Towards A Smart-City Security Architecture

Proposal and Analysis of Impact of Major Smart-City Security Issues

Felipe Silva Ferraz[1,2],Carlos Candido Barros Sampaio[1,2], Carlos André Guimarães Ferraz[1]

[1]Informatics Center
Federal University of Pernambuco
Recife, Brazil
{fsf3, ccbs, cagf }@cin.ufpe.br

[2]CESAR
Recife Center for Advanced Studies and Systems
Recife, Brazil
{fsf, ccbs }@cesar.org.br

Abstract—**Concepts and solutions related to smart cities have been the focus of related studies and improvements for several years. Part of the motivation to the growing body of research in this field comes from the eminent need for solutions to address the present situation of urban environments. For the first time in human history, more than 50% of the population now live in big cities and not in the countryside. In this matter, computer networks and systems have an important role towards the construction of solutions that enable cities and citizens to maintain a continuous and agile use of those environments. At the same time that new solutions come forth offering readily available, integrated, and reliable information to citizens, new challenges related to information security arise. In this context, this paper explores a set of information security issues in the environment of a smart city and proposes a new approach (City Security Layer) based on the use of different and unique identifiers for each entity (citizen or sensor) involved in the relations of a city to its systems.**

Keywords—security; smart city; architecture; identification

I. INTRODUCTION

Beginning in the early 2000, a major proportion of the human population started to move from small towns to live in big cities [1]; this change in the world's urban structures has led to an unprecedented consumption of natural resources and added an enormous load on city systems [1][2].

To attempt to address this situation, cities have started to put efforts in creating more sustainable and green environments [1][3][4], and to offer its citizens with more and diverse services coming from existing systems of Education, Health, Public Safety, Resources, Government, and Public Transport [5]. To do so, investments in both time and money have been made to increase IoT adoptions to provide the city with more detailed and precise information [6][7][8] and services interoperability, guaranteeing increasing systems evolutions [5][9]. Combined with other definitions, such urban environments that are now extremely connected and highly technological are known as smart cities [10].

Pursuing interoperability in such a heterogeneous environment, new challenges arise, such as performance in the face of enormous amount of generated and transferred data [6][11][12][13]. Another is services availability to assure both citizens and the city with access every time they have a need [14][15][16]. Information security also becomes a concern and how to ensure that sensitive data like a patient's medical records, a driver or vehicle's location or an engineer's structural plan, are dealt with appropriate and expected confidentiality [17][18][19][20].

Information security is an important challenge yet to be properly and fully addressed in the construction of smart cities. At the same time that it is necessary to develop the means to maintain data trafficked by such cities private, integrated, and available upon access, it is also necessary to provide the city systems with ways for the same data to be shared and to be equally protected.

Furthermore, Sen et al. [17] states that there are information security issues related to privacy in the role of a smart city. Thus, it is vital to deal with this situation because the data shared among a smart city environment is as sensitive as the citizen itself, but affirming that privacy issues are the main problem in terms of security would be over simplistic [18][21]. There are other kinds of issues that may pose as a threat to the entire urban system if they are not properly addressed [22][23]. In this scenario, it is vital to develop different architectures, protocols, and other policies that will allow citizens to better manage and access their data [24][25].

Standards such as OpenID [26][27], OAuth [28][29], and SAML [11][30] appear as good choices to provide cities with the means to integrate its services in an environment, with authorization and authentication capabilities. However, their strength relies on offering a unique ID within an environment that is responsible for sharing permission rather than them offering tools to manage individual IDs as separate information.

Rather than just providing an environment with authentication and authorization, it is important to provide citizens with the means to manage their own identity across a heterogeneous system [9][25], without compromise; the environment interoperability and the citizens' privacy and anonymity, ergo identity management, is a key enabler for smart cities' evolution and maintenance.

This paper presents a communication protocol, based on identification management that aims to increase security in smart cities' environment, providing entities (citizens, services, and sensors) with a mechanics to interact with systems using unique IDs for each system. This paper is divided as follows: Section II will briefly introduce the concepts of smart cities, followed by Section III dealing with security analyses on smart cities. Section IV will depict 9 security issues that may affect smart cities' solutions, while Section V will describe the CSL (City Security Layer). Sections VI and VII will end this paper, analyzing the impact of the proposed approach.

