Sustainable Cities and Society 39 (2018) 499–507

Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs

Security and privacy challenges in smart cities

Trevor Braun[a], Benjamin C.M. Fung[a,*], Farkhund Iqbal[b], Babar Shah[b]

[a] School of Information Studies, McGill University, Montreal, Canada H3A 1X1
[b] College of Technological Innovation, Zayed University, P.O. Box 144534, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Keywords:
Smart cities
Information security
Privacy protection
Cyber-physical systems

ABSTRACT

The construction of smart cities will bring about a higher quality of life to the masses through digital interconnectivity, leading to increased efficiency and accessibility in cities. Smart cities must ensure individual privacy and security in order to ensure that its citizens will participate. If citizens are reluctant to participate, the core advantages of a smart city will dissolve. This article will identify and offer possible solutions to five smart city challenges, in hopes of anticipating destabilizing and costly disruptions. The challenges include privacy preservation with high dimensional data, securing a network with a large attack surface, establishing trustworthy data sharing practices, properly utilizing artificial intelligence, and mitigating failures cascading through the smart network. Finally, further research directions are provided to encourage further exploration of smart city challenges before their construction.

1. Introduction

It is the year 2027 and your day is full. As you finish your coffee and start to organize your desk to leave work, your boss tells you that you need to stay late. A quick moment of panic sets in, but you push past it and take action. In order to pick your son up from school you call an autonomous car with a quick swipe of your thumb and the service sends his smartphone the Quick Response (QR) code to access the car moments later. As you settle back into your chair, your son James walks out of school and into the autonomous vehicle school loading zone to find a shiny black autonomous car awaiting him with the air conditioning at his profile's preferred setting. Once you begin putting the finishing touches on the extra project, you half-consciously check in on James' journey via his smartphone's Global Positioning System (GPS) and see that he is leaving the food stop you approved in order to avoid a stern talking to by your spouse. The autonomous car app shows you that James' car was rerouted to avoid congestion on the highway and he should arrive at home shortly. Meanwhile, at home, the house smart systems kick into high gear in anticipation of James' arrival and change the temperature to make sure the air conditioning is used only when needed. With a dull buzz, your smartphone informs you that your son is picked up, fed, and comfortably sitting at home.

Considering the technologies mentioned all exist today, such a scenario is not far fetched. It is the seamless intersection of these technologies that seems so futuristic, and that is exactly what a smart city seeks to offer. However, it will be necessary to anticipate various security and privacy threats during the construction of smart city systems. For example, by completing the route from school to the home, intimate details about your child's schedule, preferences, and whereabouts are being provided to the service provider. The service provider now has stored information on what fast food James enjoys eating and what route he travels home, opening up numerous opportunities to make suggestions to James and his parents on where and what to eat. Furthermore, even if the service provider refuses to monetize the valuable behavioral data of its passengers, the opportunity for cybercriminals to gain access to this information is unsettling. Clearly, it would be worrisome to know that someone could gain knowledge of where your son goes to school and how to follow him home. In 2013, a group of researchers from the University of Texas at Austin were able to take control of an 80-million-dollar yacht in the Mediterranean by manipulating the GPS signals that the yacht relied upon for transportation; it would not be a stretch to suggest that a single autonomous vehicle could be remotely controlled with an unwitting passenger still in it (UT News, 2013). As technology becomes more embedded in our daily activities and city infrastructure, it is expected that new privacy and security concerns will emerge. The purpose of this article is twofold; first, it will survey existing privacy-preserving techniques that are applicable to the development of smart cities, and second, the article will identify research gaps surrounding smart cities and suggest avenues of future research.

First, it is necessary to establish a definition for a smart city. IBM states that the citizens and components of a smart city are "Instrumented, Interconnected, and Intelligent", or "IN3" for short (Elmaghraby & Losavio, 2014). Essentially, a smart city integrates

* Corresponding author.
E-mail addresses: trevor.braun@mail.mcgill.ca (T. Braun), ben.fung@mcgill.ca (B.C.M. Fung), farkhund.iqbal@zu.ac.ae (F. Iqbal), babar.shah@zu.ac.ae (B. Shah).

https://doi.org/10.1016/j.scs.2018.02.039
Received 9 August 2017; Received in revised form 19 November 2017; Accepted 28 February 2018
Available online 07 March 2018

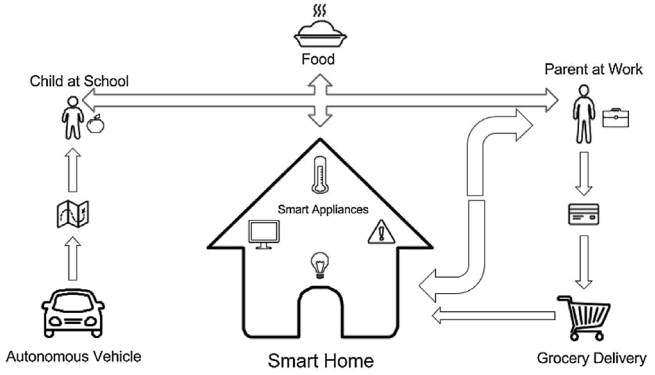

Fig. 1. An example of smart city interconnectivity.

smart technology in a manner that serves to increase efficiency, safety, and convenience. Current examples of cities that are incorporating smart city principles include New York, Toronto, Barcelona, Copenhagen, and Paris (Martinez-Balleste, Pérez-Martínez, & Solanas, 2013). For these cities and others looking to establish themselves as smart cities, addressing potential smart city privacy and security concerns before the infrastructure is in place will determine their success. In order for a smart city to offer increases in efficiency and the quality of urban life, citizens within smart cities must feel confident and secure enough to participate in the smart city. Without the citizens' interest, the smart city is obsolete. Therefore, fundamental security and privacy protections for the city's users are paramount to the success of a smart city (Fig. 1).

When anticipating smart city privacy and security challenges, it is important to realize that many of the same challenges exist today, albeit not as frequently as when these technologies become fully interconnected. Current deliberations and attempts to solve security and privacy challenges will lead the way to understanding how smart cities can be securely constructed. For example, the U.S. Supreme Court ruling on a major case involving smart technology set a legal precedent on how the U.S. government's GPS surveillance tracking could violate reasonable privacy expectations in a more serious manner than conventional surveillance (Elmaghraby & Losavio, 2014). In United States v. Jones, Justice Sonia Sotomayor updated the legal notion of privacy by contending that since GPS data can be collected in huge quantities at little cost and stored for data mining into the distant future, it posed an outsized privacy risk to society (Elmaghraby & Losavio, 2014). Thus, when considering GPS technology that will play a vital role in smart city transportation, rulings like those of the Supreme Court should be consulted and dissected to better anticipate future privacy concerns. Similarly, a smart city's security should no longer be conceptualized along traditional norms of physical security, but instead it should build off of current research surrounding cyber security and the Internet of Things (IoT). Also, when constructing solutions to potential smart city challenges, researchers should do so with an understanding of the various smart city stakeholder groups and the trade-off between a smart city's effectiveness and its security.

