An Approach to Information Security by Applying a Conceptual Model of Identities in Smart Cities Projects

[1]Moises Toapanta, [2]Enrique Mafla and [3]Jose Orizaga
[1]Department of Computer Science, Universidad Politecnica Salesiana Ecuador, Robles 107 Chambers,
Guayaquil, Ecuador
[2]Faculty of Engineering Systems, Escuela Politecnica Nacional, Ladron E11-253, Quito, Ecuador
[3]Department of Information Systems, Centro U. Ciencias Economico Administrativas (CUCEA),
Universidad de Guadalajara, Periferico Norte # 79, Zapopan, Jalisco, Mexico

Abstract: It analyzed different projects of intelligent cities related to information security were analyzed that mitigate vulnerabilities and risks of citizens, cities and organizations that integrate. The objective is to provide sufficient arguments for a conceptual model of identities to be considered at a strategic level for important projects in a country. A deductive method was used for exploratory research to determine the approach to securing similar projects. A general prototype of a conceptual model of identities was obtained to mitigate the security of the information that originates in the civil registry of Ecuador and its relation with the institutions involved for this management. It was determined that to mitigate the vulnerabilities and risks of information in future projects of smart cities for Ecuador in the first phase is considered as alternative the development of a conceptual model management of identities.

Key words: Identity models, smart cities, information security, information management, integrity of information, vulnerabilities

INTRODUCTION

Information security is considered at the global level by all organizations as the main and strategic asset for development; the projects smart cities consider information security with Confidentiality, Integrity and Availability (CIA); Ecuador like other countries in the world is structuring smart cities projects for Quito, Guayaquil, Cuenca, among other major cities in the country, due to the terrorist attacks and organized delinquencies that have proliferated every time in all the major metropolitan cities especially in the aerial terminals, human conglomerations, among others for this reason it is looking for alternatives to ensure the identity of the users of the systems and the people that circulate in all the cities. Future projects in Ecuador's smart cities will take information from secure databases; through the agencies responsible for the delivery of information such as the "National Directorate of Public Data Registry" the same that is supplied by the "National Directorate of Civil Registry of Ecuador" of a database under a distributed environment which at the moment is in a research project with the topic "Algorithms and Security Protocols for the Civil Registry of Ecuador" of the mentioned projects the

researchers have articles scientists published as: Analysis to define management of identities access control of security processes for the registration civil from Ecuador (Toapanta *et al.*, 2016a); Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador (Toapanta *et al.*, 2016b).

Why it is necessary to consider an approach to mitigate information security by applying a conceptual model of identities for futures projects of smart cities for Ecuador?

For carry out the analysis and as is focuses the conceptual model of identities to mitigate the security of the information in future smart cities of Ecuador.

The objective is to provide sufficient arguments for a conceptual model of identities to be considered strategic to mitigate the security of information with confidentiality, integrity and availability. The revised papers related to the research topic are as follows.

Using conceptual modeling to support innovation challenges in smart cities (Bork *et al.*, 2016), Cyber security challenges in smart cities: Safety, security and privacy (Elmaghraby and Losavio, 2014), security and privacy in smart city applications: challenges and solutions (Zhang *et al.*, 2017); more than meets the eye in

Corresponding Author: Moises Toapanta, Department of Computer Science, Universidad Politecnica Salesiana Ecuador,
Robles 107 Chambers, Guayaquil, Ecuador

smart city information security: exploring security issues far beyond privacy concerns (Ferraz and Ferraz, 2014); Cyber security in smart city of Dubai (Efthymiopoulos, 2016), Midgar; Detection of people through computer vision in the internet of things scenarios to improve the security in smart cities, smart towns and smart homes (Garcia *et al.*, 2017); information security in a public safety, participatory crowdsourcing smart city project (Cilliers and Flowerday, 2014); the design and implementation of information system based on the hybrid identity authentication technology (Zhong and Chen, 2011); automatic assets identification for smart cities: Prerequisites for cyber security risk assessments (Waedt *et al.*, 2016), cross-layer security framework for smart grid: physical security layer (Farag *et al.*, 2014); LTE network strategy for smart city public safety (Raza, 2016), the privacy case: matching privacy-protection goals to human and organizational privacy concerns (Ionescu and Engelbrecht, 2016); Producing linked data for smart cities: the case of Catania (Consoli *et al.*, 2017), cyber-security in smart cities: the case of Dubai (Efthymiopoulos, 2016), data security and threat modeling for smart city infrastructure (Wang *et al.*, 2015).

