Smart Cities Security Issues: An Impeding Identity Crisis

Felipe Silva Ferraz, Carlos André Guimarães Ferraz, Ademir Gomes

CESAR-Centro de Estudos e Sistemas Avançados do Recife
Recife, Brazil
Email: fsf@cesar.org.br

Informatics Center
Federal University of Pernambuco
Recife, Brazil
Email:{fsf3, cagf}@cin.ufpe.br

Engineering department
Federal Rural University of PE
Recife, Brazil
Email: ademir.ferraz@gmail.com

***Abstract* — Cities have changed the manner in which population is distributed around the globe. Beginning in the 70s, a large number of people began to migrate from the countryside to a metropolis. In such a scenario, it is necessary to build city systems and provide citizens with different methods to interact with these systems. Further, citizens play an important role in building this interoperable environment, and they are required to provide data and information about themselves in order to improve the functioning of the systems. However, citizens do not want their personal and private data to be disseminated in the city. This study explores problems in information security, and, more specifically, those related to identifier and identity management in the context of a smart city environment. This study proposes to address such problems by using an architecture that separates identifiers from data, thus creating a multiple identity infrastructure.**

Keywords- Identity; Security; Smart Cities;

I. INTRODUCTION

The first decade of the 21st century has seen a major change in population distribution in the world. Owing to revolutions in industry and changes in commerce, many people began to migrate from the countryside to big cities [1] [2].

In order to deal with this new scenario in which a majority of the population lives in metropolises, cities are imposing an additional load on their core systems such as the Education, Public Safety, Transportation, Energy and Water, Healthcare, and Government systems [3]. Thus, cities have been created and developed, and citizens have been empowered technologically owing to the increasing number of instrumented and interconnected urban solutions and systems.

To develop this ubiquitous and intelligent ecosystem, several studies are focusing on the concept of a smart city. This concept involves better management of the infrastructure and data of a city [3]. In a smart city, better urban performance must not depend solely on its hardware infrastructure or the physical concepts of infrastructure, but must start taking into account the social interactions, the large amount of generated data, and a faster deployment of information and services to every citizen. The adoption of a smart city solution is becoming increasingly inevitable in order to present entities with an interoperable environment, which is capable of influencing web-based systems in data storage and sharing, and inter-communication among systems and other entities. Henceforth, entities will serve as a reference for various aspects of a smart city system such as citizens, sensors, and services.

Issues related to the development of smart cities into interoperable urban environments pose a fundamental hurdle in solving complex problems of core systems in cities [3]. Further, one of the most critical barriers that prevent mainstream users (or citizens) from adopting the smart cities solution is the uncertainty concerning the safety of their data in the various collaborative systems, which form part of a unified set of systems that address the problems of urban environments.

It is important to provide citizens with the means to manage their own identity across ubiquitous and interoperable systems [4]–[6]. This solution must not compromise the environment solution in any manner and must increase the privacy and anonymity of the citizen. Hence, for citizens, identity management is a key enabler for the evolution and maintenance of smart cities [7][8].

This study enumerates a set of security issues, identity issues in particular, that remain to be addressed from the perspective of a smart city. It also presents a reference architecture based on the management of identifiers. This architecture aims to increase security in the environment of smart cities, and provides entities (citizens, services, and sensors) with a method to interact with systems by using unique IDs for each system. Finally, an analysis of these issues is performed for the proposed architecture.

This manuscript is organized as follows: After a brief introduction, the concepts of smart cities are introduced in Section II. In Section III, security analysis of smart cities is presented. The proposed architecture is described in Section IV. Section V consists of the evaluation of the proposed architecture. In Section VI, the conclusion is presented and future work is discussed.

II. SMART CITIES: AN IDENTITY CRISIS

The current level of urbanization in smart cities has attained an unprecedented economic and social growth; large cities now accommodate a majority of the world population and an increasing percentage of the most skilled, educated, creative, and entrepreneurial men and women in the world [1]. Today, more than 50% of the people on the planet live in large cities. According to the United Nations, this number will increase to 70% in less than 50 years [1]. This city growth or emergence of urban life is leading to unprecedented pressure on the infrastructure of the city owing to an increasing demand for basic services that result in exponential overloading [3].

 ISBN: 978-1-61208-498-5

The smart city concept is based on intelligence, connection, and instrumentation. Another perspective, represented in Fig. 1, demonstrates three main characteristics in a smart city definition; it is an environment that is instrumented, interconnected, and intelligent [7]. A system that has only one or two of the above mentioned three characteristics results in a scenario in which a vital part will be missing.

