Contents lists available at ScienceDirect

Sustainable Cities and Society

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

Engineering advance

A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities[☆]

Hadi Habibzadeh[a,*], Brian H. Nussbaum[b], Fazel Anjomshoa[c], Burak Kantarci[d], Tolga Soyata[a]

[a] Department of Electrical and Computer Engineering, University at Albany, Albany, NY, USA
[b] College of Emergency Preparedness, Homeland Security, & Cybersecurity, University at Albany, NY, USA
[c] Department of Electrical and Computer Engineering, Clarkson University, NY, USA
[d] School of Electrical Engineering and Computer Science, University of Ottawa, ON, Canada

ARTICLE INFO

Keywords:
Smart cities
Cyber security
Government policy making
Cryptography
Security and privacy
Authentication

ABSTRACT

Deployments of Cyber Physical Systems (CPSs) in smart cities are poised to significantly improve healthcare, transportation services, utilities, safety, and environmental health. However, these efficiencies and service improvements will come at a price: increased vulnerability and risk. Smart city deployments have already begun to proliferate, as have the upsides, efficiencies, and cost-savings they can facilitate. There are, however, proliferating challenges and costs as well. These challenges include important technical questions, but equally important policy and organizational questions. It is important to understand that these policy and technical implementation hurdles are perhaps equally likely to slow or disable smart city implementation efforts. In this paper, a survey of the theoretical and practical challenges and opportunities are enumerated not only in terms of their technical aspects, but also in terms of policy and governance issues of concern.

1. Introduction

The unprecedented proliferation of IoT services has fueled an ever-increasing competition in introducing new and innovative products for smart city applications; system developers are typically compelled to comply with strict deadlines to avoid losing their competitive advantage. This hastened development process often treats security and privacy requirements as afterthoughts, which can be later added to the system as *features* (Arias, Wurm, Hoang, & Jin, 2015). Consequently, the process leads to immature products that fail to satisfy security and privacy requirements of their target applications, both of which are of paramount importance in IoT and consequently, smart cities (Khatoun & Zeadally, 2017; Zhang, Ni, et al., 2017).

The decision to under-implement the security and privacy aspects is an implication of the infancy of the smart city concept. Research has mostly focused on exploring possible applications and their ramifications on *smart* cities (Habibzadeh, Qin, Soyata, & Kantarci, 2017; Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014) and *smart* citizens (Pouryazdan & Kantarci, 2016). Security and privacy in smart city systems were not viewed as an important aspect until the recent unexpected—and large-scale—DDoS attacks and ransomware threats (such as cryptolocker (Liao, Zhao, Doupe, & Ahn, 2016), cryptowall (Cabaj & Mazurczyk, 2016), and wannacry (Mohurle & Patil, 2017)). The reprecussions of these attacks stirred a sense of mistrust against the IoT to the extent that some criticized the Internet of Things for turning into the *Internet of Vulnerabilities* (Angrishi, 2017).

IoT and smart city communities have reacted to these developments by creating a new tidal wave of research toward investigating cybersecurity and data privacy within the smart city context. Companies have begun advertising *secure* smart city products. Nonetheless, the aforementioned considerations in smart city cybersecurity have left many of these *secure* products vulnerable to non-conventional cyberattacks (Arias et al., 2015). Designing robust and secure services is contingent upon the understanding of various aspects of cybersecurity research in smart cities.

The ongoing research in cybersecurity and privacy of IoT is advancing in two parallel—yet complementary—branches. In the first branch, researchers and involved policy makers, such as Federal

[☆] This work was supported in part by the U.S. National Science Foundation grants CNS-1239423 and CNS-1464273, and by the Natural Sciences and Engineering Research Council of Canada DISCOVERY Program under Grant RGPIN/2017-04032.