II. SMART CITIES

Today's level of urbanization has reached an unprecedented economical and social growth different from other ages; large cities now have the most part of the world's population and an increasing share of the world's most skilled, educated, creative, and entrepreneurial women and men [1]. More than 50% of people on the planet now live in large cities. According to the United Nations, this number will increase to 70% in less than 50 years [1]. This so-called *city growth* or emerging of urban life is driving the city infrastructure into a stress level never before seen as the demand for basic services increases and is exponentially overloaded [5].

Cities are becoming increasingly empowered technologically as their core systems (i.e., Education, Public Safety, Transportation, Energy and Water, Healthcare and Services) are instrumented and interconnected, enabling new ways to deal with massive, parallel, and concurrent usage. In the same pace, new challenges in the field of information security rises and must be properly addressed.

Tracing the genealogy of the word 'smart' in the label 'smart city' can contribute to an understanding of how the term 'smart' is being used in this field. In marketing language, smartness is centered on user perspective. Because of the need for appeal to a broader base of community members, 'smart' serves better than the more elitist term 'intelligent'. Smart is more user-friendly than intelligent, which is limited to having a quick mind and being responsive to feedback. Smart city is required to adapt itself to the user needs and to provide customized interfaces [36]. In the urban planning field, this defines smartness.

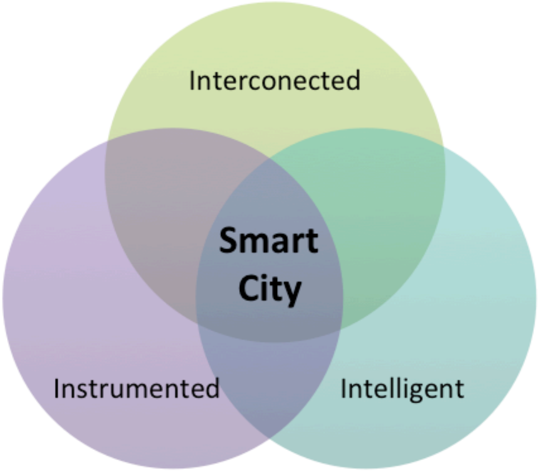

Figure 1. Smart city concept based on intelligence, connection, and instrumentation

Another perspective, represented in Figure 1, points out three main characteristics towards a smart city definition; it is an environment that is instrumented, interconnected, and intelligent [32].

Each one has a meaning:

Instrumented: means a city covered by a set of sensors that could be both physical and social. Through those sensors, the cities' core systems have access to real-time and reliable information. This relates directly with the IoT concepts.

Interconnected: means a vast set of systems working together to offer information from different points and sources. A correct combination of interconnected and instrumented systems creates a connection from the physical world to the real world.

Intelligent: refers to an instrumented and interconnected environment that makes the best use of information obtained from different sensors and systems, to offer a better life to the citizen.

Offering just one or any combination from those three concepts creates a scenario where a vital part will be missing. To illustrate, a system may have the means to extract the best from a set of information, but it does not have data to analyze. A system may also have the data to analyze but does not have ways to pass through other points of the environment its discoveries and information.

However, offering an environment so broadly constructed could have the side effect of creating a different set of scenarios where security information flaws could be created and explored.

III. SMART CITIES' SECURITY ANALYSES

Apart from the number of studies and protocols related to information security, the amount of vulnerabilities in connected applications has increased in the past few years [14]. In this matter, smart-city systems will demand a specific treatment to address its specific information security challenges [18].

According to [5][17][18][19][36], smart-city solutions depend on a high degree of connectivity, so that their systems (such as Education, Government, Traffic, Security, Resources, and Health) can create an interoperable network, offering citizens with more powerful, accurate, and innovative [35] services. For this reason, one of the biggest challenges facing smart-city development is associated to information security in the scope of interoperable systems [1]. Information security is a critical issue due to the increasing potential of cyber attacks and incidents against critical sectors in a smart city.

Information security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the system in unpredictable ways. To protect a smart city in a proper way, a number of security problems have to be faced according to a specific design/plan.

Believing that a traditional security approach based on privacy keeping, authorization, and authentication concept can simply be added into a city's critical infrastructure to make it safer as a city becomes smarter, is far from the real scenario. To deal with new paradigms related to smart cities is necessary to think about in terms of new architectures and not only to improve services and current solutions [36].

