERVICE MANAGER

After having understood the CSL, it is seen that there is a demand for the Service Manager module. The module is integrated above the security solution by orchestrating the management of services. This section will detail the module by describing its architecture and its functionalities.

A. Motivation

The Service Manager is a module for managing and controlling services that are present in a smart city. This module is characterized as a plug-in which, when added to the CSL, will be responsible for controlling its services.

The need to have the service manager arises because the CSL need to know all the services that can communicate with each other in a smart city. The need for registering services is met by obtaining and filling in the CSL hash table so that organizations know who is available for them to communicate with.

Figure 1 shows two levels of security depth where the CSL and Service Manager are present.

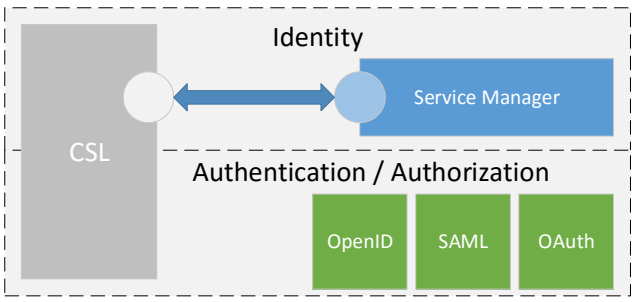

Figure 1. Summary of the ideal security environment

OAuth, SAML and OpenID appear as similar solutions that are on the same level of security of the CSL. After the two levels of security, there are network protocols that helped complement the solution.

B. API

The API provided by the Service Manager consists of the entry points provided by the CSL. These are:

Registration of Services: This allows the insertion of services that are part of the interoperable systems and solutions of a city. For registration, the service information that needs to be sent includes: name, description, public identifier and the URL address. On entering the service, negotiable validations are made to avoid replication of the same services and mandatory data. If the registration of the service satisfies the validation, the service is registered and returned to whoever requested the registration.

Alterations of Services: Editing information of the registered services. The alteration is carried out with validations to avoid the inconsistency in the data of the service. This precaution is taken because some data of the service comprise the Table of identifiers that the CSL uses to route information to the services.

Removal of Services: Exclusion of services that do not take part in the environment of the city. This is only authorized if the service has not taken part in any interaction in the city, otherwise it should be disabled.

Listing of Services: Listing the information that make up the services, such as: name, description, address of the service and public id. The service assembles a dynamic table of the services apt to play a part in an interaction in the city.

Loading of Services: The function guarantees the possibility of migrations of the services from a city to the CSL. To load the services, a file in text format will be requested, in which a standard must be respected: {name, description, public id, URL address}, {name, description, public id, URL} ... When the file is loaded, the services present in it will be inserted if they respect the inclusion rules.

Address Resolver: This provides the URL address of the service being requested to in order to send on the piece of data of whoever asked for it to the party requested.

C. Look and Feel

Figure 2 shows the main screen responsible for maintenance services. On this screen, the user can manage each service used by the CSL.

Figure 2. Main screen maintenance services

Figure 3 presents the screen related to editing a registered service.

Figure 3. Editing registered Services

These two screens refer to the core parts of service management. They also they play an important role in the general functionality of CSL.

 ISBN: 978-1-61208-438-1

D. The Workflow of Service Manager

The workflow between CSL and the Service Manager is described in Figure 2:

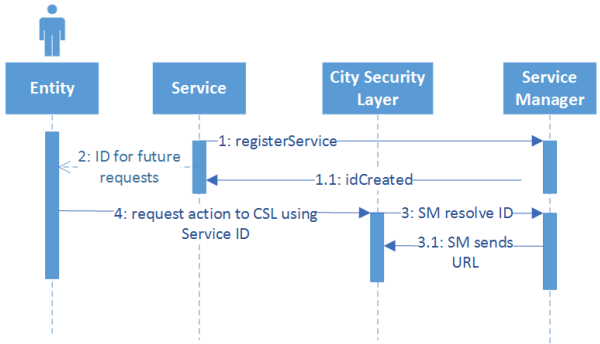

Figure 4. Sequence diagram with the workflow between CSL and Service Manager

Description:

1. A service is registered on Service Manager;
1.1. The Service Manager returns the identifier to the new service;
2. This identifier will be used for future requisitions;
3. CSL, by using the identifier of the required service, makes requests to the Service Manager at the URL for this service.
4. The entity will keep on requesting service information by sending messages through CSL.

E. Technologies Used

The programming language in which the solution was structured was Java. The choice was based on the fact that the CSL was originally built with it, thus facilitating its integration and because it has a large number of communities which aim to facilitate development work by constructing frameworks [21].

In the presentation layer of the Service Manager, Java Server Faces (JSF) version 2.2 was used. JSF is a technology which permits Java for Web applications to be created using ready-made visual components so that the developer only has to be concerned about its use [22]. Together with the JSF, Primefaces was adopted. According to [23], this extension of the JSF stands out due to its simplicity, performance and template options.