[*] Corresponding author at: Department of Electrical and Computer Engineering, University at Albany, Draper Hall, Suite 116, 135 Western Ave, Albany, NY, 12203, United States

E-mail addresses: hhabibzadeh@albany.edu (H. Habibzadeh), bnussbaum@albany.edu (B.H. Nussbaum), anjomsm@clarkson.edu (F. Anjomshoa), burak.kantarci@uottawa.ca (B. Kantarci), tsoyata@albany.edu (T. Soyata).

https://doi.org/10.1016/j.scs.2019.101660
Received 24 August 2018; Received in revised form 11 June 2019; Accepted 12 June 2019
Available online 21 June 2019

departments and agencies, identify and categorize various types of threats, dominantly from a social and financial perspective. The main contribution of this effort involves investigating the depth and extent of the implications of cyberattacks and the output is often used as the basis of new policies and regulations. The second branch consists of computer scientists and researchers, who inspect the technical tools to meet the security and privacy requirements of smart city regulations. The research community has come to the realization that technical implementation of smart city security is also a multi-faceted problem, in which the overall security of the system is determined by the weakest link. This observation proves to be the source of many vulnerabilities in existing smart city systems, where developers wrongly assume that they can improve the security of their products by securing a portion of the system and neglecting others.

It is, therefore, critical to view the security of smart cities through bifocal lenses to avoid biased—and common—magnification of technical considerations against policy aspects; even with ideally functioning technological solutions, cities with ossified bureaucracies and decades old civil service titles will struggle to make their cities smarter. A major—and wildly underexplored in the literature—factor in the distance between what smart city applications could help achieve, and what they have so far is in the non-technical realm. Issues of politics, bureaucracy, liability, and other non-technical factors are driving slow implementation, even when the technologies are considered ready to use. In fact, Scientific American has called the need to improve the policy side of smart city implementation (Smith, 2017): "*A big reason for the disconnect between smart city potential and reality is the fact that smart cities are where the digital world blends, but can also collide, with the non-digital world. Non-digital issues such as legacy governance, social justice, politics, ideology, privacy and financial elements that are not so smart, efficient or resilient when smart-city planning starts can become large factors* (Smith, 2017)."

Outside of smart cities, this is seen as obvious and normal (Whittaker, 1999), however with a few exceptions (Nam & Pardo, 2011), there has not been a lot of focus on the non-technical implementation challenges. And this insight is not a new one; in a 1999 study of "unsuccessful information technology projects," (Whittaker, 1999) the three most common reasons for failure were non-technical (or depending on how you interpret the first, at least two of three were)—they were "poor project planning," "weak business case," and "lack of top management involvement and support." It seems clear that non-technical challenges routinely derail information technology projects; it would be strange if smart city implementations were different.

This problem is particularly pronounced in the public sector. Within the public administration literature, there is a long history of the study of information technology implementation projects, however that literature suggests several reasons to show pessimism (Goldfinch, 2007) about technology adoption in government agencies. Heeks and Bhatnagar suggest that "conception-reality gaps" often lead to failure in public IT projects (Heeks & Bhatnagar, 1999). These gaps exist along various axes; they name six: Information, Technology, Processes, People (objectives, values, and motivations), People (staffing and skills), Management and structures (Heeks & Bhatnagar, 1999). Of these six areas of disconnect, at least half are entirely non-technical, focusing instead on the people and organizations that are attempting to adopt or implement the information technology process. The fact that this clear empirical literature is so often ignored in the smart city world is surprising, illustrating that there seems to be some bias toward solving the concrete engineering problems (the technical ones) and devaluing or ignoring the often times harder to measure and manage policy problems (the non-technical ones). This has lead to serious lacunae in the field.

Yet even from the technical standpoint, securing IoT is a difficult task. Some of the challenges root from Wireless Sensor Networks (WSNs). Particularly, the limited computational capability of CPSs (Shishvan, Zois, & Soyata, 2018; Soyata, 2018) hampers the deployment of advanced security mechanisms (Soyata, Copeland, & Heinzelman, 2016). Nonetheless, the majority of stubborn challenges are based on inherent characteristics of IoT. Furthermore, the scale of IoT poses various practical limitations in implementing suggested security mechanisms (Kocabas, Soyata, & Aktas, 2016; Zhang et al., 2014). The dynamic nature of such systems along with the mobility requirement of some of the CPS devices exacerbates the problem. This characteristic is particularly preeminent in smart cities, where the ever-changing conditions of the cities and direct interaction between CPS devices and citizens result in a highly dynamic system.