In spite of various studies and protocols related to information security, the number of vulnerabilities in connected applications has increased during the past few years [9]. Therefore, smart city systems require a distinct approach to address specific information security challenges [10][11].

According to [3][6][12][13], Smart city solutions depend on a high degree of connectivity in order to enable their systems (such as Education, Government, Traffic, Security, Resources, and Health) to create an interoperable network, thus offering citizens more powerful, accurate, and innovative [14] services. Thus, one of the major challenges in smart-city development is related to information security in the scope of interoperable systems [1]. Information security is a critical issue owing to the increasing potential of cyber-attacks and incidents in critical sectors of a smart city.

In addition to deliberate attacks, such as those from disgruntled employees, industrial espionage and terrorists, information security must also address accidental compromises of the information infrastructure owing to user errors, equipment failures, and natural disasters. Vulnerabilities may allow an attacker to penetrate a network, gain access to control software [11][15], and modify load conditions to destabilize the system in an unpredictable manner. In order to protect a smart city effectively, various security problems must be addressed according to a specific design or plan.

The belief that a traditional security approach based on privacy maintenance, authorization, and authentication can simply be added to the critical infrastructure of a city to make it safer as the city becomes smarter does not correspond to the actual scenario [4].

A. Distinct concepts: Identity versus identifier

Identity is not absolute. An identity describes an entity within a specific scope. In our context, an entity could be a citizen, computer, service, sensor, organization, or one of many other actors of a smart city environment.

In formal terms, the identity of an entity, within a scope, is the set of all characteristics attributed to this entity within that scope. For example, one could have an identity related to an educational system that contains information about the educational record, courses taken, and/or grades received; another possible identity could be related to the resource systems of a citizen, and the data stored may include the amount of energy or water consumed in the home of a citizen. Therefore, identities are only valid within a specific field and represent more than simply information that distinguishes one entity from another; they also represent who the entity is, along with its characteristics.

In order to uniquely identify an entity, it is necessary to rely on identifiers and not only on identities. This distinction between identity and identifier is essential, and is not always correctly understood. The confusion is understandable because, in common phrasing, identity is almost synonymous with personal data or information used to identify an entity, which, in turn, is understood to be a unique identifier. Identifiers (such as a user name, sensor identifiers, social number, passport number, serial number, or serial ID) are also valid and guaranteed to be unique only within a scope.

Thus, instead of considering an entity with a single identifier to represent a single identity across different systems, it is more natural to view an entity as a collection of multiple identifiers (a set of sets), each with its own scope, that can represent different identities of the same entity because the entity is identified differently within different possibilities. Note that this concept is aligned with the idea that privacy ensures that information about a person does not leak from one scope to another.

The goal of permitting citizens to manage their own identities encompasses the integration of the identity of a citizen across multiple systems and services and the ability to provide a joint response to the needs arising from daily events. This goal also includes the ability to control the type of information about the citizen that is released to a particular system or at a particular time; however, anonymously aggregated data are made more widely available [6].

Thus, identity management is a key enabler for future cities. A unified identity system, which may be able to integrate itself with multiple identity providers, and different methods of authentication and identification are necessary to manage the extensively “wired” nature of the city and the density of data transactions, systems, and solution diversity [6].

Citizens or entities can use their identities to gain access to services and systems and utilize through the benefits that they have to offer. This is a method to integrate several solutions (systems and services); eventually, entities and services repeat their identification artifact at various instances of time and in various situations.

Ideally, every citizen and/or entity should have various identifiers corresponding to various identities, each of which is composed of the scope combined with several attributes that are either exposed or used to validate a claim without revealing information. The use of multiple identifiers and identities limits the exposure of truly important credentials, thus minimizing the risk of abuse and identity theft, while allowing the exposure of less critical information that is helpful to participants in the ecosystem of the city such as retailers, building operators, service providers, and governments [6].

 ISBN: 978-1-61208-498-5

Citizens are responsible for their identities, for the information that constitutes such identities, and the condition under which this information can be exposed.
Smart cities will pass through information security problems. This paper alerts to security problems, more specifically, the problems generated by the relation of identity and identifiers. The following sections will depict some of this eminent identity threats in the scope of a smart city.

B. Identity management is not a primary objective

For users and administrators, Identity Management and Information Security are not primary concerns. Sometimes, issues with privacy are also ignored depending on the purpose of an interaction. Citizens, entities, and users, in general, are more focused on the task that must be executed rather than on the manner in which that task will identify the responsible entities.