This article will be arranged as follows. Section 2 poses five questions regarding potential security and privacy challenges in a smart city, and offers some possible solutions. These questions will be broad in scope in order to properly address the fundamental challenges that increased interconnectivity and data driven computer decision making pose to inhabitants of a smart city. Section 3 outlines the "cascading effects" of how the aforementioned issues could impact life beyond their primary effects. Lastly, Section 4 outlines areas of research that will help further the effort to provide secure smart cities.

2. Security and privacy challenges

Throughout this paper, expectations of security and privacy will center around the following ideas. Security as a concept is not absolute, but it is a dynamic, genuine attempt to prevent harm to the smart city and its inhabitants, both directly and indirectly, through digital and physical connections. The security challenges discussed in this paper will mostly involve the abundant opportunities for security corruption within a smart city framework. When it comes to privacy, Elhaghraby and Losavio's first two general principles regarding privacy and cyber privacy are helpful. They state that (1) "activities within the home have the greatest level of protection", (2) "activities that extend outside of the home depend on *reasonable expectations of privacy*" (Elmaghraby & Losavio, 2014). The identified smart city privacy challenges will mostly revolve around what constitutes 'reasonable expectations of privacy' and the appropriate level of privacy protection necessary for inhabitant participation in the smart city. This paper will focus on the following five questions regarding potential privacy and security challenges in a smart city.

To solve the aforementioned privacy and security challenges facing smart cities, stakeholders must address issues holistically in order to make sure that the challenges will not continue plaguing the rest of the smart network. To do so, security professionals and smart city planners should utilize projects and current cities that simulate a smart network. An example of an IoT infrastructure project can be seen in Santander, Spain called SmartSantander (Ijaz, Shah, Khan, & Ahmed, 2016). SmartSantander is made up of over two thousand IoT devices mimicking an urban environment with the intention of developing a smart network with experimentation support and service provision (Ijaz et al., 2016). Experimentation support allows researchers to put their theories to the test in a real life scenario and service provision allows SmartSantander to provide services to people described in the form of use cases (Ijaz et al., 2016). Thus, projects such as SmartSantander are a useful resource for testing solutions and corroborating theories surrounding smart city security and privacy challenges.

2.1. Privacy threats in data sharing and data mining

How do we ensure personal privacy throughout a smart city that relies on rapid data sharing and data mining techniques with multiple stakeholders?

By nature of smart city interconnectivity, data will be transferred and utilized throughout the smart city processes, with multiple parties communicating and gaining access to information. From the makers of the smart sensors, to the city's transportation authority, to individuals accessing the smart city through their smartphones, each organization contributing to the smart city will uniquely use and handle data in ways that may endanger personal privacy. Furthermore, since each smart city stakeholder will have different priorities, there will exist gaps between the different stakeholders' privacy standards. There are already currently disparities in privacy standards between the private and public sectors based on the unique purposes that those two sectors serve. Businesses make risk/profit evaluations when deciding on how much privacy protection is enough (Basi, 2016). The goal of businesses is to make profits by offering products or services, so companies will offer just enough privacy protection to ensure that their brand is not tarnished and customers continue to buy their products (Basi, 2016). On the other hand, public sector organizations like health care providers or transportation authorities run critical services for the benefit of the public (Lum, 2016). The public sector will most likely have a more ambitious scope of what constitutes privacy protection, but its funding and livelihood will not be directly tied to its success in achieving privacy protection, unlike the private sector. This gap in protection will be no different in smart cities, but it will come with higher stakes. For example, health care in a smart city might rely on seamless partnerships

between public and private industry. While a public hospital may administer care on sight and be a central decision maker, the distribution of patients and medicine between facilities may be more efficiently achieved through a private sector partnership. In such a scenario, sensitive information regarding a patient's condition, treatment schedule, and home address will need to be transferred and analyzed by the relevant parties.

This process of data transmission between multiple organizations for a common purpose often results in techniques called data mashup and data integration. Data mashup refers to the simple joining of two or more data sets with a common subject of interest, while data integration joins multiple datasets in a manner that alters the existing data. In a smart city environment, privacy preserving high-dimensional data mashups will allow multiple parties to share and access pertinent data without compromising individual privacy. However, current practices of data mashup have their own challenges. Fung et al. (2012) explain three privacy problems that occur with high-dimensional private data mashups. First, by combining together multiple private data sets, the resulting data set would reveal more sensitive information to the other data providers. Second, the integrated data set could make identification of individuals easier by providing more data points for re identification. For example, simply knowing that a 30-year-old lawyer has leukemia does not quite help a malicious actor determine which patient has the cancer, but knowing that a 30-year-old lawyer born on April 2nd in Burlington, Vermont has leukemia could be traced back to a single name. Third, mashup data from multiple sources may contain so many data attributes that traditional privacy models, like K-anonymity (Samarati, 2001; Sweeney, 2002a, 2002b), would render the protected data useless for analysis. The K-anonymity privacy model takes a dataset with multiple attributes and then generalizes certain values within these attributes to obscure individual identifiers without compromising the information utility for classification analysis (Mohammed, Chen, Fung, & Yu, 2011). For example, instead of displaying that a 30-year-old lawyer from Burlington, Vermont has leukemia, the dataset can be generalized for that entry to indicate that a 20–30-year-old professional from Vermont has leukemia. Yet, when a data set, such as those in smart cities, includes a high number of variables that can identify an individual, generalization methods become so broad that they make the transformed data unusable for analysis. Also, partition-based privacy models such as K-anonymity are vulnerable to privacy attacks, including deFinetti attacks (Kifer, 2009), composition attacks (Ganta, Kasiviswanathan, & Smith, 2008), and foreground knowledge attacks, where the attacker has some background knowledge of the individuals in the data set (Chen, Fung, Desai, & Sossou, 2012).

Smart cities cannot rely on traditional privacy-preserving methods when regulating or partaking in data mashing. Furthermore, when anticipating privacy attacks, assumptions of an adversary's knowledge can be harmful for privacy security. Thus, when considering methods for preserving individual privacy in smart city data sets, the concept of differential privacy (Dwork, 2006) should be considered. Differential privacy has been regarded as one of the strongest privacy models because it empirically guarantees privacy regardless of an attacker's background knowledge and computational power (Dwork, 2006). Simple aggregation and generalization techniques with K-anonymity are not effective in preserving high dimensional data sets. Data aggregation can be helpful to prevent eavesdropping and traffic analysis on smart utility meters (Rebollo-Monedero, Bartoli, Hernández-Serrano, Forné, & Soriano, 2014). Confidential information can be extracted from smart utility metering devices that could record precise measurements with timestamps, such as electricity, heat, or internet consumption (Rebollo-Monedero et al., 2014). As this utility information travels through smart city channels, there is a risk of it being intercepted and leveraged to deduce confidential information.

Another way to address the privacy issue of high-dimensional data is to conduct analysis on a reduced number of attributes, implying that a preprocessing step of selecting attributes is required. The challenge is that the feature selection process itself may cause privacy threats. Thus, there is a line of work (Matatov, Rokach, & Maimon, 2010; Pattu, Kantarcioglu, Ulusoy, & Malin, 2015; Zhang, Mohammed, Dave, & Hasan, 2017), focusing on reducing selecting a set of relevant attributes in a privacy-preserving manner.

