Information Security in Smart Cities

Using OpenID, SAML and OAuth to increase security in urban environment

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
emails: {fsf3, ccbs, cagf }@cin.ufpe.br

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

***Abstract* — As the population living in cities and metropolis grows, the need for the transformation of a city into a Smart City grows, too. The Smart City concept refers to a broad range of definitions and technologies; among those it is possible to identify topics such as Internet of Things, ubiquity, empowering citizens, interoperability of services/systems, green systems, and open data. Whatever is the explored concept, all of them try to reach a single goal, namely, turn the city into a better place to live through the use of Information Technology. In this context, more specifically, interoperable environments play an important role as it provides means to connect different services by creating new systems that are able to provide a bigger variety of information to its users. In this matter, a new range of challenge rises; among those challenges, information security is one of the most important to be discussed. This paper presents a group of security issues that raises a dangerous concern in Smart City solutions, discusses how identity standards, such as OpenID, SAML and OAuth, impact on those issues.**

Keywords — Smart City; Information Security; Security Standards.

I. Introduction

The evolution of cities has been taking a toll both on the environment, as well as on the shape of human population. Its needs have been increasing, and so the pressure on the ecosystem of systems has been constantly escalating.

In the modern world [1], sustainability is a major issue; if we keep on exploiting resources and services without any thought about the following generations, the future of human race may no longer have enough resources to survive. But also, industrial development is as important as environmental issues; safety is as important as saving time; continuous availability of resources is as important as not exploiting them, and so on [2]–[4].

To match this kind of situation, the citizens of major cities around the world must become more informed, responsible and efficient, in order to gain and provide faster and more continuous access to information [3][5][6]. Every structure, whether its intended use relates to resources, health, government, transportation, education, or public safety systems was designed, built and maintained with advanced, integrated materials, sensors, electronics, and networks to provide those citizens with the means to attend those needs [7]–[9].

In this area, new solutions are absolutely necessary not only to improve the quality of daily-life with innovative, sustainable, long term and efficient protocols but also in terms of security/reliability. Security and/or reliability are important paths mostly because the solutions will be exposed to an extensive range of attacks. Internal and external parties are not trusted, and privacy, integrity and availability will be a vital prerequisite for the approval of the citizens. In addition to it, since the assumptions and requirements for smart critical infrastructures are very different, implying that networks for smart cities should be engineered quite differently, it also raises a problem of integration or interoperability [10].

With cities progressing towards smarter societies, worldwide Information and Communication Technologies (ICT), a class of software is also advancing and ushering itself to the IT sector, nowadays, called ‘green software’ or ‘smart software’ [11]. The primary role of a smart software is to enable the functioning of the devices, running them in such a way that the device is eco-friendly and aids the smart behavior of a city [9][12]. For a smart software to increase the functioning and sustainability of a Smart City as a whole, the devices with smart software must contribute to the entire system. As software systems are vulnerable to threats, the Smart City should be prepared for such attacks and breaches of security [11].

Web-based protocols, for instance, protocols as OAuth [13], Security Assertion Markup Language (SAML) [14], and OpenID [15], play an important role in web and cloud platforms [16]. They present means to guarantee access to specific services in order to provide authorized access to its private data to the users. Furthermore, they present a major contribution to single signing needs.

This paper presents an analysis on 9 security issues proposed in previous works [14][15], facing three different security standards. This paper is divided as follows: after a brief Introduction, Section II will introduce the concepts of Smart Cities, followed by Section III dealing with security analysis on smart cities; Section IV will depict 9 security issues in the role of smart cities solutions. Section V will explore differences and strengths on OpenID, SAML and OAuth. Finally, Sections VI and VII will finish this paper analyzing the impact of the mentioned standards and presenting some conclusions, respectively.

II. Smart Cities

A long and exhausting talk has been taking part in research areas – solutions of Smart Cities, studies and implementation play an important role in solving a visible problem. How to deal with the unprecedented level of citizens living in cities? Differently from other ages, large cities have now most part of the world population and an increasingly share of the world's most skilled, educated, talented, creative and entrepreneurial personalities. For the first time in human history, more than 50 percent of the population of the world now lives in large cities, and what is more alarming is that, according to the United Nations, this number will increase to 70 percent in less than 50 fifty years [19]. This *city growth* or emerging of urban life is taking the city infrastructure to a stress level that has never been seen before, since the demand for basic services increased and are exponentially overloaded [7].