The other technologies used in the CSL were not altered so that the solution of the manager does not have an impact on the existing security layer. For transactional control, the CLS uses the Spring framework [24] which besides assisting communication with the other layers aims to remove the dependencies between entities with the injection of dependency. In the data layer, use is made of the JPA framework [25] which will orchestrate the transactions with the database and avoid code repetition when dealing with the persistence of data. The view of the layers can be seen below in Figure 5.

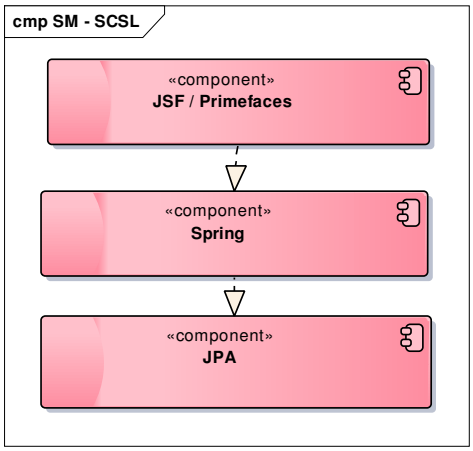

Figure 5. Technologies used

The Java programming language contributed to the creation of a modular environment and with independent layers, whereby one layer provides a service to the one above it. The CSL provides basic services to the Service Manager, and delegates responsibility for validation, treatment and manipulation of services.

The JSF helped in dealing with requests for communication with the service layer of the CSL and dealing with events. Primefaces was used to provide graphical interface components, such as templates, buttons, and dynamic tables.

VI. VALIDATION

The validation process will evaluate the Service Manager incorporated into the CSL. To do so, it will count the time spent on including, excluding, and requesting services on CSL, with and without using this management module. By using this measure, a stress test will be exclusively used to validate performance.

A. The infrastructure for measurement

The validation environment was executed on an Intel Core I5 computer, with 8GB memory RAM, which uses the Windows 8 operating system.

B. Unity and count tool

The unit of measurement was milliseconds (ms). To draw up the validation test for inclusions in, exclusions from and requests to the CSL, the JMeter tool was used, which is a free, open source tool by the Apache Foundation and used to test the performance of software applications.

The metrics defined is a time-count of conducting 1000 samples of including, excluding, and consulting services. This activity will consider the presence, or absence, of the Service Manager, and will record a comparison of time-counts before and after using the manager in the CSL solution.

 ISBN: 978-1-61208-438-1

C. Results and Analysis

The results obtained after applying the metrics of the previous topic are shown in Tables II and III.

TABLE II. VALIDATION RESULT

Operation	Median	
	With Service Manager	without Service Manager
Include	4.000	3.850
Remove	2.9000	2.500
Query	3.800	3.600

TABLE III. VALIDATION RESULT IN PERCENTAGE

Operation	Percentage Increase
Include	3.75 %
Remove	13.79%
Query	5.26%

As seen in the above tables, the addition of the Service Manager, even when there is an interface and control layer did not cause a significant increase in the basic operations of addition, deletion and consultation of services.

VII. CONCLUSION

Cities grow constantly. This is caused by people migrating to urban areas, or the growth of their own populations. This growth is forcing cities to organize themselves better and continuously, since people are demanding even more resources and consuming even more services. It is also obliging cities to invest in information technologies, and to start to become smarter. The new technologies are helping cities to obtain faster results and to attend to the demands of their citizens.

By using these technologies, cities are starting to be called smart cities. Nevertheless, this new technological scenario has led to such cities having to face a set of fragilities. For example, since the services that cities provide are extremely vital, and some of these may require data to remain confidential, the new focus is now on security in the smart city.

Nowadays, there is a set of solutions that partially covers these fragilities, as seen in this study, namely OAuth, SAML and OpenID. Even though these solutions are focused on authentication and authorization, throughout this article, it was demonstrated that the issue of identity control in the smart city has not been adequately addressed. It was as a solution for this identity issue that CSL was conceived as a layer that would be responsible for ensuring anonymous communication between entities and services, thereby covering some of the security problems of smart cities.

As a way of complementing CSL, this article puts forward a structure for creating a service manager. As demonstrated, CSL needs to know all the services that will be available for communication purposes in a smart city, since CSL needs to maintain a table of identifiers.

Because of these needs, a service management module was developed for CSL. To validate this module, a scenario was built in which to test the performance of including, listing, excluding services and requesting these services, with and without this new module.

On analyzing the results, it was shown that adding a new module to compare the time spent on each type of operation leads to barely increasing the time spent on management, thus showing this new module when plugged in to CSL is viable.

For future studies, more research on CSL will be needed as CSL evolves, since its current scope only contemplates a small set of security concerns. In addition, a future study should contemplate using CSL with the service manager module in a more complex smart city, to enable further validations and metrics.

REFERENCES

[1] T. Nam and T. A. Pardo, “Conceptualizing smart city with dimensions of technology, people, and institutions,” Proc. 12th Annu. Int. Digit. Gov. Res. Conf. Digit. Gov. Innov. Challenging Times - dg.o ’11, 2011, p. 282.