The main result that has been obtained is the general prototype of an identity management model with the possible actors involved in future projects of smart cities in Ecuador; the revised articles do not specify a similar proposal for this reason I consider it a challenge in the first phase to develop as an alternative an identity management model.

It was determined that to mitigate the vulnerabilities and risks of information in future projects of smart cities for Ecuador in the first phase is considered as alternative the development of a conceptual model of identities.

MATERIALS AND METHODS

The method used in this research is the deductive in order to review the information of the reference and determine the approaches to mitigate information security, applying a conceptual model of identities for future projects of smart cities for Ecuador.

Analysis of the information security approach smart cities: All projects developed by public and private organizations require that the information they receive for their management has confidentiality, integrity and availability to continuation an analysis of the information related to the topic.

It proposes the integration of services in smart cities through a conceptual model for the purpose of managing the administration, planning and operation of technological infrastructures (Bork *et al.*, 2016). The

security challenge is based on the fact that most have mobile phones, smart devices in cars, among others that have to do with the internet of things; You can use all this technological infrastructure for the design of an smart cities that are integrated with a Geographic information System (GPS), that allow us to integrate public, private and relief institutions (Elmaghraby and Losavio, 2014). A smart city must be able to control the physical world and provide information in real time to local citizens foreigners in land terminals, aerial on the situation of the environment, health, places of visit, availability of energy, however, there is concern about security and privacy and intelligent applications; considers above all the confidentiality and integrity of the citizen's information on any technological infrastructure to be used at the software and hardware level (Zhang *et al.*, 2017). In smart cities above all things, the confidentiality, integrity and availability of the citizen and the smart city must prevail with responsibility for urban systems, also defines a fourth important factor is the interoperability of the within the urban and integrated sector (Ferraz and Ferraz, 2014). Dubai is an example of a city integrated with the aim that the government and the city be an example of development, stability and security by 2020 Dubai according to its planning would be one of the smart cities integrated throughout is a strategic planning model to be a first rate developed city, the success for this project is the business, economic, security and strategic management as policies and processes in view that acquiring a state of the art technological infrastructure is not a problem for them for this reason you must work under a multilevel scheme (Efthymiopoulos, 2016). The purpose is to create security areas for people, cities or homes through IP cameras through computer vision, considering the internet paradigms of things and automate the use of IP cameras for this reason proposes the analysis of the images with the method of computer vision to automate the events (Garcia *et al.*, 2017). Crowdsourcing is used to gather information from smart cities; the citizen should consider how to use this utility to mitigate security in a participatory way in projects of smart cities; states that it is important to maintain Confidentiality Integrity and Availability (CIA) in the crowdsourcing smart cities project, also indicates that legislation and technologies must work together to protect the confidentiality of citizens (Cilliers and Flowerday, 2014). The design of the security system must be hybrid where identity authentication is the main component for information security, proposes a new hybrid identity authentication technologies combined with smart cards, chaos theory and fingerprint recognition for recognition as a mixed system (Zhong and Chen, 2011). Smart cities assets should be considered within the