Privacy-enhancing technologies

In order to properly address the challenges of preserving individual privacy in the smart city environment, the level of privacy should be quantified and mapped (Rebollo-Monedero et al., 2014). This way, researchers and engineers can know where certain technologies and processes stand in terms of privacy protection. This can be achieved by utilizing measures of uncertainty, information, and the attacker's estimation error and diversity (Rebollo-Monedero et al., 2014). For uncertainty, Shannon's entropy, a statistical tool that evaluates the uncertainty of a random event with respect to the probability distributions of possible outcomes, can serve as a helpful indicator for understanding the privacy of communications (Rebollo-Monedero et al., 2014). The latest privacy-preserving techniques should satisfy the standard of differential privacy, or similar semantic privacy model, in order to properly protect smart city inhabitants. The model of differential privacy makes no assumptions about an attacker's knowledge and provides a quantifiable level of privacy protection (Mohammed, Alhadidi, Fung, & Debbabi, 2014). Once privacy risks are mapped and measured, it is crucial for organizations within the smart city to effectively communicate with one another in order to better protect privacy as information travels throughout the network. Public sector organizations need cybersecurity and cyber privacy professionals with good communication skills, vendor understanding, and business analysis skills (Lum, 2016). With such professionals, public sector organizations will be able to effectively partner with private sector companies on privacy matters that are in the public interest.

It is helpful to combat broad privacy challenges with privacy frameworks. For example, data privacy professionals can choose between interactive and non-interactive privacy frameworks when tailoring privacy techniques. Interactive frameworks allow data miners to privately access databases where the database owner releases custom relevant information, while non-interactive frameworks anonymize the data sets and allow private or public access (Mohammed et al., 2014). Data as a Service (DaaS) providers may use mashup models to integrate multiple database owners by using non-interactive frameworks (Khokhar, Fung, Iqbal, Alhadidi, & Bentahar, 2016). In terms of overall network privacy, the W3 and 3D privacy models attempt to provide a framework for protecting the entire system. The W3 privacy model for location-based services seeks to protect three aspects of personal privacy: where, what, and who (Martinez-Balleste et al., 2013). The model seeks to protect an individual from location tracking, systems learning what a user is doing, and invasive identification efforts. This can be accomplished through location obfuscation techniques, private information retrieval techniques, and temporal pseudonyms, respectively (Martinez-Balleste et al., 2013). The 3D privacy model splits privacy into three dimensions: respondents, users, and owners (Martinez-Balleste et al., 2013). Thus, the model is constructed such that respondent privacy is focused on avoiding individual re-identification, user privacy guarantees a user's query privacy, and owner privacy seeks to protect a database owners privacy from those querying (Martinez-Balleste et al., 2013).

In terms of technical privacy solutions, there are several important techniques. First, intelligent data aggregation techniques should be used when possible to minimize the amount of raw personal data being transmitted in the smart network (Bartoli et al., 2011). If aggregation techniques can be integrated into smart devices throughout the network (when raw personal data is not needed), this could both increase device decision making efficiency by decreasing used storage space and simplifying data, and decrease the amount of personal information traveling throughout the smart network. For passenger flow analysis, trajectory data can be anonymized in a manner that does not diminish

the data's usability. Ghasemzadeh, Fung, Chen, and Awasthi (2014) describe a method where a passenger flow graph is extracted from the raw dataset, serving as a benchmark for the raw data's explanatory power. Then, the data is anonymized in a manner that minimizes the difference between the new flow graph and the raw flow graph (Ghasemzadeh et al., 2014). Chen et al. (2012) presented a method to achieve differential privacy with the Montreal transit system's (STM) data by adopting an efficient data-dependent approach with a hybrid granularity prefix structure that can also be used to effectively transmit and learn from transit data. In situations that feature two organizations who need to collaborate for business reasons, but do not generally want to reveal more than the necessary information, the semi honest adversary model is fitting. This method from Mohammed et al. (2014) uses the rigorous basis of differential privacy on vertically partitioned data in a two party setting where the organizations may be potential adversaries. More general privacy techniques include location cloaking and effective key management for crypto security (Bartoli et al., 2011; Martinez-Balleste et al., 2013).

2.2. Privacy threats in mashup data

Data integration and data mashup in a smart city increase the digital surface in a way that provides more opportunities for security breaches. How will this challenge be overcome?

Since a smart city is actually a well connected system of technologically intelligent objects, smart city security is inherently more difficult than securing individual smart objects, such as smartphones, IoT objects, and service platforms. All the individual objects' vulnerabilities pose an alarming risk to the security of the smart city when connections between these objects are relied upon to make the city truly 'smart'. This phenomenon increases the smart city's attack surface by giving potential attackers a vast landscape to compromise the smart city. With access to the smart network, hackers can methodically collect information about the security posture of organizations operating in the smart city (Sen, Dutt, Agarwal, & Nath, 2013). For example, if a network relies upon a secure connection to a smartphone, a secretly compromised smartphone could use the secure connection for malicious purposes. It is for this reason that the sum of the individual vulnerabilities will be higher than each of the dependent systems (Bartoli et al., 2011). This poses difficulties because of the aforementioned necessity for security in a smart city, without which inhabitants would be reluctant to participate.

Smartphone vulnerabilities that could compromise smart city security include malicious smart applications, botnets, location and gps, spyware, threats from social networks, Wi-Fi, and Bluetooth (Ijaz et al., 2016). Ijaz et al. (2016) state that "[s]mart phones are one of the core component[s] of IoT infrastructure in a smart city as they give access to various services and smart applications [and] are also the main source of peoples' role in a smart city." Attackers may upload malicious smart applications onto an unsuspecting user's phone in order to infect the device that serves as a connection to the smart city (Ijaz et al., 2016). If an attacker is able to infect multiple smartphones, he may form a botnet that can launch simultaneous attacks on the smart network (Ijaz et al., 2016). A smartphone user's privacy and security could be compromised by compromising the GPS features available in smartphones, much like the previously mentioned 80-million-dollar yacht manipulated by researchers (Ijaz et al., 2016). Spyware can be used to listen to a user's conversations or gain access to their sensitive information. Such attacks could occur through the internet, over unsecured Wi-Fi connections, or unconsented Bluetooth connections. Furthermore, social media websites that house a smartphone user's personal information may be subject to attack or manipulation when used as a personal identifier in a smart city (Ijaz et al., 2016).

While smartphones connect users to the smart city, the network will also rely heavily on machine-to-machine (M2M) communication which will automate many processes within the smart city. Machine-to-machine communication may take place after smart object sensors cross a threshold value or after receiving signals from another device. Smart devices that engage in machine to machine communication can pose a risk to smart cities because of security concerns such as physical attacks, attacks on authentication tokens, protocol attacks, threats in network security, breaches in privacy, and configuration attacks (Ijaz et al., 2016). Physical attacks using compromised M2M communication can be executed through configuration attacks utilizing malicious software to commit fraud by manipulating the integrity of existing M2M software and associated data (Ijaz et al., 2016). Authentication tokens that grant certain machines access to the smart network can be cloned and used to infiltrate the network. Threats in network security, like device impersonation and Denial-of-Service (DoS) attacks, between smart devices can either infiltrate or disrupt a smart network, respectively. Protocol attacks occur mainly against devices, such as man-in-the-middle, OAM, and denial-of-service (DoS) attacks (Ijaz et al., 2016). All of these attacks disrupt fast, automated communications between smart devices which make rapid access to information possible in a smart city.