Another fundamental complication arises from the heterogeneity of the system; the protocols and the architectures used within a smart city are diverse and incompatible. The interoperability among these various implementations is not guaranteed, which impacts various aspects of the system, including security and privacy considerations. This heterogeneity also implies that a single security and privacy initiative cannot be comprehensive enough to satisfy the requirements of all applications.

Cities are, and have been, facing serious economic and resource challenges in recent years. These include budget declines (Reuben, 2011), decreasing state aid (Maciag & Wogan, 2017), and increased budgetary uncertainty (Pagano & Hoene, 2018). It is in this precarious or worsening resourcing environment, that cities have been embracing smart city solutions. While this makes sense because some smart city applications can improve efficiency or save money, it creates serious challenges to the cities ability to both make the major upfront capital investments such applications require, and also to recruit and retain a sufficiently sophisticated information technology workforce to run and monitor such applications. Just as cities are becoming more interested in pursuing smart city applications, many of them are becoming less able to do so effectively. In this paper, we review the privacy and security of smart cities from the perspective of policymaking and technical aspects. To study the implications and urgency of cyberattacks that target smart cities, we analyze the latest developments in the field and investigate some prominent attacks against critical smart city infrastructure. We then provide technical breakthroughs that can mitigate the vulnerability of smart cities against various attacks and study their strengths and weaknesses.

The rest of this paper is organized as follows. We first review the implications of cyberthreats on security and safety of smart cities infrastructure in Section 2. In Section 3, we discuss how policymakers have reacted to these vulnerabilities by enforcing new laws and regulations. We study the underlying architecture of the smart city in Section 4 and explain how this structure imparts vulnerabilities common among all smart city services. In addition to this shared susceptibility, each smart city applications faces domain-specific security concerns. We investigate these challenges in Section 5. We conclude the paper by discussing open issues, as well as a summary of our manuscript.

2. Potential security and safety implications for critical infrastructure in smart cities

There is little question that the growth of *smart cities* will introduce numerous risks while making many aspects of the city operation more efficient. In this section, we study these risks in multiple categories.

2.1. Infrastructure risk in the smart city

One of the most important risks are the ones involving the smart city critical infrastructure and related systems, often called *lifelines* (National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis, 2015). These infrastructure risks come in numerous variations and types and so it is important to think about ways to conceptualize and link such risks together. There are two key conceptual aspects of smart city cybersecurity: Firstly, the massive increase in embedded computing capacity rapidly expands the attack surface that network defenders must secure. In the consumer space, this involves taking items as diverse as televisions, refrigerators, video cameras, routers, and all of the *smart* devices and turning them into attack vectors or resources for malicious activity (e.g., conducting Distributed Denial of Service (DDoS) attacks). The emerging ubiquity of computers and sensors in all matter of urban infrastructure and hardware—from parking meters to traffic signs to waste water infrastructure—is likely to have comparable effects on urban networks.

Secondly, the presence of *actuators* that adjust/control things in the physical infrastructure of the smart city (e.g., heating elements, switches, valves, filters, and the like), as opposed to *sensors* that measure things, means that those who can compromise such systems have the potential to cause physical damage in addition to data theft or denial of services. In this sense, the expansion of computing power—-particularly when joined with sensors and actuators—expands two of the three components of infrastructure risk as described by Sandia National Lab (Baker et al., 2019). While the *smartening* of cities and infrastructure does not increase the threat (the number, capability, or intent of threat actors) necessarily, it does in fact increase the vulnerability (in the form of a much larger and more complex attack surface) and increase the potential consequence of an attack (by allowing attacks on networks and data to cause physical damage in the real world). Thus, it is fair to say that, for all the myriad benefits that smart cities bring with them, it is important to remember that they do seriously increase infrastructure risk as well. Fig. 1 conceptually depicts the consequences of cyber threats on a smart city infrastructure.