global platform environment, interrelating the different administrative, legislative and technical habits to carry out a good management of the projects of smart cities (Waedt *et al.*, 2016). It is proposed that information security be handled at the layer level because of the different vulnerabilities that may exist in each layer and domains of the network or servers, considers that a conceptual model of intelligent network layers and an overview of security with the application of CyNetPhy integrates and coordinates to interrelate the real time security of the systems in different section and several layers of the cyber network, physical domain of operational problems and security requirements (Farag *et al.*, 2014). The tetra networks will be aligned to the concepts of smart cities in this document a survey of the use of the public security service; a defined strategy for public networks are the LTE networks that constitute an important point the evolution of smart cities (Raza, 2016). The concern of privacy with its respective risks helps to define the goals as far as the privacy of the people and organizations to solve this conflict must be done through strategies, technical and non-technical solutions that can be incorporated into projects of smart cities (Ionescu and Engelbrecht, 2016). Semantic technology allows the development of smart cities through the discussion of the importance of syntactic and semantic interoperability, we present a comprehensive data model for smart cities including geo-referenced data, public transport, urban fault reporting, road maintenance and municipal information collection with information security (Consoli *et al.*, 2017). Dubai is one of the first cities in the world that has been concerned that smart cities projects are with technological innovation, infrastructure design and strategic security is a world leader in smart cities projects with the challenge of becoming a smart city by 2020 in an integrated shape with strategic technology, innovation and management to mitigate the security of the information of the people and organizations with privacy, provides infrastructures, smart services on the network and protect the environment (Efthymiopoulos, 2016). Troubleshooting security issues with different software and hardware has not been enough to mitigate the security of information, it is necessary to define information security policies to the organizations to guarantee security controls in the local environments; considers that security management should be done through Confidentiality Integrity and Availability (CIA) and issue policies to alert security administrators to develop integrated projects of smart cities that guarantee the management of information security (Wang *et al.*, 2015).

Organizations that should consider participating in future smart cities projects in Ecuador: The main institutions and organizations to be subscribed in participate in the projects of smart cities in Ecuador to mitigate the vulnerabilities of the information security in a globalized form are: Directorate General of Civil Registry, National Direction of Data, National Security System 911, among others in order to use all existing resources at the software and hardware level, considering as main factor the privacy of the people and organization, through the management of information with Confidentiality, Integrity, Availability (CIA) under the concept of a management model with Identity, Authentication, Authorization and Audit (IAAA).

Situation of smart cities projects in Ecuador; the different public institutions dependent on the central government, autonomous municipalities, universities, polytechnic schools of Ecuador, undergraduate students, masters, doctorates among others have undertaken projects of smart cities without considering an appropriate integrative identity management model that allows to mitigate the security of the information, this has caused losses for the Ecuadorian state in human, technical, operational, management which has not allowed the reuse of the technological infrastructures available to the different institutions and organizations of the country in the area of information security of future projects of smart cities for Ecuador, the privacy of individuals and organizations must be taken into account as a priority.

RESULTS AND DISCUSSION

Provide sufficient arguments for a conceptual model of identities to be considered strategic to mitigate the security of information;provide the support of the authorities at strategic level and the paradigm shift of professionals and researchers in the area of information security; that the future projects of smart cities are managed in every structure of the organization at the operational, tactical, strategic level considering an identity management model.

After reviewing the reference articles for the purpose of arguing "An approach to mitigate information security by applying a conceptual model of identities for futures projects of smart cities for Ecuador" the following results were obtained.

The majority of the reseachers of the analyzed scientific articles consider that the security of the information is strategic to guarantee different projects of technologies of the information and communications, since, the main asset of an organization is information. The degree of influence of security with interpretation was determined for the different organizations and Institutions that deliver the information for future smart cities projects of the Ecuador.

Table 1: Scale for measuring the degree of influence (table of influence)

Security	Interpretation	Score
Networks	Not present or no influence	0
Networks	Not present or no influence	0
Database	Incidental influence	1
Mechanics	Moderate influence	2
Computing	Average influence	3
Adminitrative	Significant influence	4
Integrated identity management models	Strong influence throughout	5

Table 1 observed the degree of influence of information security with a zero to five interpretation for future smart cities projects. Description of the scale to measure degree of influence; network security is based on the different facilities provided by the layers of the OSI model, encryption software, networking equipment, servers and media. In reference to the security of the database independently is given according to the facilities provided by the base engines and the administrator.