According to a research called *Smarter Cities and Their Innovation Challenges* [20], there is an urgent need for urban scenarios and cities to be smarter in the management of their infrastructure resources and interactions [20]. The urban performance must not rely only on its hardware infrastructure, or the physical concepts of infrastructure, but it must start taking into account the social interactions and a faster deployment of information and services.

Cities are becoming increasingly technologically empowered as their core systems; e.g., 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 rise and must be properly addressed.

III. Smart Cities Security Analysis

Despite the number of studies and protocols related to information security, the amount of vulnerabilities in connected applications has increased in the past few years. In this matter, Smart Cities systems will demand a specific treatment in order to address its specific security challenges information.

According to [9][21]–[23], Smart cities solutions rely on a high degree on connectivity, so that their systems (such as Education, Government, Traffic, Security, Resources and Health) can create an interoperable network, providing more powerful, accurate and unique services to the citizens. For this reason, one of the biggest challenges facing Smart City development is related to Information Security 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 deliberated attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to the user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control the software and alter load conditions to destabilize the system in unpredictable ways. To protect the Smart City in a proper way, a number of security problems have to be faced according to a specific design/plan.

It would be too simplistic, and probably a lapse, to believe that traditional security approach based only on privacy and authorization concepts can simply be added into a critical infrastructure of a city to make it safer as much as it becomes smarter. New architectures are necessary not only to improve the security services, but the interoperability and the security in general.

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 details. 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 joined-up response to life events needs, comprises the goal of allowing the citizens to manage their own identity and what information is released about them to who or when, while anonymous, aggregate data is made more widely available.

So, Identity Management is an essential key for future cities. A unified identity system, one that can integrate itself 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 diversity of solutions.

Citizens or entities will use their identities to get access to services and systems, and through that the benefits offered by those. This way, to integrate several solutions (systems and services), entities and services will eventually repeat their identification artifact in different moments and situations.

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

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

IV. Security Issues in the role of a Smart City

Based on previous studies [14][15], which brought to attention the need to make further improvements, related to information security on Smart Cities environment, this session will depict a set of 9 Security issues that an urban system and a city may be under the risk of.

It is important to complement that, even though the technical solutions applied in those environments handle with matters, such as Code Injection [24], Cross Site

Scripting [24], Cross Site Request Forgery [24] and Buffer Overflow [24], and others, the issues presented in this work explore concepts related to the nature of a Smart City system. Our proposal 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.

Figure 1 presents an overview of this difference.

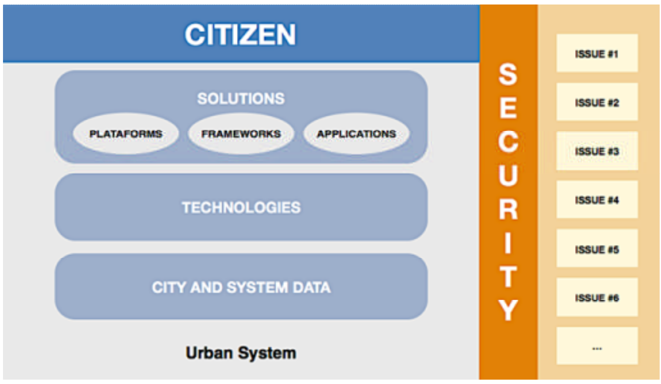


Figure 1. Security issues overview

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 the role of a Smart City are situations that can be put as problems to the infrastructure as a whole.

In the following section, those issues will be depicted, in order to illustrate the impact on OAuth [13], Security SAML [14], and OpenID [15].

A. *Access to information from applications*

According to Sen et al. [25], packet transfer must be addressed, in order to apply efforts to add security improving data privacy and integrity. Looking from a network and access perspective, devices have the meanings to access a packet, or a set of packets, in different ways and locations and with different efforts. For instance, to reduce latencies during data transfer, local copies or cache values of those packets could be created.

Let us assume that a sensor connects to a server to identify and authenticate user A and retrieves its permissions. During this process, a 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, as 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; it 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.