An identity management system should focus on methods to simplify daily tasks while offering the security, transparency, and privacy that a user needs. Citizens expect an Identity Management system to be secure and transparent, and privacy to be enforced in such a manner that daily tasks become easier and not more complex. Although these are latent concerns for many users and citizens, it has been demonstrated that they are unwilling to invest money and/or time to increase security measures in any aspect of the interaction with a system or set of systems in spite of the hidden problems that such investments could avoid [8].

C. Sensing that I have been followed

Owing to the nature of a smart city, which must be an interoperable and interconnected environment and utilize various sensors (physical or social), the sensors are used to collect data from several city scenarios. This data enables urban systems to implement better city management.

Based on this assumption, it is extremely important that the information used by System B and that is originally from System A cannot be traced back to its source. Further, information provided by a citizen to improve System C must not be used to determine where that citizen is or what the citizen does [11].

Therefore, it is important to ensure that the described interchange of data has resources that prevent tracking of an entity identity.

D. Identity trust is a sensitive matter and must be earned

In recent times, account managers have been accused of fraud related to identity theft. If the person responsible for identity management is a suspect, the question of whom a citizen can entrust with identity data arises. The answer for this question must be deeply analyzed, taking some risk assessment into account. Each unique authentication and/or authorization service is susceptible to failures or attacks. Services are also vulnerable to theft because mistakes could occur. These mistakes, in addition, could create a data disclosure related to ID.

Various privacy policies are presented by approximately 20 Identity Providers (IdPs)—some focus on preserving the privacy of user transactions, some focus on enabling a single sign on environment, and others focus only on identity privacy [8][15].

E. Various types of system and services access

Identity management systems, or just IdM, have been used to create different sets of access rights. These rights offer different risk profile, thus it assumes different relations between users, identity provides, and relying parties. Unfortunately, users and system designers are not aware of this discrepancy in access rights. This may promote a set of unacceptable risks; the distinction between membership and ownership of a specific resource is fundamental.

In the context of cities, IdM were first used to centralize access rights managements to business systems and in educational environment to grant students access to wireless areas, digital libraries, laboratories and/or grade systems. In either case, identity management was used to verify whether a certain citizen is a member of a group, and not the owner of a right. Even more, IdM systems are used to enforce ownership of a resource.

Illegal accesses to different types of account could impact finances and the correct use of a system. In this context, the danger involved in using IdM systems will mainly affect a user, in a Smart City context; it may impact citizens and sensors. This affects an identity management system by enforcing membership, through the creation of different trust relations, rather than enforcing data ownership. Both cases, an identity management scheme that enforces membership is conceptually different from an IdM system that promotes ownership [16].

F. The paradigm of a single access point

Identity management systems require the user and the accessed system or service to place a large amount of trust in the identity provider. A significant part of identity and identifier information is stored with the provider; in this scenario, entities can take no action other than simply trusting the identity server and service to preserve their privacy, identifiers, and security, and to properly secure their information. However, mistakes can occur and privacy-sensitive information can become public, a group of attackers can focus their effort on invalidating the server, or a bottleneck from entities to service could be created, thus making the service unavailable [8][17].

Thus, the identity provider becomes the single point of failure. In different providers, the IdP is a critical and unique point of access, and hence, it creates a threat that allows security measures and definitions to be converged at a single point. However, this point can also become the focus of intense attacks.

G. An easy "phish" to catch even in the ocean

Today, identity management solutions provide the user with a single authentication mechanism, and the user is unable to authenticate a new IdP and Relying Party (RP). This feature is necessary in order to avoid phishing attacks in which the attacker makes users believe that their identity

 ISBN: 978-1-61208-498-5

data and credentials must be revealed. With the extent of identity management increasing, phishing attacks based on obtaining IdP and login credentials will most likely increase [8][18].

Hence, it is necessary to create and define a centralized solution in which it is feasible to moderate the number of points in the transactions performed in order to reduce the possible locations where a phish could occur. This feature would also allow data to be updated when a system flaw or compromise occurs.

H. To be or not to be, an identity crisis

One of the many advantages of identity management for citizens is that the entities do not need to remember every single identifier that may be used in order to access various solutions. In some scenarios, an entity requires only one identifier, e.g., a user name and password, in order to log in and receive a multisite token.

Based on this perspective, it would be suitable to have a single identity provider that uses a single user name/password or another authentication token to guarantee and apply a broad identification feature across different systems.