Another security challenge in a smart city comes from the vulnerabilities of radio frequency identification (RFID) tags, which are used in several potential smart city sectors including smart environment, smart industry, and smart mobility (Ijaz et al., 2016). RFID, or similar technology, has helped improve real-time information visibility and information traceability, but it is also prone to attacks and threats that diminish its security posture (Ijaz et al., 2016). RFID tags are susceptible to unauthorized access requests that allow the perpetrator to gain access to sensitive information, a fact that undermines data confidentiality and privacy (Ijaz et al., 2016). RFID tags can be intercepted by an RFID reader that produces the correct Electronic Product Code (EPC), and attackers who gain access to RFID readers or an EPC can intercept and read confidential tags (Ijaz et al., 2016). RFID corruption can be achieved through tag killing, tag cloning, signal interference, jamming, denial of service attacks, and eavesdropping (Ijaz et al., 2016). In each situation an attacker can disrupt the frequency and guide the message away from the intended receiver. Since RFID technology is already being used for several potential smart system components, security vulnerabilities of this technology must be addressed.

Finally, smart city security challenges go beyond the individual technological vulnerabilities. Economic pressures from limited city resources can hinder security efforts, especially since smart cities have very dynamic security challenges that may evolve and multiply over time (Sen et al., 2013). Patching a structurally insecure system will prove very costly in the long run, so security investments should go towards preventative measures that increase security across the entire system. Security teams must pay particular attention to attacks that have the intention or ability to disrupt the entire smart city network. Denial of service (DoS) attacks are the kind of blunt, broad, crippling attacks that are designed to shut down a smart city (Bartoli et al., 2011). Special attention should go to such attacks in order to prevent widespread devastation.

Systems security hardening

To effectively counter an ever increasing cyber attack space throughout the smart network, smart cities must move beyond patching issues that arise and instead implement models that structurally secure the network. Helpful security models include a layered approach and the 3-layer onion model. The layered approach features a system where all smart network devices have a unique identifying number and they operate within three layers of security: data protection application for the server, data scrutiny layer, and secure smart software for devices (Sen et al., 2013). The data protection application for servers would review data being exchanged between servers and the rest of the network in order to catch any malicious information that could corrupt the server (Sen et al., 2013). Thus, this layer serves as a policing force to identify malicious content in the network. The data scrutiny layer

shields servers from direct communication with the smart network and acts like a firewall to protect servers from any corrupting presence in the smart network (Sen et al., 2013). The secure smart software for devices layer attempts to prevent malicious software from entering the smart network in the first place by making sure that individual devices are not infected (Sen et al., 2013). In this way, the layered approach aims to provide multiple layers of security around the servers that control the smart network. The 3-layer onion model for smart city security aims to provide services and secure data acquisition in compliance with privacy and security laws (Khan, Pervez, & Ghafoor, 2014). The onion layered approach is comprised of three layers: governmental control domain, smart city inhabitants/infrastructure, and service providers (Khan et al., 2014). The governmental control domain layer acts as a regulatory body with its main goal being smart network compliance to regulations and policies (Khan et al., 2014). The smart city inhabitants/infrastructure layer authenticates and validates users within the smart network in order to secure the privacy and security of the inhabitants from malicious tampering (Khan et al., 2014). The service provider layer focuses on service provisioning and securing data sharing amongst trusted and untrusted domains (Khan et al., 2014). This layer allows service providers to utilize smart city data in the hopes of increasing efficiency and the quality of life within the smart city without compromising security and privacy (Khan et al., 2014) (Fig. 2).

Along with the need for security models comes the perhaps obvious, but often overlooked, necessity of testing security equipment. The same concept applies in smart cities. Cesar Cerrudo, the CTO at the security research firm IOActive Labs, has pointed out that governance authorities often do not test the security systems they purchase for their constituents (Ijaz et al., 2016). This seemingly fundamental step needs to be undertaken in order to ensure proper network security. System security testing should be undertaken before implementation of devices, but it should also be done continuously with the help of outside and internal security consultants (Creery & Byres, 2005). This will allow white hat hacking teams to find security deficiencies before a malicious actor potentially saving the smart city and its inhabitants from privacy and security intrusions. Similarly, ordinary people operating inside the smart network need to be incentivized or motivated to report cyber intrusions when they encounter them (Freyssinet, 2016). By continually assessing a smart city's security posture and employing an effective security model, the probability of cyber attacks will decrease.

Along with macro level security, there are some security techniques that will aid in combating smart city attackers. Smartphones operating within the smart network can be further secured through anti-virus programs, firewalls, secure APIs, authentication control, filters, and cellular M2M solutions (Ijaz et al., 2016). Anti virus software, filters, and firewalls will scan and protect smartphones from malicious

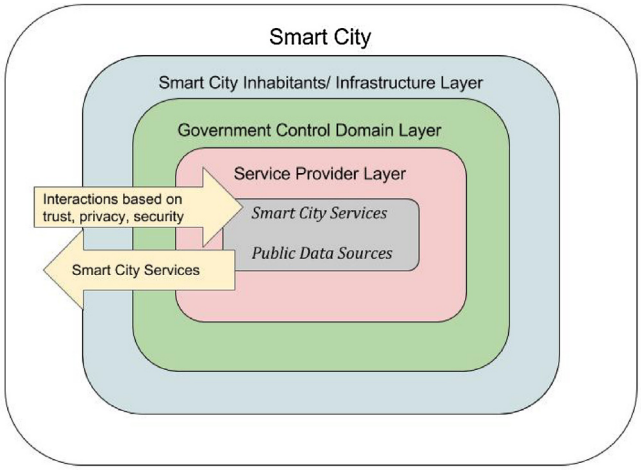

Fig. 2. 3-Layer onion model.

malware that could potentially spread throughout the smart network (Ijaz et al., 2016). Secure APIs provide a secure cryptographic method of running applications that connect to a smart network (Ijaz et al., 2016). Authentication control will add a layer of security by requiring users seeking to connect to the smart network to possess the right credentials (Ijaz et al., 2016).

Machine-to-machine security solutions include several Institute of Electrical and Electronics Engineers (IEEE) mechanisms that can help secure a smart city. The IEEE standard mechanisms include IEEE 802.15.4, IEEE 802.15.1, and IEEE 802.15.11 (Ijaz et al., 2016). IEEE 802.15.4 examines smart objects' power management, energy detection, and link quality in order to assess security threats (Ijaz et al., 2016). IEEE 802.15.11 helps secure Wi-Fi through the Wi-Fi Protected Access (WPA) security protocol, and IEEE 802.15.1 is used in Bluetooth (Ijaz et al., 2016).

RFID security challenges revolve around the ease with which radio frequency tags can be manipulated. A solution to interception of RFID packets known as tag sleeping allows the RFID tag to be 'put to sleep' temporarily (Ijaz et al., 2016). Other techniques such as minimalist cryptography, re-encryption, and the relabeling approach will help secure RFID transmission as well. RFID interference can be dealt with through custom data coding, multiple re transmission, and a data integrity check (Ijaz et al., 2016). For increased authentication, security Hash Lock and Hash Link techniques utilize symmetric key distribution, which is necessary during the authentication procedure (Ijaz et al., 2016).