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

Let us supposed 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. This situation could destroy the anonymity in A and compromise witnesses and citizens victims of crimes, for example.

C. *Citizen Tracking*

Solutions for smart cities use 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.

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

Among the possible problems raised by this topic, it can be appropriate: Unauthorized citizen tracking, discovery of movement patterns and flood of directional advertisement/ merchandising.

D. *User/Citizen data loss*

This issue 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 mechanisms related to client cryptographic storage [7][22], system isolation and even solutions related to authorization and authentication mechanisms.

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.

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 since both systems share a common area or permissions that must be respected in order to avoid this kind of behavior.

F. *Crossed access in client side*

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

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

Different from issue #D, which the concern is about *every* information saved and that are NOT properly stored, and liable to undesired access within the context of a device.

If, 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 gains access to values presented in B, and even more, it is possible that a malicious third part system may be installed and, then, gains access to both systems information [28].

G. *Lack of Security in Depth*

According to OWASP TOP 10, one of the Top Ten risks to WEB application is related to code injection. Also according to OWASP, sanitize inputted values and remove undesired texts is one of the measures to avoid that and other security flaws [24].

This flaw, #G, is related to systems that do not validate data in different layers, and are compromised in any level, by data originated from other services.

In other words, if system A provides a rich UI environment to the user 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 defense in depth concepts.

H. *Viral effect in urban environment*

A Smart City uses an interoperable environment to provide solutions with the opportunity to interact with other system, exchanging data and creating more value to its citizens [2].

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.

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 the 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 since 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. Exploring OAuth, SAML and OpenID

To address some issues mentioned on the previous section, identification management will play an important role [28]; therefore, this section will present architectural solutions that addresses security issues, specially related to identification, authorization and authentication across an interoperable environment. This section will depict three different approaches that offer a set of functionalities that could aid mitigating previous issues.

According to approaches related to, or making use of, OAuth 2.0 [27][28], SAML [29][30] and OpenID [31][32], it appears as the bigger responsible for security assurance in interoperable environments. For this reason, OAuth, SAML and OpenID will be depicted in the following section, and compared with the mentioned issues in order to understand if there are positive impacts on a Smart City environment.

A. *OAuth*

Open Authorization (OAuth) is an authentication standard used by service providers to store protected resources in a way that a resource owner do not have to hand out their credentials to gain access to the protected assets. It means that through OAuth is possible to authorize another website, with access to the user information stored within another service provider, without the need to share their access permissions.

The basic structure of OAuth is composed by a Resource Owner, that is an entity responsible for storing protected assets and is capable of granting access to the assets under its control, an Authorization Server is responsible for handling authentication and authorization of different entities involved and a Resource Server that is a server that hosts the client asset [27][28][33].

Figure 2 shows the basic flow of an OAuth structure:

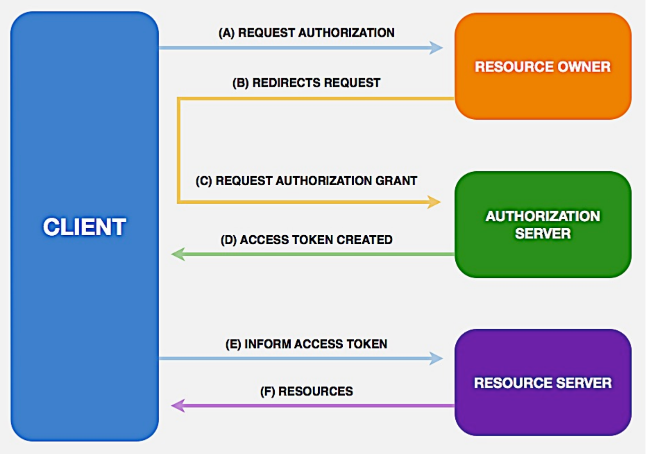


Figure 2. OAuth basic flow

(A) In the first step, a **client** requests an authorization from the **resource owner**.

(B) The **resource owner**, replies to the **client** and redirects the request to **authorization server**.
(C) The **client** requests an authorization grant from the **authorization server** by presenting the client credentials.
(D) The **authorization server** validates the **client** credentials and the authorization grant, and if valid issues an access token.
(E) The **client** requests the protected resource from the **resource server** and authenticates by presenting the access token.
(F) The resource server validates the access token, and if valid, serves the request.