Based on a less optimistic view, this much-needed feature may not be feasible owing to the fact that users may not trust a single identity provider having access to all their services, tokens, and systems [8].

I. What you are looking at and should not: Privacy issues

Every day, solutions responsible for identifier management are requested to intervene in numerous transactions from different users on the Internet. Based on the approach, these solutions mediate transactions from entity to entity, RP, devices, systems, services, and components involving personal data information, thus registering data related to who connects with whom.

This property raises obvious privacy concerns owing to the fact that a user is prompted to provide identity (and/or identifiers) information in order to connect with different services using a unique identifier. This information is sent to an environment that audits those transactions [5][19][20].

J. Linkability across domains

A smart city uses an interconnected and interoperable environment to provide applications and solutions that have the opportunity to interact with each other, thus exchanging data. In this context, a broad linkability across all the systems involved in a smart city is potentially harmful and can result in the risk of a viral effect being created [20].

If the boundaries that delimit the connections between systems are not well protected, a system may encounter a scenario in which a value is changed in System A, and the use of this changed value by System B may corrupt the information created or stored in System B. The consequence of this behavior is known as viral effect because a system will affect another system, thus propagating a situation throughout the environment, which, in this case, is a city.

Identity Management plays an important role by providing a user the capability to track an entity across all the systems using that entity. To maintain privacy, it should be possible for users to keep their information and data private, or to create a scenario in which it is not possible for a domain to resolve "who" an identifier is in another domain, thus preventing the domain from maintaining records of who an entity is and what the entity has been doing [8].

K. Where has my data gone?

Smart systems, within the context of urban environment or smart cities, may utilize devices such as smartphones, tablets, and other gadgets. These devices provide smart systems with a wide range of data and information. Depending on the data type handled by these devices, it is possible to store personal data such as messages, pictures, appointments, bank account, and contacts.

In addition to being responsible for enabling communication with everyone, mobile devices have changed the way common citizens handle their daily tasks. A smart device has become a vault for storing and saving valuable and sensitive data that is accessible instantly. This model could create a sensitive scenario in which valuable information could be lost if the applications and solutions responsible for storing, saving, and accessing data are not well implemented and lack security measures [11][15][20].

L. Crossed access to information in data centers

In this scenario, we address situations related to undesired access to information resulting from exploitation of breaches on the server side.

This issue deals with a situation that is beyond the authentication and authorization of a particular entity. The focus must be on correct restrictions and definition of boundaries in an interoperable environment.

For example, while accessing information related to the education of a student, a given entity (application) can recover criminal records related to this citizen although the solution should use only information related to Educational Services. This situation may occur if both the systems share a common space or permissions that must be respected in order to avoid this kind of behavior are not implemented [11][15][20].

III. SMART CITY SECURITY ARCHITECTURE

OAuth, Security Assertion and Markup Language (SAML), and OpenID are solutions for authentication and authorization of assets. They are based on the assumption that each ID will be created as a unique identifier for a set of systems.

The assets could be any type of information or entities such as documents, data, and photos. Through the mentioned technologies adoption, it is feasible to create mechanisms that make it possible to transfer the responsibility of ensuring security to a third party, which could be a known server (Facebook, Google, etc.), or to

 ISBN: 978-1-61208-498-5

implement the same approach in an in-house solution. However, the demands of a smart city are considerably different from the ones addressed by these solutions. It is important to define demand-specific solutions in order to solve specific problems.

As previously mentioned this paper intends to present identity security issues under the scope of s smart city, nonetheless it also slightly presents an architecture proposal that detaches identity, identifier and data, thus mitigating the identity security issues [21].

A. Objective

The main objective of the proposed architecture is to be a layer in which an identifier is transformed into another one. The new identifier will be generated from a combination of an entity ID and the accessed service.

This mechanism will enable an entity to maintain the secrecy of its identity from a unique service and within an environment composed of several systems and services.

This approach will be valid even when the same entity accesses different sets of services. The new ID is created from a combination of two other identifiers, and hence, the resultant ID will be unique for each service accessed by the same entity.

B. General view

This sub-section describes the general components of the proposed architecture. Fig. 1 shows three layers with several components.

Each component represents a framework or technology that is well-known and adopted to guarantee information security in applications and solutions in a smart city context.