2.2. *Information security and operational security*

Few cyber threats have received more press recently than the many ransomware campaigns that have wrought havoc on individual users' computers and on organizations of all stripes. Ransomware, malware that encrypts files in order to deny data access until the owner pays a ransom (typically in Bitcoin or some other virtual currency), has been widespread and very disruptive (Al-rimy, Maarof, & Shaid, 2018). Variants like reveton, cryptolocker, cryptowall, and wannacry (Hampton & Baig, 2015) among many others have resulted in large numbers of users paying ransoms, as well as in immeasurable loss of data. A typical ransomware victim likely loses important work or personal files ranging from financial information to family pictures (O'Gorman & McDonald, 2012); however there is a different class of victims for whom the damages are more complicated—enterprises that rely on data for operations.

Numerous police agencies have been infected with ransomware (Francescani, 2016) and some non-trivial portion have paid ransoms to recover their data. There are even reported cases where police agencies lost digital evidence; such cases affect pending trials or appeals (Mathews, 2018). A higher profile series of cases appeared in the healthcare sector. First, Hollywood Presbyterian hospital in California was forced to pay a larger-than-normal ransom in order to recover their data and their operations were crippled as a result of this ransomware infection (Wagstaff, 2013). The wannacry ransomware infections in early 2017 had similar impacts on numerous sites of the British National Health Service (NHS) (Dwyer, 2018; Ehrenfeld, 2017; Martin, Ghafur, Kinross, Hankin, & Darzi, 2018). These are cases where the inability to access key data—e.g., dosage levels, drug interactions, medical histories—could well result in injury or loss of life. The attachment of computers to medical devices is a small scale version of the informatization of infrastructure, which is common in a smart city.

What happens when data denial or availability attacks hit critical infrastructure, for example transportation infrastructure? Assume a scenario where public transportation system becomes the victim of a massive ransomware attack that does not target the industrial control system networks and infrastructure that actually controls the trains; instead, it aims to disable the ticket machines and payment infrastructure, through which purchases are made. The attack may also impact computer systems that are used to *manage the city's buses* (Gallagher, 2016). Attackers of this type, seemingly cognizant of the impact of their attack, are likely to attempt to extort a ransom payment of over some tens of thousands of dollars or a similar amount in Bitcoins (Stewart, 2016); far more than the typical ransomware payments which tend to be in the range of hundreds of dollars. In the presence of such an attack, the public transport system may simply allow the riders to travel for free and lose revenue, as the Bay Area Regional Transit system did in California (Bay Area Rapid Transit, 2017). Furthermore, the transit system has to re-image machines and do other work to clean up their systems, all the while unable to process most of the payments.

2.3. *Financial impacts vs. operational and safety impacts*

Ultimately, this move from cyber attacks impacting data (with a focus on confidentiality concerns) and having significant financial consequences, to impacting operational networks and having potential operational and even physical impacts (in addition to financial impacts) is one of the key conceptual changes that smart cities, the IoT, and other embedded computing systems are making manifest. In fact, Microsoft includes a variation on this insight in a recent white paper on Cybersecurity Policy for the IoT, and state that the *operations depend on data integrity and availability* (Abendroth, Kleiner, & Nicholas, 2017).

Infrastructure systems such as the electrical grid, transportation networks, and even water and waste water systems have long had computerized controls. Historically however, those systems were discrete, unconnected, and fairly limited. The computerization and real-time analysis and manipulation of more and more urban infrastructure—from traffic lights to public WiFi networks to parking management systems—and the connection of these new networks and the often-insecure legacy infrastructure systems into *smart city* management portals and systems will vastly increase the complexity,