This class of services is fundamental to the success of the future city, and represents a topic of such complexity that it is beyond the scope of this paper to cover in detail. As an illustration, let us explore the design of identity services for the future city – which is required to maintain privacy while maintaining security.

The integration of the identity of *the citizen* across multiple systems and services, and the ability to provide a joint-up response to the needs of life events, comprises the goal of allowing the citizen to manage their own identity. This also includes what information is released about them to whom or when, while anonymous, aggregate data are made more widely available [25].

Thus, identity management is a key enabler for future cities. A unified identity system albeit one that can integrate with multiple identity providers and different forms of authentication and identification is needed to handle the extensively 'wired' nature of the city and the density of data transactions, systems, and solutions diversity [25].

Citizens or entities will use their identities to gain access to services and systems, and through benefits that they offer. This is a way to integrate to several solutions (systems and services), entities and service will eventually repeat their identification artifact in different moments and situations.

Ideally, every citizen and/or entity shall have a number of identities, each of which is made up of a number of attributes, which are either exposed, or used to validate a claim without exposing the information. The use of multiple identities limits exposure of truly important credentials, minimizing risk of abuse and identity theft, while allowing for the exposure of less critical information that is helpful for participants in the city ecosystem such as retailers, building operators, service providers, and governments [25].

Not only will citizens be in charge of their identities, but also the information that constitutes them, and when this information could be exposed. The proposed solution is intended to build a trusting relationship between the city, the services/systems, and the citizens. This will allow the acquisition and flow of information that are helpful to all participants without compromising their identity.

IV. Security Issues in the context of a Smart City

Previous studies brought into attention the need to make further improvements related to information security on smart-city environments [5][17][18][19][36]. Based on this need, this section will describe a set of 9 security issues that an urban system and a city may be under the risk of [22][23].

It is important to add to this train of thought that even though the technical solutions applied in those environments handle questions, such as Code Injection [37], Cross Site Scripting [37], Cross Site Request Forgery [37], Buffer Overflow [37], and so on, the issues posted in this work explore concepts related to the nature of a smart-city system. Our approach is to present a set of issues that, regardless of the technical solution applied, may be a threat to urban cities (or a smart-city system) in a different level.

Urban systems are composed by *Citizens* using *Solutions,* which could be *Platforms, Frameworks*, and *Applications*; all of those built on *Technologies* to receive and use *Data*. Urban system security issues or security issues, in brief, in the context of a smart city are situations that can pose as problems to the entire infrastructure of a smart city [22][23].

In the following, 9 security issues will be described; the focus will be the explanation of scenarios and situations that could be a potential threat to an urban environment and its systems.

A. Access to information from applications

According to Sen et al. [17], packet transfer must be studied to apply efforts on adding security to improve data privacy and integrity.

From a network and access perspective, devices have the means to access a packet, or a set of packets, in different ways and locations using different amounts of effort. For instance, to reduce latencies during data transfer, local copies or cache values of those packets could be created, and from there, the mentioned data could be retrieved not only from the network or during a transfer, but also from a local device.

To illustrate further, a sensor connects to a server to identify and authenticate user A and retrieves its permissions. During this process, user B could intercept the packet in different points of the network or of the device, and gain a set of information from user A and the service it is accessing.

B. Information tracking

It is important to have an interoperable and interconnected environment for systems to interact with one another like in [5][11]–[15]. It is also extremely important that, for instance, the information used by system B and that are originally created by system A, cannot be tracked back to its origin. This means that even though system A has provided a set of information to B, a user from system B should not realize that this information is from another part or user.

As an example, let us assume that system A provides information to a solution B.

Let us suppose that A is a system of criminal reports; B is another solution that uses those criminal reports to define the most suitable place to open a new commercial building, based on criminal records. The information used by B, which was provided by A, must not be unveiled or disclosed. This situation could destroy the anonymity in A and compromise, for instance, witnesses and victims of crimes.

C. Citizen tracking

Solutions for smart cities make use of different sensors (physical or social); those sensors are used to collect data from several city systems, and based on this, it is possible for urban systems to have a better city management.

To avoid further problems, such sensors must be under the control of a responsible entity to preserve the integrity of its functionality and generated data.

Among the possible problems raised by this feature is that it may be open or subject to unauthorized citizen tracking, discovery of movement patterns, and may cause 'flooding' of directional advertisement/merchandising.