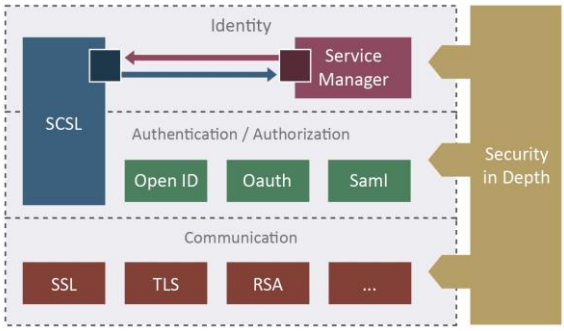

Figure.1 Architecture General view.

Each layer in Fig. 1 is described below:

Identity: It represents the portion of the reference architecture responsible for managing identifiers. It is composed of two core components: a Smart City Security Layer (SCSL) and Service Manager.

SCSL: It is an architectural module responsible for receiving a set of information and combining this information to create a new identifier for an entity.

Service manager: It is a module responsible for managing services that are used by SCSL and, indirectly, by the entities. In a following subsection more details about the Service Manager and SCSL will be explained.

Authentication/Authorization: It represents the part of the proposed architecture responsible for authentication and authorization. In this layer, various technologies such as OAuth, OpenID, and SAML are available and should be combined with the remainder of the solution.

Security in Depth: According to Schumacher et al. [17], it refers to the adoption of several security measures in various parts of a system, or solution, in order to increase overall security. This transversal module represents the need for security measures in different sections of the code responsible for service and identifier management, i.e., the implementation must take into account good practices related to security such as avoiding security risks indicated by the Open Web Application Security Project (OWASP) [22].

Communication: The proposed architecture explores the manner in which identifier management can increase security. The communication from an entity to SCSL and from SCSL to a service uses security communication protocols such as Security Sockets Layer (SSL) and Transport Layer Security (TLS).

C. A unique identity provider

The proposed architecture is a mechanism based on the concept of change identifiers involved in a system relation. A system relation is related to an entity sending and receiving values from a different set of services.

In Section IV(B), the general view, with the basic components to be adopted, was explored. In the proposed architecture, the adoption of SAML, OpenID, or OAuth is recommended for the authorization and authentication process. Further, two integrated components must be developed. These two components, SCSL and Service Manager, are responsible for providing the basic infrastructure for an entity to communicate with a service through the Internet by managing different identifiers for different identities of the same entity.

The Service Manager functions as a name register service that is responsible for receiving an address from a service. This address represents a system that will handle requests from entities. The address is made secure and is stored, and an identifier for that address is created and sent back to the requester.

This service identifier must be used by any entity that wishes to communicate with the service through SCSL.

Fig. 2 represents the basic flow associated with the architecture mechanism that is responsible for changing the ID.

 ISBN: 978-1-61208-498-5

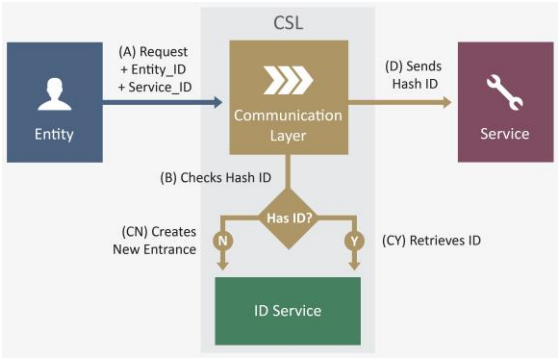

Figure 2. SCSL basic flow.

Fig. 2 is composed of:

Entity: A component that requests information from a service. A citizen, a sensor, or a service that is interoperating with another service can be an Entity. Thus, any actor of a city can be an Entity.

Service: It represents any service contacted by an entity. The Service is composed of systems of an urban environment.

Communication Layer: It represents a contact point between an Entity and a Service, and is responsible for transforming the identifier sent by the entity to the correct ID that must be used within the service.

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

The basic flow in Fig. 2 shows an Entity sending a message composed of an Entity_ID, Service_ID, and a packet.

This message is processed in SCSL, where Entity_ID is combined with Service_ID. In our case study, we combined these values to generate a 256-bit hash value.

This hash value is verified with an internal database. If the hash value does not already exist, a new register will be created with the service ID, the entity ID, and the hash value. If it already exists, it is passed to the service or used to retrieve the original ID of the Entity. This hash value is used as the Entity ID, and then, the packet is sent to the service that is retrieved from the Service Manager using the transmitted Service_ID.

D. Sequence Diagram

The sequence diagram in Fig. 3 depicts the flow implementation for registering a service and sending a message using the proposed architecture.