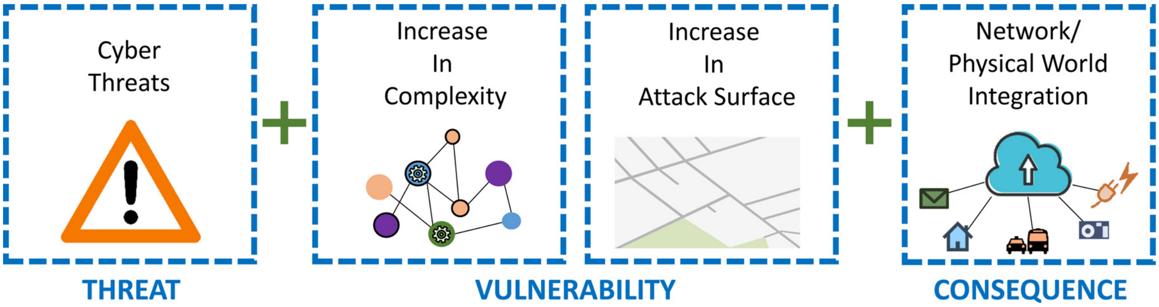

Fig. 1. The infrastructure risk in smart cities is determined by three parameters: (i) threat, (ii) vulnerability, and (iii) consequence (Baker et al., 2019). Making cities *smarter* does not increase the threats they face. However, it does create new vulnerabilities by increasing the system's complexity and attack surface. Because the cyber world and physical world in smart cities are integrated, any successful attack to the former can lead to tangible consequences in the latter, thereby aggravating the consequence parameter (Baker et al., 2019).

interconnectedness, and vulnerability of urban infrastructure networks.

Smart cities will bring with them major advances in efficiency and capability for cities. Smart devices do the same for many consumer products. The important thing for policy makers and those concerned with security to remember is that the "smart" in smart cities can be read in many ways. While it can mean smart in the sense of optimizing operations based on the best available data, it can also mean "hackable." Ultimately smart just means having computing power and sensing capabilities embedded in or appended to it, and like most sensors and computers, these too are likely to remain susceptible to manipulation, misconfiguration, malicious misuse, and outright attack.

3. Policy implications at the city, regional, national, and international levels

Intricate connections among various aspects of smart cities form a complicated web of technologies, policies, and services, which by entangling the attack surface, imparts new security dimensions into city's management. A robust approach to overcoming such complications must involve close cooperation among city authorities, engineers, and different levels of the government. In this section, we investigate the integral role of the latter in safeguarding the security of smart cities.

3.1. Smart city security: a key factor of governance

The cyber security community has begun to respond to the growth in smart city technologies with a growing stream of analysis and insight that make clear that cities will have their work cut out for them as they attempt to become *smarter* while remaining secure (or perhaps even increasing security). As cities adopt these technologies, and particularly as they attach them to physical infrastructure systems, it will become incumbent upon the cities to assure traditional variations on confidentiality, availability and integrity; the latter two of which become particularly serious in the case of cyber-physical systems (Mosenia & Jha, 2017). While much of the work of the traditional cybersecurity community, particularly much of the highest profile work that has received public attention (Data Breach Investigations Report, 2018), has focused on issues of confidentiality (through data breaches and the like); the security community has begun to focus on the threats to availability—from ransomware to DDoS attacks—and integrity that are tied to the IoT and Smart Cities (Bartoli et al., 2011; Cerrudo, 2015; Logota, Mantas, Rodriguez, & Marques, 2014).

Conti, Cross and Raymond (Conti, Cross, & Raymond, 2015) describe additional challenges and vulnerabilities facing smart city deployments including a review of multiple instances of cyber attacks targeting corporations and businesses and underlying infrastructure such as air quality control and airport security, all of which can lead to exploitation, deception, diversion, disruption, delay, and degradation of/in citizens and services. The authors also detail some of the interdependencies among key infrastructures, critical and non-critical city sectors, and their possible domino-like failure. In (Cerrudo, 2015), the researchers detail numerous cyber vulnerabilities that are common to many large smart or informatized cities; these include (i) common information technology problems such as the lack of patch deployment capabilities, (ii) specific problems like overlapping infrastructure systems and personnel challenges, and (iii) limited cyber incident planning or incident response teams. This research also analyzes a host of potential attack targets and vectors that could be of concern to cities, including potential attacks on (a) traffic control systems, (b) water and waste water systems, (c) street lighting systems, and (d) the potential manipulation of smart electrical infrastructure (Cerrudo, 2015).