[2] S. Dirks and M. Keeling, “A vision of smarter cities: How cities can lead the way into a prosperous and sustainable future,” IBM Inst. Bus. Value. June, 2009.

[3] F. Duarte, “Smart Cities: technological innovation in urban areas”, São Paulo em Perspect., vol. 19, 2005, pp. 122–131.

[4] J. Shapiro, “Smart cities: quality of life, productivity, and the growth effects of human capital,” Rev. Econ. Stat., vol. v88(2,May), 2006, pp. 324–335.

[5] M. Sen, A. Dutt, S. Agarwal, and A. Nath, “Issues of Privacy and Security in the Role of Software in Smart Cities,” 2013 Int. Conf. Commun. Syst. Netw. Technol., 2013, pp. 518–523.

[6] Global Electronics Industry, “The IBM vision of a smarter home enabled by cloud technology,” 2010, p. 16.

[7] F. Ferraz, C. Sampaio, and C. Ferraz, “Towards a Smart City Security Model Exploring Smart Cities Elements Based on Nowadays Solutions,” ICSEA 2013, 2013, pp. 546–550.

[8] A. Bartoli, M. Soriano, J. Hernandez-Serrano, M. Dohler, A. Kountouris, D. Barthel, Security and Privacy in your Smart City , in Proceedings of Barcelona Smart Cities Congress 2011, 29-2 December 2011, Barcelona (Spain).

[9] D. Washburn, U. Sindhu, and S. Balaouras, “Helping CIOs Understand ‘Smart City’ Initiatives,” Forrester, 2009.

[10] R. M. Kanter and S. S. Litow, “Informed and Interconnected : A Manifesto for Smarter Cities Informed and Interconnected : A Manifesto for Smarter Cities,” Working Paper 09-141, Havard Business School, 2009.

[11] I. Verbauwhede, “Efficient and secure hardware, for cryptographic algorithms on embedded devices,” 2012, pp. 1–4.

[12] C. Bodei, P. Degano, and G. L. Ferrari, “Formalising security in ubiquitous and cloud scenarios,” In Proc. 11th IFIP TC 8 International Conference on Computer Information Systems and Industrial Management, 2012, pp. 1-29.

[13] F. S. Ferraz and C. A. G. Ferraz, “More Than Meets the Eye In Smart City Information Security: Exploring security issues far beyond privacy concerns,” in IEEE computer science, UFirst-UIC 2014, 2014, pp. 677-685.

[14] F. S. Ferraz and C. A. G. Ferraz, “Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment,” in 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 842–847.

 ISBN: 978-1-61208-438-1

[15] W. Li, J. Chao, and Z. Ping, “Security Structure Study of City Management Platform Based on Cloud Computing under the Conception of Smart City,” 2012 Fourth Int. Conf. Multimed. Inf. Netw. Secur., 2013, pp. 91–94.

[16] F. J. L. Ribeiro, J. C. R. Lopes, and A. C. P. Pedroza, “Analysis of security processes in mobile third generation systems,” I Escola Regional de Redes de Computadores, Porto Alegre, Brazil, September 2003.

[17] F. S. Ferraz, C. Candido, B. Sampaio, C. André, and G. Ferraz, “Information Security in Smart Cities Using OpenID , SAML and OAuth to increase security in urban environment,” SOFTENG 2015 First Int. Conf. Adv. Trends Softw. Eng., 2015, pp. 7–13.

[18] F. Yang and S. Manoharan, “A security analysis of the OAuth protocol,” IEEE Pacific RIM Conf. Commun. Comput. Signal Process. - Proc., 2013, pp. 271–276.

[19] S. Saklikar, S. Saklikar, S. Saha, and S. Saha, “Next steps for security assertion markup language (saml),” Proc. 2007 ACM Work. Secur. web Serv., 2007, p. 65.

[20] F. S. Ferraz, C. Candido, B. Sampaio, C. André, and G. Ferraz, “Towards A Smart-City Security Architecture Proposal and Analysis of Impact of Major Smart-City Security Issues,” SOFTENG 2015 First Int. Conf. Adv. Trends Softw. Eng., 2015, pp. 108–114.

[21] “Java.” [Online]. Available: https://java.com/pt_BR/about/whatis_java.jsp. [Accessed: 20-Oct-2015].

[22] “JavaServer Faces.” [Online]. Available: http://docs.oracle.com/javaee/5/tutorial/doc/bnaph.html. [Accessed: 28-Oct-2015].

[23] “Primafaces.” [Online]. Available: http://www.primefaces.org/whyprimefaces. [Accessed: 28-Oct-2015].

[24] “Spring Framework.” [Online]. Available: http://projects.spring.io/spring-framework/. [Accessed: 02-Mar-2015].

[25] “JPA - Java Persistence API.” [Online]. Available: http://www.oracle.com/technetwork/java/javaee/tech/persistence-jsp-. [Accessed: 30-Apr-2015].

 ISBN: 978-1-61208-438-1