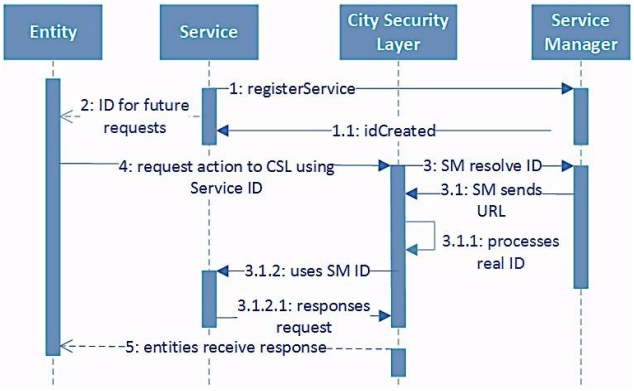

Figure 3. Platform sequence diagram.

In this scenario, a Service must initially register itself by sending a message to the Service Manager.

This action will provide the Service with an ID that is used in future requests by devices, sensors, citizens, etc.

An Entity sends a message to SCSL using this ID. The message contains the Service ID, the Entity ID, and the packet containing the data to be transmitted. The data packet format could be JSON, XML, or Plain Text.

The city security layer will execute the process described in Section IV(C), and the entity ID will be modified to the ID that must be used in the service context.

Finally, after the change in identifier, the data packet contained in the original message will be forwarded to the service.

IV. VALIDATION

In order to conduct the case study, an infrastructure was created using AWS.

This structure is composed of four sets of virtual machines. The first has the instances responsible for data generation; the second group presents the scenarios; the third group is the SCSL implementation, and the last group represents city systems.

The instance type used in this process is t2.medium, which has two vCPUs (equivalent to a 1,25GHz) and 4 GB of memory RAM.

The Relational Database Service chosen for SCSL is db.t2.medium with two vCPUs and 4 GB of memory RAM. For the set of machines responsible for the systems, we selected a db.t2.small with one vCPU and 2 GB of RAM.

With regard to the responsibilities of each set of machines, please note the following:

City systems: responsible for simulating urban services. This is composed of three systems: Natural Resources, Educational, and Government. Each system is composed of a set of web services, which in turn are built using Representational State Transfer Application Program Interface (REST API) implemented using JAVA APIs [29].

 ISBN: 978-1-61208-498-5

Each system uses one EC2 instance (t2.medium) and one RDS instance (db.t2.small).

SCSL: represents the implementation responsible for service management and ID changes.

The service manager is deployed in one EC2 (t2.medium) and one RDS (db.t2.small). The ID manager is deployed in one EC2 (t2.medium) and in one RDS (db.t2.medium).

Note that the RDS instance used for SCSL has more resources because every request passes through SCSL for ID changing.

Data generator: Responsible for generating random data used by the systems. This uses three Virtual Machine (VM) instances, where each instance generates random data for one system exclusively.

The generated data is sent in the form of a JSON request composed of an entity ID that represents the ID to be changed in SCSL, a service ID that represents the service to be requested, and nested JSON packet that contains data related to the service to be requested. In addition, the generator is responsible for creating a different and random amount of data for each system used by the applications. This means that, for example, the educational system can have a random number of Schools, each School can have a random number of Courses, and each Course can have a random number of Students. [29].

Scenarios: Scenarios 1, 2, and 3 represent a client application that consumes data from the system in the form of JSONs. Each scenario is deployed in a separate instance.

A. ID changed and functionalities preserved.

The first test used the proposed systems, and built applications to create and consume the information. Afterward, SCSL was included as a step after the applications and before the system to verify whether the applications continued to work as designed.

The changes needed to implement SCSL required each application to adopt the consumed/requested services by changing them to call the SCSL service using the Service_ID instead of directly calling a desired service.

In addition to these changes, no more updates were required, and the applications worked without modifications.

B. Different and unique ID created. Separting data from IDs..

Systems may be composed of different services in order to create a unique solution. For example, the education system uses services related to Grades, Schools, and Classes. Thus, a system can opt to use a unique ID for every service (e.g., the same Student_Number to identify student grades and classes), or it could use different IDs for each service (e.g., Student_Number for grades and Student_Number_Year for the classes taken by a particular student in a given year).

The option selected for TbE was to use different IDs per service. In this case, the result is that several IDs were created for different scopes of the same system. To validate the strengths of the proposal, IDs were revealed through applications; and in the services, an attempt was made to recover more information using the breached IDs. It was not possible to recover information from that entity in the services and system. This indicates that the IDs are indeed different from one service to another.