Ultimately, the *smart cities* and *smarter cities* face a large number of security challenges that range from technical problems like *large and complex attack surfaces* to *insecure legacy systems* to people and process issues arriving from public sector bureaucracy (Cerrudo, 2015). In all of these cases, the technology has often arrived—and been deployed—much more quickly than these cities can change their personnel practices, contracting vehicles, security policies, and other agency and municipal practices. Thus, there is the emergence of a *security debt*, in which the upsides of smart city technologies are realized very quickly, but security downsides are often pushed off into some as-yet-unclear-when future. Despite these clear security challenges facing smart cities, cities are hardly the only stakeholders with an interest in securing smart cities.

3.2. Smart cities, federalism, and national security

One of the further challenges presented by the Internet of Things and embedded computing to traditional governance models involves questions of ownership, control and regulation, guidance and strategy, all across different levels of government. Smart cities are likely to exercise the most control over sensors and other embedded devices in their networked infrastructure; however if other areas of technology adoption are an indicator, governments in other levels of federalism (like states, provinces, and national governments) are likely to play numerous roles as well. These *higher* levels of government might play roles in terms of regulation, standard setting, funding of research and development, as well as funding both pilot programs and larger rollouts of such technologies. This multi-layer governmental involvement—particularly when paired with the complexities of public-private partnerships and contracting with vendors—will result in a very complex web of governance. While cities will often own and operate much of the *smart city* infrastructure (in conjunction with vendors and contractors), state/provincial and national governments obviously have strong interests in the security of such systems.

Two national examples of this illustrate interesting—and differing—sets of priorities in the case of the United States and Ireland. In both cases, the national governments are decidedly not attempting to intervene directly and regulate or set requirements for smart city infrastructure; rather, in both cases, the national governments are investing in research and strategy formation to think about security and privacy concerns with the hope that such resourcing will improve the quality of municipal decision-making around security.

In the US, the Department of Homeland Security issued a 2015 document entitled The Future of Smart Cities: Cyber-Physical Infrastructure Risk (National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis, 2015). The document takes a broad look at infrastructure risks that emerge from the adoption and potential expansion of smart city technologies. It examines such risks in the transportation, electricity generation and delivery, water and wastewater subsectors. In each of these areas, it looks at potential versions of corruption, malfunction, manipulation, disruption, or other compromise. Throughout all of these concerns, it focuses on three themes that draw them together—changing *seams* (i.e., new interactions, new stakeholders, and new access points or attack surfaces), inconsistent adoption, and increased automation (National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis, 2015). In Ireland on the other hand, much focus was placed on the data collected by smart cities, and the security and particularly privacy implications of such data (Kitchin, 2016). This focus on the myriad aspects of privacy obviously differs in some important ways from the US DHS focus more narrowly on the security of particular infrastructure systems. That being said, both are key to understand the security implications of smart cities, and both illustrate that different governments (whether in different countries or at different levels within the same countries) are likely to prioritize security concerns around smart cities differently. The US government has also looked at issues around privacy in the IoT and smart cities (Internet of Things, 2016). In addition to national level documents outlining approaches to smart city security, supranational entities—like the European Union—have also issued some suggestions about how they will view smart city security. For example, the EU Network and Information Security Agency (ENISA) issued (Lévy-