B. SAML

Security Assertion Markup Language (SAML) defines an XML based framework used to describe and exchange information related to security between secure web-based entities [1][34]–[37].

SAML is a reference standard that implements identity provider that has the capability to address several security scenarios and technologies. The main strength of a SAML based system is that it can create a trust relationship using entities that relies on different security mechanism. Different from other security systems SAML approach is to express assertions about an entity that other application within the same network or environment can trust

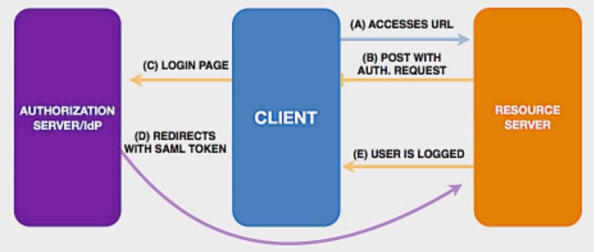


Figure 3. SAML basic flow

(A) A **client** tries to access an asset in **resource server**.
(B) The **resource server**, redirects the request to the **authorization server**.
(C) The **client** informs login and password.
(D) Once the authentication is made, the **authorization server** redirects the SAML token to the **resource server**.
(E) The asset access is granted to the **client**.

C. OpenID

OpenID is a distributed open standard technology, used to identify users with URL typed ID. Any type of system can use an OpenID protocol without any kind of fee.

The final user also does not need to depend on a specific site or domain to keep their ID controlled. It means that they do not need to enter any of its personal information such as email, name, address or other identifiers to have an ID and password for every site, instead all that is necessary is to lot in using their OpenID in a site that adopts and OpenID system [21]. Due to this property, a user do not need to have a separate ID and Password for each site further OpenID creates the effect of a outsourced user authentication service.

OpenID basic flow is composed of a Client, which represents and entity using the OpenID system, Relying Party (RP) that is the service provider and the OpenID Provider that holds the logic related to IDs and Passwords [29][38], as presented in Figure 3.

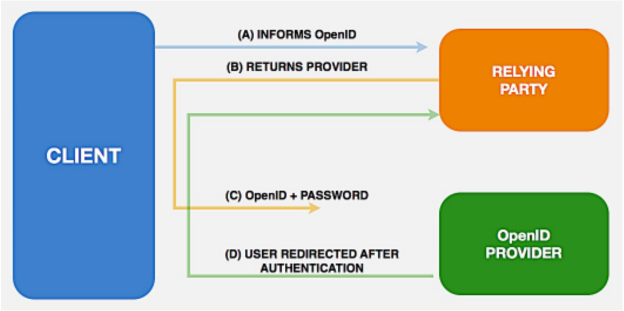


Figure 4. OpenID basic flow

(A) The client informs the OpenID to a **RP**.
(B) The **RP** normalizes the clients OpenID, identify the OpenID and redirects it to the client.
(C) The **client** informs credentials for the ID.
(D) After authentication, access is granted.

VI. TOWARDS ISSUES ANALYSIS

In this section, the impact of OAuth, SAML and OpenID, under the vision of the security issues mentioned in Section III, will be analyzed.

The three-depicted protocols have a direct relation with both creation and maintenance of identifiers and with authorization and authentication in an interoperable environment.

A. Access to information from applications

Once the token is generated, and somehow stored within the client, only the OpenID presents means to avoid this threat, due to its characteristic of asking for a password once the ID is presented. This way even if the ID is compromised, the attacker needs to have extra security information about the ID. OAuth and SAML, on the other hand, it does not request other verification after the token is created.

B. Information Tracking

This issue is related to the concept of an information source not being able to be discovered. About this idea, the three mentioned protocols have no ways to avoid the issue if the correct authorization attribution is not made. In other words, the protocol can address the problem, but if not well used, or by any human misconfiguration it can still be explored.

C. *Citizen tracking*

Considering that the token generated by OAuth and SAML are compromised, it is possible to track information from different systems. To both mentioned protocols, even if it is possible to explore the flaw, it also is unlikely that every system used by the citizen could be reachable by the same token. In OpenID relies the trust that, even though the ID is compromised, the user needs to achieve also the password of the citizen.