D. User/Citizen data loss

Smart systems, within the context of smart cities, may use devices, such as smart phones, tablets, and other gadgets to gather a wide range of data and information. Depending on the data type handled by such devices, it is possible to have personal and sensitive data, such as messages, pictures, appointments, bank account numbers, contacts details, and others.

This issues deals with the concept that applications are saving precious data in the device, and if are not well treated, those data could be lost or compromised, creating significant problems to the citizen.

This could be achieved by adding a mechanism related to client cryptographic storage [5], system isolation, and even solutions related to authorization and authentication mechanics.

E. Crossed access to information in data centers

For this scenario, we deal with situations related to unauthorized access to information by exploiting flaws on the server side.

If by any means data security is violated, for instance, while they are under storage, analysis, and management procedures, the entire system may be compromised.

For example, when accessing information related to students' educational systems, a given entity (application) can recover criminal records, from a non-specific connection related to this citizen even though the solution should only be using Educational Services. This situation may occur because both systems share a common area or permissions that must be respected to avoid this kind of behavior.

F. Crossed access at the client side

Description (E), *Crossed access to information in data centers*, details a situation related to unauthorized access in the server side.

Issue (F), in this current topic, brings forth a subject related to unauthorized access at the client side, for instance in a mobile that holds sensitive information.

This is different from issue (D), which is concerned about *every* information saved and that is not properly stored, and is liable to undesired access within the context of a device.

For instance, system A saves in a device values related to paid fees, and system B uses the same mechanism to store information regarding the user financial account. If the device does not provide A and B with the correct isolation, it is possible that through A, an attacker can gain access to values presented in B, and even more, it is possible that a malicious third part system may be installed, and then gain access to both systems information [36].

G. Lack of in-depth security

According to OWASP TOP 10, one of the top-ten risks to web application is related to code injection. Also according to OWASP, sanitizing input values and removing undesired text are measures that can be used to avoid this issue and other security flaws [37].

This flaw, (G), relates to systems that do not validate data in different layers, and are compromised in any level, by data coming from other services.

On the other hand, in-depth security relates to the concept of adding several security measures in different layers of a solution [38].

In an interconnected environment, like in an urban system, if a system C does not provide the entered data with proper sanitization, other solutions that do not use concepts of in-depth security may also be affected.

In other words, if system A provides the user with a rich UI environment, and has several validations and sanitization in this part, if the back-end structure does not apply the same criteria, whenever a system C sends data to system A, system A may use this data. It means that if C has a malicious code inputted, it might be transferred to A once A misses its defense in terms of in-depth security check.

H. Viral effect in urban environment

A smart city uses an interoperable environment to provide solutions with the opportunity to interact with other systems, exchanging data, and creating more value to its citizens[36].

If the border of these relations is not well defined, the systems may face a scenario where a value is changed in system A and when system B uses this changed value, it may corrupt the information used in system B.

For instance, let us assume that this environment is made of a set of systems (named A, B, C… Z), we can foresee a situation where A provides B with an infected value while B may provide or transfer to C, D ... Z systems the same infected value. For an attacker to infect the entire environment, only a small portion of the system needs to be infected and then the contamination may spread throughout the entire system.

In issue (G), our main concern is with the lack of protection in every layer, and how this could be a problem that an urban scenario is highly connected. In the present issue, our concern is with the consequences of issues like issue (G), if the system is highly connected and lacks protections in several parts, the consequences of an attack can be exponentially increased, infecting the entire solution through the infection of a small part.

I. Infection traceability and recovery

The amount of data used and stored by a smart city has reached unprecedented levels. Moreover, the connection between systems has created a system of systems structure that provides those solutions with data coming from different services.

Issue (H) presents a viral threat related to a set of data that can share or provide another service with different data, creating, at some level, a self-sustained system. From that point of view, this issue presents a consequence for issue (I). Due to the amount of data and interconnected system, it is possible for an infection to maintain its origin undetected and beyond data recovery.

Using as an example, system A, with terabytes of data, exchanging values with a System B, that feeds systems C and D with updated and new values, processed from A data. D, on other hand, keeps passing some fine-grained data back to system A. If A suffers an infection having its data compromised, B will be fed with infected data, spreading the infection to other systems, like C and D. As soon as the infection could be detected, recovery processes may not be an option because the amount of data compromised is too big to be restored to a previous form. In addition, due to the relation between systems, the infection source may not be detectable.