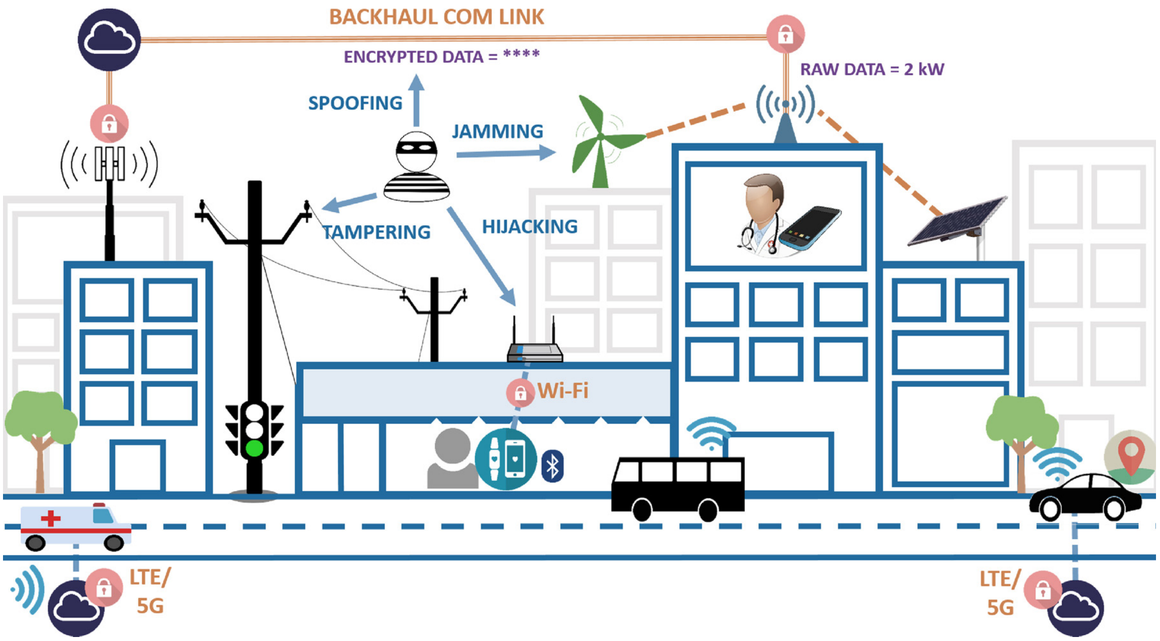

Fig. 2. An abstraction of the smart city and, the interactions among its various component, and the flow of data to and from local to back haul networks. The adversary can target the system during sensing, transferring, and processing of data. As shown in the figure, the complexity, scale, and extent of smart services provide more opportunities for the adversary.

Bencheton & Darra, 2015) an exploratory analysis of cybersecurity for smart cities focused on the public transportation sector. These parallel prioritizations of security issues will inevitably lead to complicated negotiations and governance challenges.

Many of the security questions raised by smart cities are broader even than individual countries, levels of government, or agency stakeholders. Some end up as broad, almost philosophical, legal and regulatory questions.

4. Security implications of the smart city architecture

Smart cities are realized through an assembly of interacting embedded CPSs, shared infrastructures, and distributed systems, which are interconnected through a heterogeneous communication platform (shown in Fig. 2). This platform is proven to be a weak link in security and privacy management of smart cities, as it is vulnerable to various attacks that might be originated by insiders, outsiders, or a collaboration of both (Ijaz, Shah, Khan, & Ahmed, 2016). Although several studies have proposed countermeasures against security challenges in smart city settings (Balte, Kashid, & Patil, 2015; Elmaghraby and Losavio, 2014; Zhao, 2013), existing well-established information security and privacy techniques—which originally target non-smart city applications—still need to be tailored to address the latent flaws and weaknesses of smart city systems. A comprehensive approach entails a multi-layer—yet coherent—security mechanism that can cater rigorous protection to all levels of the systems, which consist of (i) physical, (ii) communication, and (iii) processing and storage components. Although existing cybersecurity research primarily focuses on a single component of the system at a time, a robust CPS can only be implemented by balancing the cybersecurity capabilities of all of its components, as the overall potency of the system against cyber attacks is typically determined by its weakest link. This section investigates the security characteristics pertaining to these three components and reviews existing solutions to address them. Since many smart city applications leverage the same structure, these vulnerabilities and their associated remedies are applicable to a wide range of services.