Mechanical security integrates the two previous levels considering all networking equipment LAN, MAN, WAN and the different servers with their respective operating systems. The fourth level refers to information security that integrates the previous phases and considers the administrative policies at all tactical and strategic operational levels.

Administrative security issued at strategic levels and implemented at all levels to mitigate the security of information. Identity management models integrate all previous security levels with international standards for handling communications, intellectual property, confidentiality, integrity, availability, identity, authentication, authorization auditing to achieve the privacy of citizens, users and organizations without dependence on a specific technological infrastructure; this type of model must be developed for future projects of smart cities of Ecuador.

Referring to Table 2, the information that each institution or organization in projection must provide for future projects of smart cities in Ecuador must comply with the security of the information established in Table 1 of the degree of influence.

Table 2 it can be observed that the organizations that have a rating of 5 are those that directly must deliver the information in the future projects of smart cities.

It is determined the elaboration of a general prototype with the main actors for future projects of smart cities of Ecuador, since, the revised articles do not clearly specify a similar proposal for that reason I consider it a challenge that the information security of future projects of smart cities for Ecuador in the first phase, an identity management model.

Figure 1 prototype conceptual model for smart cities of "an approach to information security by applying a conceptual model of identities in smart cities projects" it was considered that the basic information to be taken

Table 2: Institutions that can be considered to integrate a smart cities project in Ecuador (influence in security)

Types/Description	Score
Strategic	
General Directorate Civil Registry of	5
Ecuador Public Data Office of Ecuador	5
National Security System 911 (Integran: Armed	5
Forces, National Police, Hospitals, Firemen,	
Civil Defense, International Organizations)	
Tactical	
Ministries	4
Municipalities	4
Universities and polytechnic schools	4
Operational	
Airports, land and sea terminals	3
Social organizations	3
Federation of taxi drivers	3
Urban and interprovincial carriers	3
Private security companies	3
Foundations	3
Shopping malls, entertainment, among others	3

for future projects of smart cities will be from the database of the Civil Registry of Ecuador with Confidentiality, Integrity, Availability (CIA) under a conceptual model with Identity, Authentication, Authorization, Auditory (IAAA), that allows mitigating the vulnerabilities and risks of information for future projects of smart cities in Ecuador.

It is note that the prototype of a conceptual model for smart cities, it is important to do prior to the start of a smart cities project in the area of information security for the following reasons; first with the conceptual model I can clearly identify where the information will be taken for the smart cities project: second, if the information I am going to have has an Identity, Authentication, Authorization, Audit (IAAA) with Confidentiality, Integrity, Availability (CIA) of those who provide; third, that this information provides privacy for the delivery to local citizens foreigners and organizations. At this stage, there is no appropriate identity management model for information security projects for future smart cities in Ecuador in view only prototype was obtained.

The prototype of the conceptual model for smart cities and revised articles agree that information security should be managed at a strategic level.

This research may be validated for any country with similar organizational structures to Ecuador and be taken as a reference for future information security projects.