C. ID captured in an application did not compromise the system

This topic discusses how solutions that use different systems behave if the IDs from one system are revealed.

Nevertheless, even if all IDs are breached from all services, no corruption or recovery could be found within a different scope (in this case, systems in different scenarios).

D. Entities separated from their data

The architecture core proposes the creation of a unique and different ID for each relationship between an Entity and a Service. By doing this, the architecture achieves a separation from an Entity to its Identity. Assuming that each Identity is composed of an Identifier and its contextual Data, the architecture achieves a separation of an Entity from its Data.

E. Compartmentalization and security in depth

Compartmentalization is a concept explored by Schumacher et al. in [17]. For this concept, the authors explored the gains related to defining separate compartments per functionality.

The first topic, ID changed and functionalities preserved, explored data corruption with a unique system by exposing the ID of a service that is part of an environment with a set of services. In this case, because of the basic capability of changing IDs, the services and system in their entirety were unharmed.

The second topic, IDs within systems were independently maintained, explored the ID of a system that has been breached without compromising a second system that has a relation to the first. In the third topic, ID captured in an application did not compromise the system, when corruption began in an application (or on the client side), the systems using those IDs are still safe.

These three behaviors (service-to-service, system-to-system, and application-to-system/service) indicated that, although we are considering a unique application that consumes services, the three main components (applications, SCSL, and services) were isolated from ID discovery. Finally, the last topic, Entities separated from their data, explored the… result of SCSL appliance, in which a entity is separated from its identity, and therefore, separated from its data.

 ISBN: 978-1-61208-498-5

Through the mentioned characteristics and gains it can be proved that the identity is safer into an interoperable environment; moreover, entity privacy is demonstrated to have increased.

V. EVALUATION

The main strength of SCSL is its ability to provide a citizen with a ubiquitous mechanism in which the entity is required to provide the environment with only one identifier, allowing the ID service to retrieve and build different identifiers, thus different identities, for each requested system.

The adoption of this approach enables identity management to be handled differently because the actual identification of a citizen or sensor will be hidden from the system responsible for the data, and, therefore, from eventual breaches in such systems.

The following subsection depicts the impact of the proposed architecture in order to validate how the introduced issues are addressed by this approach.

A. Identity management is not a primary objective

Identity management will still remain a secondary objective; however, the use of the SCSL approach permits this concern to be less important.

The proposed approach will ensure that an Identity System is responsible for dealing with identities and identifiers, thus diminishing the need for citizens to be concerned about this particular aspect.

B. Sensing that I have been followed

The main strength of the proposed architecture is in being a solution that separates real IDs from operational IDs used by city systems. Thus, only the central ID manager will have the ability to retrieve the ID of a citizen; however, the information related to each ID will not be available to the central ID manager. This information will be maintained in the city system.

The city system has only partial information; the actual ID is not available to this system. Thus, each component of the environment will have certain part of the entire data, and therefore, linking information to an ID, and an ID to a citizen will not be possible.

C. Identity trust is a sensitive matter and must be earned

Let us consider a scenario in which citizens would not need to be worried about identity issues by allowing a single third party to be responsible for managing their identifiers. This situation would probably increase their trust because the third party will have access to identifiers and not identities, and therefore, the data of citizens will be safe in the system.

The notion that, even if the data system is breached, the identity will remain in safety, is a powerful motivation for trusting SCSL.

D. Various types of system and services access

This issue deals with problems related to identity management systems that are responsible for applying various types of access rights and permissions. Although OAuth and other frameworks have been specified as authorization and authentication frameworks that could be used with the remainder of the solution, we do not believe that identifier management addresses this issue.

E. The paradigm of a single access point

The adoption of a single system responsible for identity and identifier management will enable the strength to be focused at a single point, thus increasing the overall security. The system responsible for the identifiers is the one that must be secure; this situation is equivalent to protecting the keys in a key-locker system. One does not need to protect the entire environment but only the portion that is capable of identifying the rest of the environment.

However, significant attention must be given to this characteristic owing to the fact that if the solution fails, the entire city will be unable to function because it will not be possible to resolve an entity ID.

F. An easy "phish" to catch even in the ocean

This issue is not addressed by the proposed approach because authentication and authorization concerns are beyond the scope of this proposal. Although we have suggested the adoption of OAuth, SAML, or OpenID as authentication and authorization handlers, our focus is on identity management.