D. *User/Citizen data loss*

Since the main focus of the studied protocols are related to the interoperability of systems, it has no direct relation with protection regarding the client side. That way OAuth, OpenID and SAML are marked with no positive impacts with issue number #4.

E. *Crossed access to information in data centers*

Similar to issue number #2, this issue is partially addressed by OpenID, SAML and OAuth, because they have the strengths to solve this kind of scenario, but due to incorrect use of the protocols or by human mistakes, when adding the permissions and authorizations, data could be compromised even in the server side.

F. *Crossed access in client side*

Similar to issue #4, issue #6 deals with the concept of client side been compromised, the difference in this case is about the notion that a data in application A could be wrongly accessed from another application B, causing data leakage from one app to another, whereas for issue #4 it is related to data loss on the client side by any other means, for example, week client storage. The same explanation for issue #4 is applied for #6 and the three protocols have no impact on this scenario.

G. *Lack of Security in Depth*

As previously mentioned, Security in Depth is a concept that suggests adding several layers of protection within a system scope. OAuth, SAML and OpenID, deals with the concept of providing few tokens to every user making it simpler to log and gain access to the proper asset. Due to that fact it is feasible to realize that the three protocols make the use of a set of services easier, but lose some security by repeating the same checks for different services.

H. *Viral effect in urban environment*

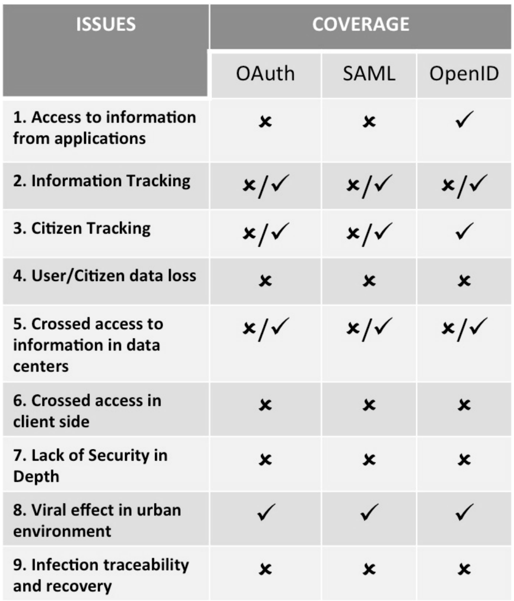
Issue #8 is potentially solved by the three protocols since they present means to avoid actions coming from unauthorized parts. Even though they are susceptible to human flaws, it is still highly unlikely that for every system using the protocols, they present bad settings or operational flaws.

I. *Infection traceability and recovery*

Finally, issue number #9 deals with the idea that if some point of a broad system is compromised, it is improbable to identify where the infection or the flaw was first initialized and also to recover the state of the system to a previous version. Since OAuth, SAML and OpenID, deal with a single ID for a set of systems, this will make it impossible to track which system the flaw came from.

Table I uses the following subtitle, to summarize the impacts of each one of the three protocols: ✗ for no positive impacts, ✗/✓ partially address the scenario. ✓ directly addresses the situation.

TABLE I. OAuth, SAML AND OpenID IMPACTS AGAINST ISSUES



ISSUES	COVERAGE		
	OAuth	SAML	OpenID
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	✗	✗	✗

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 lives in big cities. To work it out, there is an urgent need to evolve information technology systems to solutions that provide the citizens more and detailed information about different subjects of its daily usage.

At the same time that new solutions rise, new challenges are also developed. Among those, information security plays an important role, and not only due to the privacy issues of the citizens; it is a subject that may go beyond citizens and impact the entire system.

Solutions like OpenID, SAML and OAuth are fundamental to guarantee the safety of the single sign on users. Unfortunately, all the expectations rely on one of those 3 standards and it may not address and solve all the problems. Most of this concern is related to the fact that those standards are under authentication and authorization purposes, which, based on previously described issues are not enough. As a future work, is expected to go deeper in the analyses of the impact of OpenID, SAML and OAuth and to proposes and extension to those technologies to focuses more in smart cities identification management.