It is conclude that a model of security management will allow mitigating the vulnerabilities and risks of information in future projects of smart cities undertaken by Ecuador, taking as a challenge in the first phase the elaboration of this model that allows to manage the security of the information, mitigating Identity, Authentication, Authorization, Audit (IAAA) with Confidentiality Integrity and Availability (CIA), so that, the delivery of information to local citizens foreigners and organizations is with the respective privacy, finally I
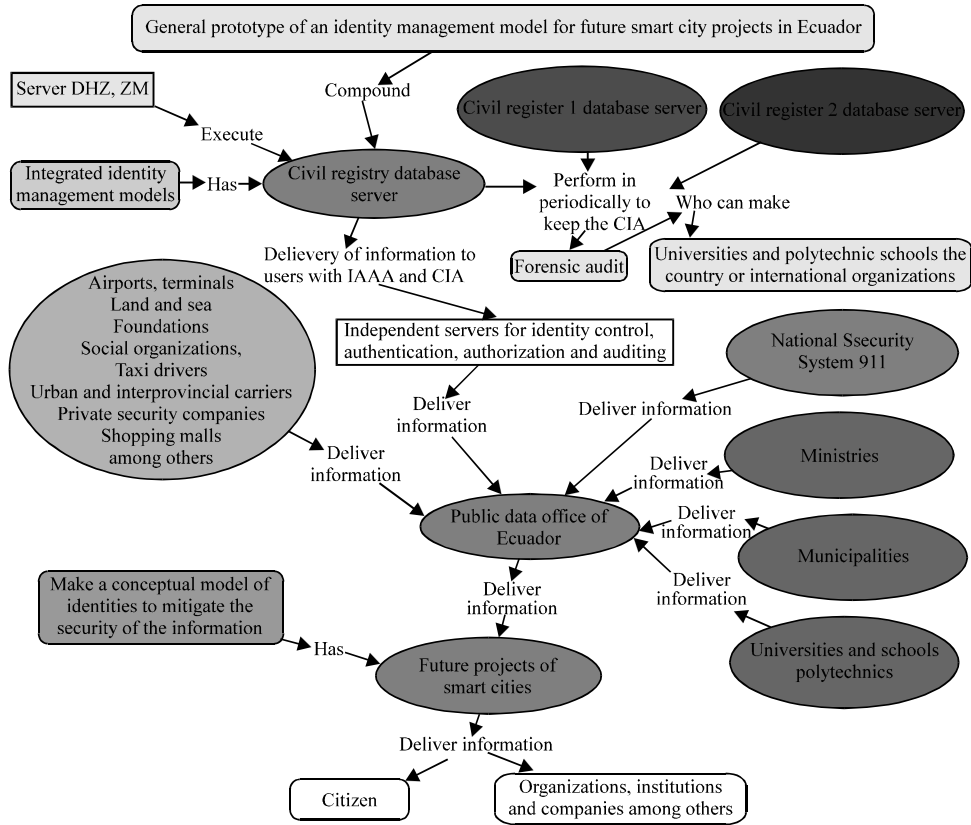
Fig. 1: Prototype conceptual model for smart cities

suggest to consider the exposed in view that with an appropriate model, I do not know will depend on specific technological infrastructures.

The mitigation of information security is not solved level network, database and mechanical, administrative without considering as an alternative the development of an appropriate identity management model in the first phase for each type of organization, depending on the business reason.

CONCLUSION

To consider as a reference this prototype conceptual model of identities and in the following phase develop the model prior to the execution of future projects of smart cities for Ecuador.

RECOMMENDATIONS

It is concluded that to mitigate the vulnerabilities and risks of information in future projects of smart cities for Ecuador in the first phase is considered as alternative develop a conceptual model of identities, it allows to manage the security of the information mitigating the Identity, Authentication, Authorization, Audit (IAAA)

with Confidentiality Integrity and Availability (CIA), so that, the delivery of information to local citizens foreigners and organizations is with the respective privacy.

ACKNOWLEDGEMENTS

REFERENCES

Bork, D., R. Buchmann, I. Hawryszkiewycz, D. Karagiannis and N. Tantouris *et al.*, 2016. Using conceptual modeling to support innovation challenges in smart cities. Proceedings of the IEEE 2nd, 14th and 18th Joint International Conference on Data Science and Systems (HPCC/SmartCity/DSS), High Performance Computing and Communications Smart City, December 12-14, 2016, IEEE, Sydney, New South Wales, Australia, ISBN:978-1-5090-4297-5, pp: 1317-1324.

Cilliers, L. and S. Flowerday, 2014. Information security in a public safety, participatory crowdsourcing smart city project. Proceedings of the 2014 World Congress on Internet Security (WorldCIS), December 8-10, 2014, IEEE, London, UK., ISBN:978-1-908320-42-1, pp: 36-41.