Preparedness and testing are the keys to maximizing the security of a smart city relying on data mining methods. When it comes to preparedness, the security personnel of a smart city should start by understanding the security risks of their city. This means mapping and quantifying the risk picture dependent on the city's stakeholders and technology. Furthermore, security personnel need to have a plan contingent on an attack against the smart city. This means crafting a plan that responds to a variety of potential incidents, and it should be personalized for commercial and public organizations (Bartoli et al., 2011). Various tools can be used to heighten the security posture of the smart network and the systems comprising it. Smart cards that replace individual passwords for authentication could secure the systems from social engineering and careless password mistakes (Igure, Laughter, & Williams, 2006). New firewalls developed by companies like Cisco can help filter information securely (Igure et al., 2006). Also, micro-firewalls that are embedded in each smart devices could protect components of the smart network from infection which could spread throughout the system (Igure et al., 2006). Furthermore, security solutions from previous sections will all contribute to securing the network from cyber attacks, which means that digitally connected physical systems would also become harder to hack. The best way to put cybersecurity tools and models into effect is through testing and constantly trying to find the vulnerabilities within the system. This method helps the smart city stay ahead of the malicious forces attempting to break in. By rewarding external bug researchers adequately, the city will actually save money on security related issues because of the immense damage a successful attack can cause. University of California Berkeley researchers found that rewarding external hackers for finding vulnerabilities was up to 100 times more cost effective than not (Enterprise, 2016). Therefore, testing not only gives the city an edge, but also makes the smart city more financially viable.

2.3. Cloud security

What happens to data collected in a smart city? Where is the data collected (different cloud storage methods)? How is it secured from cyber attacks? Who is responsible for data breaches? When is it disposed of? Will people be able to truly remove personal data once it is collected?

Smart cities will feature countless smart devices, each of which will

be communicating with the smart network by sending, copying, and processing data. This process will generate an immense amount of data, some of which will be confidential and should be secured. In order to store such large amounts of data, it is likely that smart cities will utilize cloud services. Cloud services can be obtained from multiple companies, and three varieties include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (Apprenda, 2016). SaaS, the largest and fastest growing cloud market, uses the internet to provide third-party applications to customers without those customers having to run and install applications on their own computers (Apprenda, 2016). PaaS is for applications, in order to provide cloud services to software (Apprenda, 2016). This means that developers can create software that can then be easily scaled up through cloud computing to meet rising demand, like software in a burgeoning smart city. IaaS provides remote data center infrastructure access, monitoring, and management by creating a model that users can pay for based on their usage instead of having to set up their own system (Apprenda, 2016). These cloud services, along with cloud data storage, will help smart cities avoid limitations imposed by computing power and physical memory, but they will also pose some challenges. Cloud services complicate an already difficult security and privacy picture for utilities that would be involved in creating smart grids (to optimize energy distribution) in a smart city (Ijaz et al., 2016). Farming out data services adds additional breach points, with cloud service providers further complicating matters by adding additional standards and practices for privacy and security.

Furthermore, with cloud service providers handling massive amounts of confidential information, legitimate questions surrounding responsibility and consent in a smart city arise. Are users' privacy violated when smart cities allow third parties to store, handle, and manipulate raw confidential data? The challenge here is an ethical and most likely legal one, but it is also a challenge for efficiency and reliability since data sharing and storage is crucial for a well functioning smart city. Also, who would ultimately be held responsible for a successful data breach in the cloud storage system? It will not be possible to thwart all potential cyber attacks, so when one does occur, can a cloud service company be held fully accountable? This question is relevant because such a high degree of risk paired with a strong punishment would make it difficult for cloud service businesses to stay viable. Cloud service financial and legal viability is important for the smart city to function efficiently and to make future technological growth possible. Thus, responsibility for data security will need to be shared with the government in a manner that incentivizes businesses to stay viable and provide the maximum amount of cloud security.

Data management extends beyond cloud services or government organizations, in fact, each device contributing to the smart network will be storing and handling data. As objects communicate with the smart network, the relevant data sets may be duplicated and stored locally in order to maximize the smart object's response time (Sen et al., 2013). While storage times of local copies vary depending on the smart object's purpose, it does raise questions surrounding smart object data management. If smart objects, such as smartphones, sensors, or scanners, keep local replicas of sensitive data, they can be breached, especially if they are physically accessible. This may be problematic for privacy advocates if the data replicas are made without transparency or consent of the user. It may seem unlikely, but if an inhabitant's privacy was violated because a scanner was compromised, the perceived safety of the smart city will decrease. The same can be said of smart networks that store personal data indefinitely. If personal data is used in perpetuity without transparency, smart city users may either resist using the services or call for reactionary government intervention. Europe has already begun entertaining the idea that people have the right to be forgotten on the internet and similar questions will surely arise for smart cities.

Data management and policy compliance

Data management is a very important task in a smart city because the production, transmission, and mining of data is what makes a smart city more efficient and convenient than an ordinary city. However, the volatility of cyber security puts the data centric smart city in a precarious situation. When critical services and infrastructure are digitally connected and data dependent on the smart network, the risk of cyber attacks becomes much more dangerous. Thus, if a smart city decides to utilize private sector cloud services the private entity must be held to higher than normal private sector standards. Since privacy protection and security are paramount for the viability of a smart city, companies that manage a smart city's data must be incentivized and/or regulated in a manner that aspires to these goals. Therefore, a careful balance must be struck between company liability for privacy and security breaches and limiting the amount of risk a company needs to take in order to remain financially viable. This way companies will strive to uphold security and privacy goals, but not fear the repercussions so much that they are disincentivized from providing cloud services.

It is also important to construct a regulatory apparatus that can nimbly identify wrongdoing without imposing a high burden on private sector companies contributing to the smart city. Organizations within the smart city should take initiative and ensure their own compliance with laws before a regulatory authority has to step in. One way of doing this is through *Law-as-a-Service* (*LaaS*) which is an emerging service for ensuring businesses and organizations are compliant with legal policies (Khokhar et al., 2016). Such services would help heighten data security and ensure that companies were following data handling laws. Organizations should also be incentivized and/or regulated to win the public trust. This would call for business practice transparency when dealing with personal data. If inhabitants could easily find out how their data was being utilized, it would surely increase public trust in the smart network and incentivize organizations to make ethical decisions. Transparency should include timelines for data usage in the smart network. This practice can either be standardized across the entire smart network or by sector. Timelines should include details on data disposal dates, data duplications, and data storage.

2.4. Secondary use of collected data

What can collected data be used for? Can personal data from the smart city and the conclusions drawn from data mining techniques be used commercially? Can consenting individuals provide data that then affects non consenting individuals?

While it is obvious that data will be collected and utilized in a smart city, it is a different question entirely whether data always should be collected. It is generally accepted that if an individual consents to provide their personal information for a specific purpose, say health data, then it is ethical for the health care provider to accept the patient's personal data. However, in situations where personal data is utilized in a secondary manner that does not directly benefit the data provider, the ethical implications are far less clear. For example, it is unclear whether privacy would be violated if smart city organizations monetized the personal data they collected. While present day companies already monetize personal data they collect, many of these services are not unavoidable aspects of daily life. If in a smart city a private company was contracted to perform a fundamental smart city task, it would become an unavoidable presence in the smart city, one that inhabitants would have no choice but to submit to. If ambulances in a smart city were operated by a ride hailing company with autonomous vehicles, sick individuals would not have the power to deliberate the company's privacy practices before riding to the hospital. Thus, monetization of personal data should be thoroughly examined if it is undertaken by a fundamental organization in a smart city.