References

[1] F. Gil-Castineira, E. Costa-Montenegro, F. Gonzalez-Castano, C. López-Bravo, T. Ojala, and R. Bose, “Experiences inside the Ubiquitous Oulu Smart City,” *Computer (Long. Beach. Calif).*, vol. 44, no. 6, pp. 48–55, Jun. 2011.

[2] 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).

[3] 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.

[4] J. Bélissent and S. Analyst, “What’s new in Smart Cities ?,” pp. 1–20, 2011.

[5] O. Haubensak, “Smart cities and internet of things,” *Bus. Asp. Internet Things, Semin.* pp. 33–39, 2011.

[6] A. Frost, “Moving Citizens in the Smarter City — Using a Framework Approach to Plan Intelligent Transportation Systems Strategies and Implement Solutions.”

[7] 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.

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

[9] 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.

[10] J. Ko, N. Tsiftes, S. Dawson-haggerty, and M. Durvy, “Industry : Beyond Interoperability – Pushing the Performance of Sensor Network IP Stacks,” pp. 1–11.

[11] 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.

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

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

[14] F. Nie, F. Xu, and R. Qi, “SAML-Based Single Sign-On for Legacy System,” no. August, pp. 470–473, 2012.

[15] J.-H. You and M.-S. Jun, “A Mechanism to Prevent RP Phishing in OpenID System,” *2010 IEEE/ACIS 9th Int. Conf. Comput. Inf. Sci.*, pp. 876–880, Aug. 2010.

[16] J. Sendor, Y. Lehmann, G. Serme, and A. Santana de Oliveira, “Platform-level Support for Authorization in Cloud Services with OAuth 2,” *2014 IEEE Int. Conf. Cloud Eng.*, pp. 458–465, Mar. 2014.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, and P. Williams, “Foundations for Smarter Cities,” *IBM J. Res. Dev.*, vol. 54, no. 4, pp. 1–16, Jul. 2010.

[22] 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.

[23] 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.

[24] OWASP, “OWASP Top 10 - 2013 : The the most critical web application security risks,” 2013.

[25] M. Sen, A. Dutt, S. Agarwal, and A. Nath, “Issues of Privacy and Security in the Role of Software in Smart Cities,” in 2013 International Conference on Communication Systems and Network Technologies, 2013, pp. 518–523.

[26] O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal-Meca, and J. H. Ziegeldorf, “Securing the IP-based internet of things with HIP and DTLS,” Proc. sixth ACM Conf. Secur. Priv. Wirel. Mob. networks - WiSec ’13, p. 119, 2013.

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

[28] 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.

[29] M. Noureddine and R. Bashroush, “A provisioning model towards OAuth 2.0 performance optimization,” 2011 IEEE 10th Int. Conf. Cybern. Intell. Syst., pp. 76–80, Sep. 2011.

[30] B. Leiba and H. Technologies, “OAuth Web Authorization Protocol,” pp. 0–3, 2012.

[31] 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.

[32] H. Wang, C. Fan, S. Yang, J. Zou, and X. Zhang, “A New Secure OpenID Authentication Mechanism Using One-Time Password (OTP),” in 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, 2011, pp. 1–4.

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

[34] T. T. A. Dinh, W. Wenqiang, and A. Datta, “City on the Sky: Extending XACML for Flexible, Secure Data Sharing on the Cloud,” J. Grid Comput., vol. 10, no. 1, pp. 151–172, Mar. 2012.

[35] S. Dirks and M. Keeling, “A vision of smarter cities,” IBM Inst. Bus. Value, 2009.

[36] M. Al-Hader, A. Rodzi, A. R. Sharif, and N. Ahmad, “SOA of Smart City Geospatial Management,” 2009 Third UKSim Eur. Symp. Comput. Model. Simul., pp. 6–10, 2009.

[37] A. Aldama-Nalda, H. Chourabi, T. a. Pardo, J. R. Gil-Garcia, S. Mellouli, H. J. Scholl, S. Alawadhi, T. Nam, and S. Walker, “Smart cities and service integration initiatives in North American cities,” Proc. 13th Annu. Int. Conf. Digit. Gov. Res. - dg.o ’12, p. 289, 2012.

[38] 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.