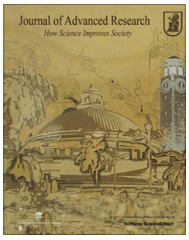
Journal of Advanced Research (2014) 5, 491–497

Cairo University

Journal of Advanced Research



ORIGINAL ARTICLE

Cyber security challenges in Smart Cities: Safety, security and privacy

Adel S. Elmaghraby *, **Michael M. Losavio**

Computer Engineering and Computer Science Department, 211 Duthie Center for Engineering, University of Louisville, Louisville, KY 40292, USA

ARTICLE INFO

Article history:
Received 29 October 2013
Received in revised form 4 February 2014
Accepted 25 February 2014
Available online 5 March 2014

Keywords:
Smart City
Internet of Things
Security
Privacy protecting systems
Security and privacy models

ABSTRACT

The world is experiencing an evolution of Smart Cities. These emerge from innovations in information technology that, while they create new economic and social opportunities, pose challenges to our security and expectations of privacy. Humans are already interconnected via smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities. Homes, cars, public venues and other social systems are now on their path to the full connectivity known as the "Internet of Things." Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. We examine two important and entangled challenges: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear. Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live. We also present a model representing the interactions between person, servers and things. Those are the major element in the Smart City and their interactions are what we need to protect.

Introduction

The benefits of Information and Computing Technologies (ICT) in a Smart City and of the Internet of Things are tremendous. Smart energy meters, security devices, smart appliances for health and domestic life: these and more offer unprecedented conveniences and improved quality of life. City infrastructures and services are changing with new interconnected

* Corresponding author. Tel.: +1 502 852 0470; fax: +1 502 852 4713.
E-mail address: adel.elmaghraby@louisville.edu (A.S. Elmaghraby).

Peer review under responsibility of Cairo University.

2090-1232 © 2014 Production and hosting by Elsevier B.V. on behalf of Cairo University.
http://dx.doi.org/10.1016/j.jare.2014.02.006

systems for monitoring, control and automation. These may include water and sanitation to emergency responders and disaster recovery.

These benefits must be considered against the potential harm that may come from this massively interconnected world. Technical, administrative and financial factors must be weighted with the legal, political and social environment of the city.

Methodology

Several paradigms and categorical structures may be applied in analyzing the benefits and detriments of this data environment. An applicable paradigm used for this analysis is that of IBM that the Smart City, its components and its citizens are

- Instrumented
- Interconnected and
- Intelligent.

This is denoted as "IN3."

"Instrumented" gives city components and citizens devices, at varying levels of features that, at a minimum, respond to a sensor network. These are, in turn, "interconnected" as to pass information into a network. That information is computationally available for analysis and decision-making, making the Smart City "intelligent" in its operations.

Security and privacy concerns rest on how the information within IN3 is used. The core of the technology is the information. A full examination of any system of the Smart City may categorize information as to sources, types, collections, analytics and use (see Figs. 1–4).

The instrumented source may have particular rights or risks associated with particular types of information, such as a person's location or actions. The collections of that information, such as on the device or on a cloud aggregator, similarly invoke issues of rights, duties and risks. From those collections analytics can build services of varied sophistication which, in turn may be used for good or ill.

The loci of activity nodes may be categorized in relation to people, workplace, transportation, homes and social/commercial interactions.

An additional way to categorize within this space is to consider information source nodes as the activities and services of social and civic life, people, work, home, transport and social life.

In all of the interactions the information generation and exchange is at least bilateral and communicative. Actions often

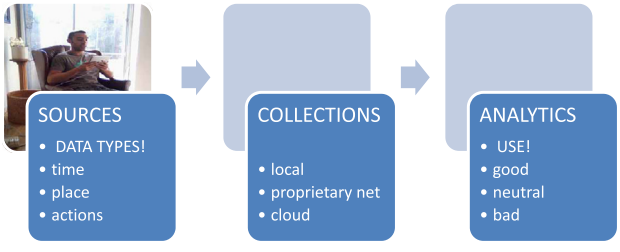


Fig. 1 Data sources feed data collections feed data analytics for knowledge.

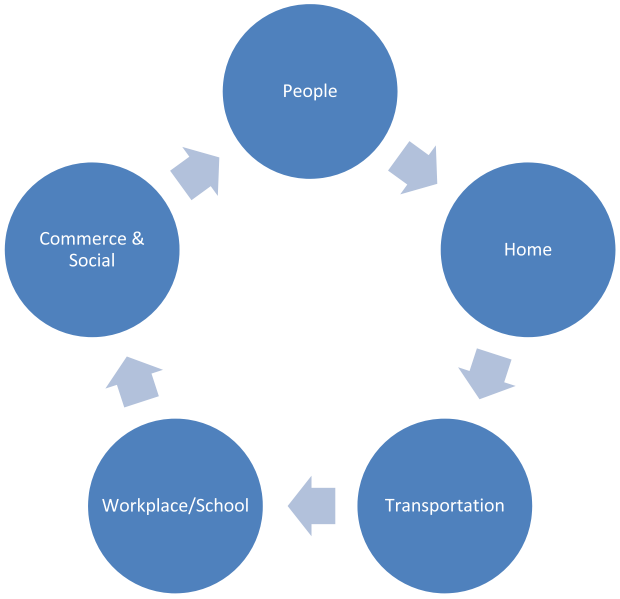


Fig. 2 The production loci of data in the Smart City.

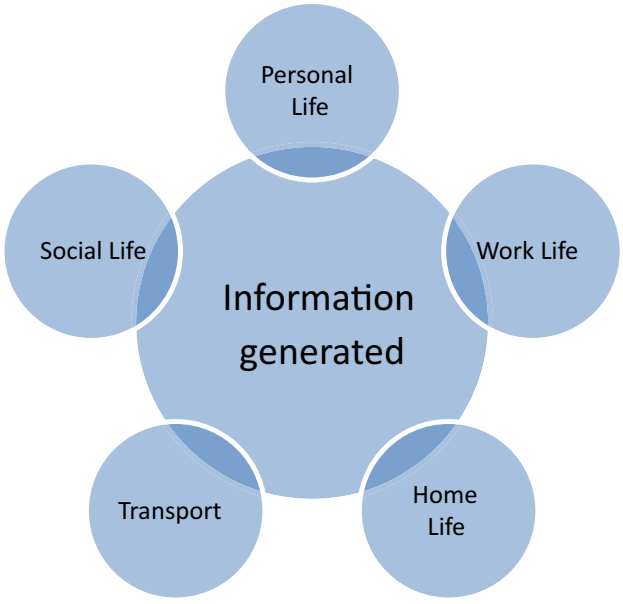


Fig. 3 Source nodes of activities and services producing data.

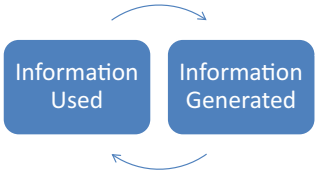


Fig. 4 The recursive cycle of data in the Smart City – information generated is information used is information generated is information used.