G. To be or not to be, an identity crisis

The existence of a single identity manager enables the citizen and other city entities to refer to a unique point using a single identifier to access all other identities that the entity may have within the entire environment. This notion permits one identifier to be multiplexed by N other identifiers by a third party, thus avoiding problems related to managing a group of IDs.

H. What you are looking at and should not: Privacy issues

Privacy issues are partially solved by identity and identifiers management. As mentioned earlier, the primary consequence of the adoption of the proposed architecture is a separation of data and citizen identifiers, and, thus a separation of identity and identifiers.

Thus, even if certain data is revealed, it will not be possible to determine the entity that the data belongs to or the data of a specific entity. Therefore, the information of a citizen will remain private.

I. Linkability across domains

This issue is addressed by SCSL owing to the capability already mentioned earlier. The same entity account will be identified differently in each system and/or service of a city; thus, the maintenance of linkability across domains will be difficult for an attacker. In order to validate an ID recovered from a system, an attacker must initially pass through the

 ISBN: 978-1-61208-498-5

identification service, and then, discover the equivalent identity in a secondary system.

J. Where has my data gone?

As mentioned in section IV, the primary strength of the three (OAuth, SAML and OpenID) standards lies in interoperability and authentication, and therefore, they do not impact the issue discussed in Section III. A similar reasoning applies to SCSL; it proposes to change the manner in which identifiers are sent and used by systems, and therefore, it does not impact this issue.

K. Crossed access to information in data centers

This issue is addressed by SCSL. Although an attacker can compromise a system, gather information about a citizen, and access other systems through the compromised system, the attacker will have the perception that the system databases are composed of different entities. An entity will be presented differently for each system or service.

VI. CONCLUSION

The development of new collaborating systems based on the current systems that support a city is an urgent need in order to enable urban environments to deliver better service to citizens and improve the current infrastructure. Further, this development plays a crucial role in the creation of new methods to sustain the changes in the composition of cities.

The new proposed paradigm, related to an interoperable environment of city systems, poses various challenges such as performance, usability, availability, privacy, and information security. Security concerns are a challenge that must be addressed. The absence of a solution to this problem will result in citizens avoiding the use of the offered solutions, and therefore, the development of smart cities will be affected.

This study explored a set of identification and privacy problems that continue to pose challenges and addressed questions that must be answered in order to offer a more secure environment to citizens. An approach based on identifiers and identity separation architecture was presented and analyzed. It has been demonstrated that the proposed architecture improves the privacy and anonymity of citizens.

In future work, we intend to conclude an ongoing study related to validating performance issues related with the adoption of the proposed architecture. Further, we will evaluate various new security issues in smart cities and deploy a cloud-based system for the identity service.

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: 20 – July -2016 ” .

[3] F. Ferraz, C. Sampaio, and C. Ferraz, “Towards a Smart City Security Model Exploring Smart Cities Elements Based on Nowadays Solutions,” ICSEA 2013, no. c, pp. 546–550, 2013.

[4] 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.

[5] A. Martinez-Balleste, P. Perez-martinez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy-aware smart city is possible,” IEEE Commun. Mag., vol. 51, no. 6, pp. 136–141, Jun. 2013.

[6] 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.

[7] P. (2010). Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, “Foundations for Smarter Cities,” IBM J. Res. Dev.

[8] R. Dhamija and L. Dusseault, “The Seven Flaws of Identity Management: Usability and Security Challenges,” IEEE Secur. Priv. Mag., vol. 6, no. 2, pp. 24–29, Mar. 2008.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] G. Alpár, J. Hoepman, and J. Siljee, “The identity crisis. security, privacy and usability issues in identity management,” arXiv Prepr. arXiv1101.0427, pp. 1–15, 2011.

[17] 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.

[18] I. D. Addo, S. I. Ahamed, S. S. Yau, and A. Buduru, “A Reference Architecture for Improving Security and Privacy in Internet of Things Applications,” 2014 IEEE Int. Conf. Mob. Serv., pp. 108–115, Jun. 2014.

[19] A. Ukil, “Connect with Your Friends and Share Private Information Safely,” 2012 Ninth Int. Conf. Inf. Technol. - New Gener., pp. 367–372, Apr. 2012.

[20] 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 2014 IEEE International Conference on Ubiquitous Intelligence and Computing/International Conference on Autonomic and Trusted 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence & Computing and 2014 IEEE 11th Intl Conf on Autonomic & Trusted Computing and, 2014, vol. 677–686, p. 9.

[21] 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,” in SOFTENG 2015 : The First International Conference on Advances and Trends in Software Engineering Information, 2015, no. c, pp. 108–114.

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