V. Smart City Security Layer

OAuth, SAML, and OpenID are architectural solutions focused on identification and assets protection. Those assets could be any type of information or entities such as documents, data, and photos, among others. Through its adoption, it is feasible to create mechanisms in which it is possible to pass the responsibility of security measures to a third party, that could be a known server (Facebook, Google, and others), or to implement the same approach in an in-company solution.

A. Objective

Smart CSL's main objective is to be a layer, where the change of a sent identifier for another identifier is made. The new identifier will be generated from the combination of an ID and the accessed service.

Through that mechanism, it will be possible to make an entity keep its identity secret from a service and unique within the whole environment. This can still be done even though the same entity can access different sets of services, as the creation of the ID is made from the combination of two other identifiers; the resultant ID will be different for the different service coming from the same entity.

B. General view

The City Security Layer (CSL) is a mechanism based on the concept of change identifiers involved in a system relation. The following are the basic components and flow of CSL.

Entity: which is a component that is requesting information to a service; an Entity can be anything from a citizen, to a sensor or a service that is interoperating with another one.

Service: represents any service contacted from an entity.

Communication Layer: represents a contact point from entity to service, responsible for changing the identifier sent by the entity into the correct ID to be used within the service.

ID Service: is a component responsible for storing and managing information to generate the correct ID.

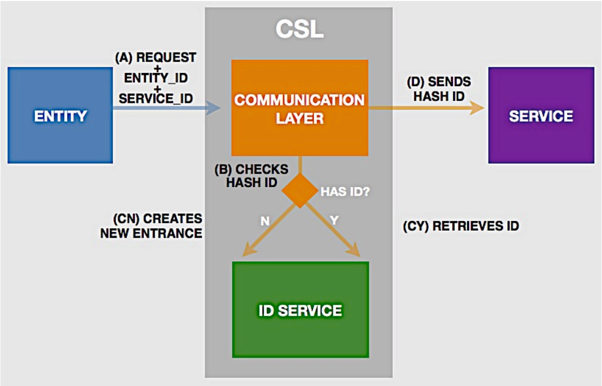

Figure 2. CSL basic flow.

C. Comparing with related works

CSL's main strengths rely on the fact that for each entity using a specific service, a unique and new ID will be presented to the service. For each system adopting this approach, the identifier sent by the layer will be interpreted as a real individual, protecting the real user through the protection of its real ID. On other hand, CSL presents no other feature, like OAuth, SAML, and OpenID, related to authentication and authorization.

Finally, CSL has presented an interesting contribution mostly due to the fact that it only relies on ID changing and management, providing the environment with means to use different IDs. However, it is also important to use an extra layer or process to take care of authorization and authentication under the scenario of an urban environment.

VI. Analyses of Issues

Analyzing through this scope, Table 1 shows a compilation of CSL impacts when compared against the 9 issues previously studied.

TABLE I. CSL Coverage

ISSUES	COVERAGE
1. Access to information from applications	✓
2. Information Tracking	✓
3. Citizen Tracking	✓
4. User/Citizen data loss	×
5. Crossed access to information in data centers	✓
6. Crossed access in client side	×
7. Lack of Security in Depth	✓
8. Viral effect in urban environment	×/✓
9. Infection traceability and recovery	✓

A. Access to information from applications

Assuming the behavior that each packet will be sent through the net with different user IDs per system, even though an 'eavesdropper' can capture many of those packets, this issue will be addressed; hence, the amount of senders will now be considerably bigger, making it even harder try to understand who is who.

B. Information tracking

For issue (B), the same toughness to identify each user will isolate information, at the same pace, it will also influence issue (C), isolating also the citizen, because information about the entity will be protected, as a consequence, the entity will also be untraceable.

C. Citizen tracking

Through the adoption of CSL, information will be hard to track; ergo, the citizen will also be hard to track because their data will be hard to track.

D. User/Citizen data loss

As mentioned in OAuth, OpenID, and SAML section, the main strength in the three standards relies on interoperability and authentication, and for that issue, they do not impact (D). The same way goes to CSL, its concept proposes to change the way identifiers are sent and used by systems; therefore, this issue is not impacted by CSL.