Another question that points to potential privacy and security challenges in a smart city is: can data from consenting individuals negatively affect non consenting individuals? For example, consumption profiling occurs when organizations collect enough data to determine,

with some degree of certainty, that certain characteristics indicate a certain type of customer. The same could be done to inhabitants of a smart city by analyzing their locations, buying patterns, and personal information to implement discriminatory pricing (Rebollo-Monedero et al., 2014). While this practice already occurs daily on the internet, if it occurred in a smart city it would be an inescapable part of life that could artificially produce different experiences within the smart city. This practice becomes further complicated if the individuals consensually providing their data are compensated for doing so and essentially profiting from the detriment of others.

Social media continues to play a large role in human interactions and it will most likely be used to facilitate social interactions within the smart city. If social media accounts are used to verify or interact with certain smart city services, privacy concerns will inevitably arise when social interactions are combined with official conduct in a city. Should government organizations have access to inhabitants' social media profiles for a more socially integrated city experience, or is this one step closer to domestic spying? Also, social media accounts yield a wealth of information about a user, data that would give an organization within the smart city a breadth of information (Ijaz et al., 2016). This may be problematic if social media integration is an unavoidable step to participating in a smart city service. As far as security is concerned, social media is far from perfect when it comes to verifying identities in a secured network. On the other hand, biometrics would provide a high level of security for a smart city. Biometrics recognize and identify people based on their biological and behavioral characteristics (Ijaz et al., 2016). According to Bill Maheu, the senior director for Qualcomm Government Technologies, biometrics could mostly solve the 3.7 trillion dollars lost in global frauds every year (Ijaz et al., 2016). However, the practice of storing intimate facial and body characteristics could be a serious privacy violation if done incorrectly. There is perhaps no information more personal than one's facial composition. Therefore, securing the smart city through such effective means will be elusive without proper implementation.

Preserving citizens' trust

Solutions will focus on preserving the trust of smart city inhabitants that is so important to sustaining the smart city. Smart city users will interact with the smart network when their personal threshold of privacy and security is achieved. In order to satisfy most citizens, the smart city should work to establish computational trust within the network. Computational trust refers to trust levels surrounding interactions in information technology, and it is crucial to facilitate interactions and cooperation through digital mediums. Establishing computational trust within the smart network will provide the necessary assurance for peer to peer interactions and incentivize all parties to abide by the laws of the smart city (Sabater & Sierra, 2005). Current computational trust and reputation models can serve as models for securing user confidence in the smart network. Ratings systems can play an important role in incentivizing users to treat each other with respect by holding individuals' reputation's accountable for their actions. Businesses that rely on effective peer-to-peer interactions, like Uber and Lyft, already demonstrate the feasibility of using ratings in a digital network. Essential services should be distinguished by the city's government on the smart network, so that citizens can identify official sources of information. To quell citizen's concerns over their personal data being further used without their consent, the network may seek to ensure there is public record every time a new organization gains access to personal information. Novel software that creates an environment within which data analysis can occur without allowing organizations to extract said data would allow smart cities to facilitate what organizations have access to the sensitive data. As mentioned in the previous section, transparency will be important for fostering trust and confidence in the smart network. Data timelines and clear parameters for data privacy and security consent will allow users to understand how their data is used and it will incentivize organizations to better serve their customers. Definitions of data consent will need to be decided through democratic means. For example, the frequency with which individuals providing data need to indicate that they consent to their data being used for secondary purposes should be decided by the inhabitants of the city, state, or country through democratic means. If possible, a sliding scale of consent could be implemented, where a user can customize the amount of data they wish to provide the company, or a specification of what their data can be used for. Organizations utilizing this data should also incentivize users that are submitting personal data when that data is used in a secondary manner to provide business intelligence. For example, subscribers to a ride sharing service could be offered a percent discount if they allow the service provider to use their personal information securely for business intelligence purposes. This way organizations receive consent and users feel compensated for the extraction of their personal information. With respect to biometrics and securing the extremely personal physical details of a human body, advanced video surveillance techniques can help in doing so. Real-time computer vision techniques can be employed to detect biometric areas of interest and protect the data generated from outside intrusions (Martinez-Balleste et al., 2013). Ultimately, with biometric technology the limits to biometrics and identifying what constitutes an invasion of privacy must be decided democratically and transparently.

2.5. Threats of artificial intelligence

How will data mining, machine learning, and artificial intelligence (AI) systems in a smart city affect the city's physical safety? To what extent can data and data mining techniques dictate the security of a city?

Smart city security often revolves around cyber threats, but it is important to note that these cyber threats pose serious problems for physical security as well. Even though there are many cyber threats to focus on, these threats can turn into physical danger in a smart city that relies on digitally connected infrastructure, sanitation systems, and healthcare. This can already be seen in current digitally connected infrastructure. In April of 2016, a German nuclear power plant was found to have infected computers that worked with moving nuclear fuel rods (Bosco, 2016). Those computers were isolated from the internet, but this instance is only one of many examples of how cyber threats could translate to physical damage. In a smart city that relies on seamless connections between physical objects, the potential for turning cyber attacks into physical attacks is real. For example, attacks on the smart energy grid would have immediate wide ranging implications on the city. If a DoS attack caused the smart grid to fail by denying network availability to customers, critical services like healthcare and transportation could be disrupted, potentially causing chaos and even death. Such vital smart city systems must be better protected than their present day counterparts; in 2016 the cybersecurity company RedTeam fully compromised a U.S. power company in 24 h (Khan et al., 2014; Szoldra, 2016).

In order to understand the potential physical threats to a smart city, an examination of current industrial systems that rely on remote sensing and computer decision making is helpful. An especially vulnerable type of industrial system is Supervisory Control And Data Acquisition (SCADA) networks (Igure et al., 2006). SCADA networks currently include industrial facilities that could foreseeably be part of smart cities, such as chemical factories, electric power plants, manufacturing facilities, and oil refineries (Igure et al., 2006). These networks utilize remote sensors, computers, and actuators to remotely control industrial plants (Igure et al., 2006). Such systems are a precursor to smart cities, which go beyond infrastructure intraconnectivity and actually digitally connect infrastructure to other city systems such as transportation. However, such powers may be used for nefarious purposes if an attacker gains control of the system. Attacks on SCADA systems have escalated since the early 2000s with 70% of security incidents originating outside of the SCADA network since 2001 (Igure et al., 2006). SCADA networks are prone to worm attacks that regularly inflict over one million dollars

in damages (Creery & Byres, 2005). One of the reasons that SCADA systems are so prone to cyber intrusions is the fundamentally insecure nature of the initial SCADA design process. When SCADA systems were initially designed and built, performance and functionality were the primary objectives, with security concerns being an afterthought (Igure et al., 2006). Even the commercial off-the-shelf software that SCADA systems use is notoriously insecure and an easy target for attacks (Igure et al., 2006). Part of the reason that SCADA systems are not rigorously secured is the misconception that SCADA networks are electronically isolated from other networks, thus making them unreachable to hackers (Igure et al., 2006). However, this is not the case. SCADA systems include sensors that require interconnectivity and those smart objects can be compromised. In fact, SCADA systems and the automation industry have moved away from proprietary standards for SCADA communication and on to open international standards (Igure et al., 2006). This makes it much easier for hackers to learn about SCADA systems and identify their vulnerabilities. Once hackers identify the SCADA network's weaknesses, they can cause sensors to react at arbitrary levels or turn off sensors entirely, leaving any emergency situation undetected (Igure et al., 2006). Some common SCADA attack techniques include viruses through Virtual Private Network (VPN), SQL injection, buffer overflow, and device threshold manipulation (Zhu, Joseph, & Sastry, 2011). Smart cities should learn from the security challenges fundamental to SCADA systems by implementing design techniques with an emphasis on security.

