Accepted Manuscript

Towards a secure service provisioning framework in a Smart city environment

Zaheer Khan, Zeeshan Pervez, Abdul Ghafoor Abbasi

PII: S0167-739X(17)31368-7
DOI: http://dx.doi.org/10.1016/j.future.2017.06.031
Reference: FUTURE 3529

To appear in: *Future Generation Computer Systems*

Received date : 30 November 2015
Revised date : 1 June 2017
Accepted date : 27 June 2017

Please cite this article as: Z. Khan, Z. Pervez, A.G. Abbasi, Towards a secure service provisioning framework in a Smart city environment, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.06.031

Towards a Secure Service Provisioning Framework in a Smart City Environment

Abstract:

Over the past few years the concept of Smart cities has emerged to transform urban areas into connected and well informed spaces. Services that make smart cities "smart" are curated by using data streams of smart cities i.e., inhabitants' location information, digital engagement, transportation, environment and local government data. Accumulating and processing of these data streams raise security and privacy concerns at individual and community levels. Sizeable attempts have been made to ensure the security and privacy of inhabitants' data. However, the security and privacy issues of smart cities are not only confined to inhabitants; service providers and local governments have their own reservations – service provider trust, reliability of the sensed data, and data ownership, to name a few. In this research we identified a comprehensive list of stakeholders and modelled their involvement in smart cities by using the Onion Model approach. Based on the model we present a security and privacy-aware framework for service provisioning in smart cities, namely the 'Smart Secure Service Provisioning' (SSServProv) Framework. Unlike previous attempts, our framework provides end-to-end security and privacy features for trustable data acquisition, transmission, processing and legitimate service provisioning. The proposed framework ensures inhabitants' privacy, and also guarantees integrity of services. It also ensures that public data is never misused by malicious service providers. To demonstrate the efficacy of SSServProv we developed and tested core functionalities of authentication, authorisation and lightweight secure communication protocol for data acquisition and service provisioning. For various smart cities service provisioning scenarios we verified these protocols by an automated security verification tool called Scyther.

Keywords: Smart city, security, privacy, trust, framework, stakeholders, secure service provisioning

1. Introduction and Context

Smart cities are emerging rapidly due to new technologies such as the Internet of Things (IoTs), e.g., RFIDs, environmental sensors, actuators, smart phones, wearable sensors, cloud computing, etc. New smart city services and applications (e.g. participatory sensing [1][2]) provide the opportunity to collect and effectively use large scale city data for information awareness, urban planning, policy making and decision making [3][4]. As a result, new models of transformed urban governance e.g. open governance are being formed where data from