E. Crossed access to information in data centers

Issue (E) is addressed by CSL from the point of view that even though an attacker can compromise a system, and gather information about citizen A and also access other systems, this attacker will have the perception that the systems databases are composed only of different entities, but in practice, for each system/service, an entity will be presented differently.

F. Crossed access in client side

The consequence behind these issues is directly related to an application A accessing information from application B in the client side, without the authorization to do so. In CSL, this has no impact because identifier changes are made not at the client side.

G. Lack of in-depth security

CSL adoption will add an extra layer, responsible for creating and maintaining different IDs for different users. If citizens are to access a service, their IDs will pass for an adaptation to retrieve the real ID. Even if the requesting party is a service, retrieving information about a specific entity, it will also be submitted to CSL approaches, enhancing security in the environment as a single piece.

H. Viral effect in urban environment

The basic idea from issue (G) applies to issue (H); it will be more difficult to explore breaches due to the existence of an extra layer, but, issue (H) deals with a further consequence, which is the creation of a viral effect. This effect could be produced in different forms and with different types of data, not only a citizen ID, and that said, issue (G) is only partially addressed.

I. Infection traceability and recovery

The adoption of CSL will increase security, mostly because it will add an extra security layer that will provide the city systems with the means to keep its entities and citizens using different IDs for different services. As a consequence, this will promote systems isolation.

Even though they are isolated, they are not disconnected, that said, issues (G) and (I) are addressed completely by the CSL proposal. Issue (G) was presented with an extra layer; for issue (I), better traceability of the origins of an infection will be possible.

VII. Conclusion and Future Work

For the first time in human history, humanity is facing a unique situation where more than 50% of the population now live in big cities. For that to work out, there is an urgent need to evolve information technology systems to solutions that provide citizens with more and detailed information about different subjects of their daily use.

At the same time that new solutions rise, new challenges also develop, and among those, information security plays an important role, and not only due to citizens' privacy issues, as it is a subject that may go beyond citizens and impact entire systems.

Solutions like OpenID, SAML, and OAuth play an important part in guaranteeing user security and single sign on. Unfortunately, lay all expectations in one of those 3 standards may not address and solve all problems. In this scenario, this paper proposed the creation of an architectural solution, called city security layer, an architecture based on a cryptography that proposes the creation of different and unique IDs for each system relating to each citizen. This way, it is possible to address more security issues than with the 3 mentioned standards.

CSL still needs further studies and evolutions to be considered as a final solution. In this matter, the next steps for this project are to develop an environment to better validate the proposed approach, and conduct some stress and performance tests to CSL implementation to guarantee its reliability and applicability.

References

[1] 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.

[2] IBM. Ibm smarter healthcare. http://ibm.co/bCJpHX, 2012. "[Online] Available: 19-March-2015".

[3] C. G. Kirwan, "Urban Media : A Design Process for the Development of Sustainable Applications for Ubiquitous Computing for Livable Cities," pp. 7–10.

[4] P. Jollivet, "Crowd sourced security, trust & cooperation for learning digital megacities: valuing social intangible assets for competitive advantage and harmonious development," *IET Int. Conf. Smart Sustain. City (ICSSC 2011)*, pp. 52–55, 2011.

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

[6] R. van Kranenburg and A. Bassi, "IoT Challenges," *Commun. Mob. Comput.*, vol. 1, no. 1, p. 9, 2012.

[7] M. Chen, "Towards smart city: M2M communications with software agent intelligence," *Multimed. Tools Appl.*, vol. 67, no. 1, pp. 167–178, Feb. 2012.

[8] M. Fazio, M. Paone, A. Puliafito, and M. Villari, "Heterogeneous Sensors Become Homogeneous Things in Smart Cities," *2012 Sixth Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput.*, pp. 775–780, Jul. 2012.

[9] Y. Wang and Y. Zhou, "Cloud architecture based on Near Field Communication in the smart city," in *2012 7th International Conference on Computer Science & Education (ICCSE)*, 2012, no. Iccse, pp. 231–234.

[10] 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*, p. 282, 2011.

[11] T. Tran and C. Wietfeld, "Approaches for optimizing the performance of a mobile SAML-based emergency response system," *2009 13th Enterp. Distrib. Object Comput. Conf. Work.*, pp. 148–156, Sep. 2009.

[12] I. B. M. Global, B. Services, and E. Report, “Smarter cities for smarter growth, How cities can optimize their systems for the talent-based economy.”