A smart city will rely on automation for peak efficiency, and artificial intelligence will be crucial for implementing automation in a versatile manner. Everything from connecting users to emergency services when they are in distress, to identifying malicious behavior within the smart city network, will rely on artificial intelligence to identify problems and implement solutions at speeds surpassing human ability. However, the natural question arises, what if the artificial intelligence system is compromised? Without a proper contingency plan, a smart city controlled by a malicious actor could put citizens and infrastructure in danger. For this reason, it is important that smart cities utilize artificial intelligence for seamless service, but also retain a human overseer in case emergency measures need to be deployed. If a human overseer sees the system acting in a manner that endangers the smart city, they should be able to suspend the harmful actions or override the artificial decision maker. In order to ensure the smoothest possible transition, security officials should develop a contingency plan that includes manually running critical services, identifying the problem, and restoring the artificial decision maker under strict supervision. Furthermore, artificial intelligence should be utilized to better identify irregular behavior and determine whether or not it is the result of malicious activity. Training neural networks on malicious and routine behavior will help smart cities identify attackers far before human detection. While such techniques rely on historical data and thus can not perfectly predict future threats, they are nonetheless useful in identifying patterns suggesting irregular behavior and automating routine decision making at a higher speed than human personnel.

3. Cascading effects

Since a smart network is by definition interconnected, security and privacy issues occurring in one area of the network will have cascading effects throughout the system. Since privacy and security vulnerabilities are amplified by the smart city's interconnectivity, user confidence in the system can be more easily shaken. This is significant since, as mentioned before, user confidence in the system is necessary for smart city adoption and functionality. Without inhabitant's full participation in the smart network, smart cities cannot offer the desired increases in efficiency and quality of life. Also, the potential knowledge that smart cities can uncover, with their rich data sets and technological pioneering, would be lost. Furthermore, when the smart city is not secured, this means that essential services like public safety, government, healthcare, and infrastructure are not secured as well. This will pose a serious national security issue to any country whose smart city is compromised.

Interconnectivity between physical and cyber infrastructure in a smart city may cause disruptions in one area of the network to cascade throughout the smart city. A cascading failure in infrastructure is defined by Rinaldi, Peerenboom, and Kelly (2001) as when “a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently causes a disruption in the second infrastructure.” Cascading failures are not a new concept. In 2001, electrical power disruptions in California caused cascading failures in multiple industries dependent on readily available electricity. The disruptions affected the extraction, transportation, and refinement of oil, natural gas, water, and agricultural crops (Rinaldi et al., 2001). Disruptions to transportation fuels then cause further failures in industries and individuals who rely on it to perform essential functions. Thus, like in California, a disruption in a single component of an interconnected smart city network can have consequences beyond the initial failure. This makes physical and cyber security even more important in a smart city since the security of these systems affects the entire network. Identifying the severity, duration, and magnitude of cascading failure in a highly interconnected network is an important step in mitigating disruptions (Zimmerman & Restrepo, 2006). According to Kopylec, D’Amico, and Goodall (2007), IT crisis managers tend to focus on mitigating the cascading failure from cybersecurity breaches at the expense of holistically understanding cascading failures. Those who work to ensure smart city safety and minimize fallout should also understand how physical threats can affect cyber infrastructure. For example, areas prone to earthquakes should be cognizant of how natural disasters may disrupt a digitally interconnected smart city and develop contingency plans to minimize damage. In order to minimize cascading effects, risks and interdependence must be modeled and aggregated. Such measures are crucial for crisis managers who deal with a deluge of information flowing from a multifaceted smart city. Actor Network Theory (ANT) can aid security professionals analyze and visualize data in complex systems by utilizing “punctualization” (Kopylec et al., 2007). Punctualization compartmentalizes layers of a sophisticated network according to their purpose; power lines, electricity plants, conduits all exist to provide electricity, much like sewers, hospitals, and water filtration stations enhance public health. Smart city security officials can use punctualization to simplify data analysis and use historical data to better understand how failures cascade through the smart network. When aspects of the smart city fail, the data will be depunctualized at the failure points; if a sewage plant fails, it will become visible as opposed to hidden inside the public health layer. Kopylec et al. (2007) introduce the software *Cascade* as a user interface for understanding such interdependencies in a smart city and visualizing their connections with layered Global Imaging System (GIS) infrastructure. Finally, to address potential cascading failures in a smart city, stakeholders across public and private industries need to cooperate. Hurdles to information sharing, such as proprietary or classified information should be overcome by information sharing protocols or organizations that preserve privacy and security. Examples of modern information sharing, such as that in the telecommunication industry between the public National Communications System and the private National Security Telecommunications Committee should be used as a model for smart cities (Robinson, Woodard, & Varnado, 1998).

Therefore, the cascading effects of not securing the privacy and security of the smart city participants in the smart network are great and should be addressed before the smart city is built. If the challenges are not addressed in the planning stages, citizens will likely resort to reactive legal regulations that will ensure their own security and privacy. However, there is no telling whether these potential regulations would be overreaching or inadequate, which is why it should be a last resort. Furthermore, if privacy and security challenges are not addressed in the planning phase, the economic costs of securing the smart

city after the fact might be too high and unsustainable. Patching the system and securing the network in a reactive way will burden city budgets and introduce fiscal instability to the planning process. Without a secure system and an unstable financial environment, key businesses that would otherwise strengthen the smart city will not be able to confidently invest in creating smart technologies and entering the smart city market. Therefore, proactive planning is key to securing the smart city because the cascading effects of not doing so are too great.

4. Further research and conclusion

Since Smart Cities are still a work in progress, there are naturally a multitude of opportunities for further research on their security and privacy challenges. Areas of further research include the following. SCADA systems alone are lacking when it comes to security monitoring tools, access controls, and security buffers such as firewalls, micro-firewalls, and smart cards (Igure et al., 2006). Further research on IoT security measures will be crucial to securing a smart city that relies on such devices. Research into advanced forensics methods, establishing a reference database for malicious code, and automatic classification of malware would be helpful for securing the potential digital points of entry into a smart city (Freyssinet, 2016). Furthermore, researchers and business leaders could cooperate to create a cyber crime label that would signal to consumers the level of protection that an IoT device provides (Freyssinet, 2016).