Consoli, S., V. Presutti, D.R. Recupero, A.G. Nuzzolese and S. Peroni *et al.*, 2017. Producing linked data for smart cities: The case of Catania. Big Data Res., 7: 1-15.

Efthymiopoulos, M.P., 2016. Cyber-security in smart cities: The case of Dubai. J. Innovation Entrepreneurship, 5: 2-16.

Elmaghraby, A.S. and M.M. Losavio, 2014. Cyber security challenges in Smart cities: Safety, security and privacy. J. Adv. Res., 5: 491-497.

Farag, M.M., M. Azab and B. Mokhtar, 2014. Cross-layer security framework for smart grid: Physical security layer. Proceedings of the 2014 IEEE PES Conference on Innovative Smart Grid Technologies Europe (ISGT-Europe), October 12-15, 2014, IEEE, Istanbul, Turkey, ISBN:978-1-4799-7720-8, pp: 1-7.

Ferraz, F.S. and C.A.G. Ferraz, 2014. More than meets the eye in Smart city information security: Exploring security issues far beyond privacy concerns. Proceedings of the 2014 IEEE 11th, 11th and 14th International Conference on Ubiquitous Intelligence and Computing, Autonomic and Trusted Computing and Scalable Computing and Communications and its Associated Workshops (UTC-ATC-ScalCom), December 9-12, 2014, IEEE, Bali, Indonesia, ISBN:978-1-4799-7646-1, pp: 677-658.

Garcia, C.G., D. Meana-Llorian, B.C.P. G-Bustelo, J.M.C. Lovelle and N. Garcia-Fernandez, 2017. Midgar: Detection of people through computer vision in the internet of things scenarios to improve the security in smart cities, smart towns and smart homes. Future Gener. Comput. Syst., 76: 301-313.

Ionescu, T.B. and G. Engelbrecht, 2016. The privacy case: Matching privacy-protection goals to human and organizational privacy concerns. Proceedings of the Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), April 12-12, 2016, IEEE, Vienna, Austria, ISBN:978-1-5090-1164-3, pp: 1-6.

Raza, A., 2016. LTE network strategy for smart city public safety. Proceedings of the IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), August 3-6, 2016, IEEE, Balaclava, Mauritius, ISBN:978-1-5090-0706-6, pp: 34-37.

Toapanta, M., E. Mafla and J. Orizaga, 2016b. Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador. Proceedings of the International Conference on Materials, Minerals and Energy Selection and Peer-Review under Responsibility, July 29-30, 2016, ELSEVIER, Ongole, India, pp: 1-6.

Toapanta, S.M.T., L.E.M. Gallegos and J.A.O. Trejo, 2016a. Analysis to define management of identities access control of security processes for the registration civil from Ecuador. Proceedings of the 2016 IEEE International Conference on Smart Cities (ISC2), September 12-15, 2016, IEEE, Trento, Italy, ISBN:978-1-5090-1846-8, pp: 1-4.

Waedt, K., A. Ciriello, M. Parekh and E. Bajramovic, 2016. Automatic assets identification for smart cities: Prerequisites for cybersecurity risk assessments. Proceedings of the 2016 IEEE International Conference on Smart Cities (ISC2), September 12-15, 2016, IEEE, Trento, Italy, ISBN:978-1-5090-1846-8, pp: 1-6.

Wang, P., A. Ali and W. Kelly, 2015. Data security and threat modeling for smart city infrastructure. Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), August 5-7, 2015, IEEE, Shanghai, China, ISBN:978-1-4673-7977-9, pp: 1-6.

Zhang, K., J. Ni, K. Yang, X. Liang and J. Ren *et al.*, 2017. Security and privacy in smart city applications: Challenges and solutions. IEEE. Commun. Mag., 55: 122-129.

Zhong, D. and C. Chen, 2011. The design and implementation of information system based on the hybrid identity authentication technology. Proceedings of the 2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering (CCIE) Vol. 1, August 20-21, 2011, IEEE, Wuhan, China, ISBN:978-1-4244-9599-3, pp: 409-412.