[13] Z. Fan, Q. Chen, G. Kalogridis, S. Tan, and D. Kaleshi, “The power of data: Data analytics for M2M and smart grid,” *2012 3rd IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Eur.*, pp. 1–8, Oct. 2012.

[14] J. M. Gonçalves, “Privacy and Information Security in Brazil? Yes, We Have It and We Do It!,” *2010 Seventh Int. Conf. Inf. Technol. New Gener.*, pp. 702–707, 2010.

[15] R. Giaffreda, “Enabling Smart Cities through a Cognitive Management Framework for the Internet of Things,” no. June, pp. 102–111, 2013.

[16] F. Hu, M. Qiu, J. Li, T. Grant, D. Tylor, S. Mccaleb, L. Butler, and R. Hamner, “A Review on Cloud Computing : Design Challenges in Architecture and Security,” pp. 25–55, 2011.

[17] 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.*, pp. 518–523, Apr. 2013.

[18] A. Bartoli, J. Hernández-Serrano, and M. Soriano, “Security and Privacy in your Smart City,” *cttc.cat*, pp. 1–6.

[19] W. M. da Silva, A. Alvaro, G. H. R. P. Tomas, R. a. Afonso, K. L. Dias, and V. C. Garcia, “Smart cities software architectures,” in *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC ’13*, 2013, p. 1722.

[20] Z. Chen, W. Fan, Z. Xiong, P. Zhang, and L. Luo, “Visual data security and management for smart cities,” *Front. Comput. Sci. China*, vol. 4, no. 3, pp. 386–393, Aug. 2010.

[21] S. Report, “Software Security Assurance,” 2007.

[22] 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.

[23] F. S. Ferraz and C. A. G. Ferraz, “Smart City Security Issues: Depicting information security issues in the role of a urban environment,” in *IEEE Cloud Computing Initiative, UCC 2014*, 2014.

[24] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, “Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things,” *2013 19th Int. Conf. Control Syst. Comput. Sci.*, pp. 513–518, May 2013.

[25] L. PlainIT, “Cities in the Cloud, a living planit introduction to future cities technologies.”

[26] A.-V. Anttiroiko, P. Valkama, and S. J. Bailey, “Smart cities in the new service economy: building platforms for smart services,” *Ai Soc.*, Jun. 2013.

[27] M. Noureddine and R. Bashroush, “An authentication model towards cloud federation in the enterprise,” *J. Syst. Softw.*, vol. 86, no. 9, pp. 2269–2275, Sep. 2013.

[28] OAuth, “OAuth 2.0.” [Online]. Available: www.oauth.net.

[29] B. Leiba, “OAuth Web Authorization Protocol” pp. 1–3, 2012.

[30] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Security and Cloud Computing: InterCloud Identity Management Infrastructure,” *2010 19th IEEE Int. Work. Enabling Technol. Infrastructures Collab. Enterp.*, pp. 263–265, 2010.

[31] M. Naphade, G. Banavar, C. Harrison, J. Paraszczak, and R. Morris, “Smarter Cities and Their Innovation Challenges,” *Computer (Long. Beach. Calif).*, vol. 44, no. 6, pp. 32–39, Jun. 2011.

[32] IBM. Ibm smarter healthcare. http://ibm.co/bCJpHX, 2012. ” [Online] Available: 19-March-2015”

[33] C. Balakrishna, “Enabling Technologies for Smart City Services and Applications,” *2012 Sixth Int. Conf. Next Gener. Mob. Appl. Serv. Technol.*, pp. 223–227, Sep. 2012.

[34] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, “Combining Cloud and sensors in a smart city environment,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2012, no. 1, p. 247, 2012.

[35] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, “Smart cities of the future,” *Eur. Phys. J. Spec. Top.* vol. 214, no. 1, pp. 481–518, Dec. 2012.

[36] I. Verbauwhede, “Efficient and secure hardware,” Datenschutz und Datensicherheit - DuD, vol. 36, no. 12, pp. 872–875, Nov. 2012.

[37] OWASP, “OWASP Top 10 - 2013 : The most critical web application security risks,”. https://www.owasp.org/index.php/Top_10_2013-Top_10, 2013 "[Online] Available: 19-March-2015”

[38] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, *Security Patterns : Integrating Security and Systems Engineering (Wiley Software Patterns Series)*. John Wiley & Sons, 2006.