Smart cities are a vision of how digitally interconnected cities of the future should operate. Smart city viability and desirability rely on their ability to increase quality of life in a secure manner. This paper put forth five smart city security and privacy challenges. How do we ensure personal privacy throughout a smart city that relies on rapid data sharing and data mining techniques with multiple stakeholders? Data integration in a smart city increases the digital surface in a way that provides more opportunities for security breaches; how will this challenge be overcome? What happens to data collected in a smart city? What can collected data be used for? How will data mining techniques and AI systems in a smart city affect the city's physical safety? Solutions to these various challenges include mapping the smart city's risk profile, layered security models, cryptographic techniques, data transparency, and emergency contingency plans, respectively. Ultimately, solutions to smart city challenges will be most effective when they utilize a holistic approach to security and privacy. The smart city is comprised of a plethora of interconnected devices, so security and privacy solutions need to center around a system of defense rather than simply a sum of individual defenses. Therefore, layered security approaches and transparent standards for privacy will be crucial to the construction of smart cities.

Acknowledgments

The research is supported in part by the Discovery Grants (356065-2013) from the Natural Sciences and Engineering Research Council of Canada (NSERC), Canada Research Chairs Program (950-230623), and Research Cluster Award (R16083) from Zayed University.

References

Apprenda. Iaas, PaaS, SaaS (explained and compared). http://apprenda.com/library/paas/iaas-paas-saas-explained-compared Accessed 20.07.16.

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011). Security and privacy in your smart city. *Proceedings of the Barcelona smart cities congress,* 1–6.

Basi, T. (2016, April). *Cybersecurity challenges: A view from the private sector.* http://www.serene-risc.ca/en.

Bosco, F. (2016, April). *Critical infrastructure threat landscape: Understanding and reacting.* http://www.serene-risc.ca/en.

Chen, R., Fung, B. C. M., Desai, B. C., & Sossou, N. (2012). Differentially private transit data publication: A case study on the Montreal transportation system. *Proceedings of the 18th ACM SIGKDD international conference on knowledge discovery and data mining* (pp. 213–221).

Creery, A., & Byres, E. J. (2005). Industrial cybersecurity for power system and SCADA networks. *Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference* (pp. 303–309).

Dwork, C. (2006). Differential privacy. *Proceedings of the 33rd international conference on automata, languages and programming – Volume Part II, ICALP'06,* 1–12.

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of advanced research, 5*(4), 491–497.

Enterprise, H. P. (2016, February). *HPE security research, cyber risk report 2016.*

Freyssinet, E. (2016, April). *Research and development when enforcing cybercrime and cybersecurity in France.* http://www.serene-risc.ca/en.

Fung, B. C. M., Trojer, T., Hung, P. C. K., Xiong, L., Al-Hussaeni, K., & Dssouli, R. (2012). Service-oriented architecture for high-dimensional private data mashup. *IEEE Transactions on Services Computing (TSC), 5*(3), 373–386.

Ganta, S. R., Kasiviswanathan, S. P., & Smith, A. (2008). Composition attacks and auxiliary information in data privacy. *Proceedings of the 14th ACM SIGKDD international conference on knowledge discovery and data mining, KDD '08,* 265–273.

Ghasemzadeh, M., Fung, B. C. M., Chen, R., & Awasthi, A. (2014). Anonymizing trajectory data for passenger flow analysis. *Transportation Research Part C: Emerging Technologies, 39*, 63–79.

Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security, 25*(7), 498–506.

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications, 7*(2) 7:612-625.

Khan, Z., Pervez, Z., & Ghafoor, A. (2014). Towards cloud based smart cities data security and privacy management. *Proceedings of IEEE/ACM 7th international conference on utility and cloud computing (UCC)* (pp. 806–811).

Khokhar, R. H., Fung, B. C. M., Iqbal, F., Alhadidi, D., & Bentahar, J. (2016). Privacy-preserving data mashup model for trading person-specific information. *Electronic Commerce Research and Applications, 17*, 19–37.

Kifer, D. (2009). Attacks on privacy and Definetti's theorem. *Proceedings of the ACM SIGMOD international conference on management of data, SIGMOD '09,* 127–138.

Kopylec, J., D'Amico, A., & Goodall, J. (2007). Visualizing cascading failures in critical cyber infrastructures. *International conference on critical infrastructure protection, 35,* 1–364.

Lum, W. (2016, April). *Cybersecurity challenges: A view from the public sector.* http://www.serene-risc.ca/en.

Martinez-Balleste, A., Pérez-Martínez, T. A., & Solanas, A. (2013). The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine, 51*(6), 136–141.

Matatov, N., Rokach, L., & Maimon, O. (2010). Privacy-preserving data mining: A feature set partitioning approach. *Information Sciences, 180*(14), 2696–2720.

Mohammed, N., Alhadidi, D., Fung, B. C. M., & Debbabi, M. (2014). Secure two-party differentially private data release for vertically partitioned data. *IEEE Transactions on Dependable and Secure Computing, 11*(1), 59–71.

Mohammed, N., Chen, R., Fung, B. C. M., & Yu, P. S. (2011). Differentially private data release for data mining. *Proceedings of the 17th ACM SIGKDD international conference on knowledge discovery and data mining, KDD,* 493–501.

Pattu, E., Kantarcioglu, M., Ulusoy, H., & Malin, B. (2015). Privacy-aware dynamic feature selection. *Proceedings of the 31st IEEE international conference on data engineering (ICDE),* 78–88.

Rebollo-Monedero, D., Bartoli, A., Hernández-Serrano, J., Forné, J., & Soriano, M. (2014). Reconciling privacy and efficient utility management in smart cities. *Transactions on Emerging Telecommunications Technologies, 25*(1), 94–108.

Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11–25.

Robinson, P., Woodard, J., & Varnado, S. (1998). Critical infrastructure: Interlinked and vulnerable. *Issues in Science and Technology, 15*(1), 61–67.

Sabater, J., & Sierra, C. (2005). Review on computational trust and reputation models. *Artificial Intelligence Review, 24*(1), 33–60.

Samarati, P. (2001). Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering (TKDE), 13*(6), 1010–1027.

Sen, M., Dutt, A., Agarwal, A., & Nath, A. (2013). Issues of privacy and security in the role of software in smart cities. *2013 international conference on communication systems and network technologies (CSNT)* (pp. 518–523).

Sweeney, L. (2002a). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 571–588.

Sweeney, L. (2002b). K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 557–570.

Szoldra, P. (2016, April). *We watched a team of hackers 'fully compromise' a power company in less than 24 hours.* Accessed 27.08.16 http://www.techinsider.io/red-team-security-hacking-power-company-2016-4.

T. U. o. T. a. A. (2013, July). UT News UT Austin researchers successfully spoof an $80 million yacht at sea. http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea Accessed 11.08.16.

Zhang, B., Mohammed, N., Dave, V. S., & Hasan, M. A. (2017). Feature selection for classification under anonymity constraint. *Transactions on Data Privacy, 10*(1), 1–25.

Zhu, B., Joseph, A., & Sastry, A. (2011). A taxonomy of cyber attacks on SCADA systems. *Internet of things (iThings/CPSCom), the 4th international conference on cyber, physical and social computing* (pp. 380–388).

Zimmerman, R., & Restrepo, C. (2006). The next step: Quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructure, 2*(2–3), 215–230.