4.1. *Physical level vulnerabilities*

The physical level of smart cities refers to the sensors and actuators that directly interact with the environment. In a large-scale smart city application, this level encompasses thousands of different sensors and actuators that are scattered across the city. This heterogeneity along with the constantly changing nature of the physical level—which is induced by the dynamic nature of the modern cities—can easily overwhelm system developers with myriad challenges. As a result, security and privacy considerations of this level are often neglected. Unfortunately, a system administrator might wrongly assume that this overlook can be remedied by incorporating additional security features in other levels of the system. In reality, however, the physical layer can become the weakest link in the system and compromise its security entirely. An example of this overlooking design practice is studied in (Arias et al., 2015), where the authors successfully hijack an exciting smart home product with robust communication and processing security features by exploiting its hardware vulnerabilities. Through the compromised device, they establish a rogue DHCP server and consequently endanger all the other devices that are part of the home WiFi network, including the residents' smartphones and laptops.

4.1.1. *Device protection*

The literature recommends various security and privacy measures for the physical level. The most straightforward approach is to use conventional cryptography. However, the computational capability of conventional cyber-physical systems is typically bounded (Soyata et al., 2016; Soyata, Muraleedharan, Funai, Kwon, ö Heinzelman, 2012), which limits the applicability of advanced cryptographic techniques. Furthermore, although cryptographic approaches provide software security, they cannot ensure immunity against side-channel (Kocabas et al., 2016) and hardware attacks (Arias et al., 2015). These shortcomings imply that solely relying on software-based cryptography cannot protect IoT devices, sufficiently. More comprehensive solutions are required.

A robust holistic device security mechanism must provide protection in four different levels: (i) firmware-level, (ii) device-level, (iii) circuit-level, and (iv) energy harvesting and storage-level. Table 1

Table 1
An overview of physical security countermeasures. An effective approach must span all four dimensions of physical security.

Dimension	Countermeasures (Description)	Effective against
Firmware-Level	**OS-Level Isolation** (Wessel, Huber, Stumpf, & Eckert, 2015) (Heterogeneity in Security Requirements for Smartphone-Integrated Applications) / **Platform Integrity Attestation** (Broström, Zhu, Robucci, & Younis, 2018) (Detecting Unauthorized Changes in Device Hardware and Software)	Hardware-based Injection Attacks, Eavesdropping Android Root Access Attack, Effective Against Insiders (if access to debug pins is limited) / Impersonation Attack, Replay Attacks Tampering, Exploitation, &Injection Attacks
Device-Level	**Provable Memory Erasure** (Ammar, Daniels, Crispo, & Hughes, 2018) (Ensuring the Erasure of Sensitive data) / **Physically Unclonable Functions** (Labrado & Thapliyal, 2019) (Generating Device-Specific Unclonable IDs)	Privacy Leakage and System Reset Attack / Tampering &Sybil Attack
Circuit-Level	**Laser Injection Protection** (Liu, Gu, Qu, & ONeill, 2018) (Counter Laser Injection Attacks) / **SIMON Round Unrolling** (Singh, Chawla, Ko, Kar, & Mukhopadhyay, 2019) (Immunity Against PSCA)	Tampering, Injection, Laser Fault &Voltage Glitch Attack / Power-based Side-Channel Analysis (PSCA)
Energy-Level	**Energy-Depletion Countermeasures** (Nguyen, Lin, & Hwang, 2019) (Detecting Abnormal Channel Activities to Curtail Energy Depletion Attacks) / **Battery-Drain Countermeasures** (Shakhov & Koo, 2018) (Detecting Abnormal Battery Level Changes Even with Temporary QoS Improvements)	Energy Depletion Attack, Battery Exhaustion Attack Vampire Attack, Denial of Sleep Attack / Battery Exhaustion Attack Depletion of Battery Attack

summarizes some of the important security solutions of each level as well as the types of threats each solution is most effective against. In general terms, firmware-level security must provide protection against firmware tampering attacks as a compromised node can readily be converted to a launchpad for data leakage and a variety of network attacks. The literature provides a long list of solutions and recommendations. From simply limiting the access to debug pins and ports to various platform integrity attestation mechanisms that can verify the authenticity of a device's hardware and firmware. Many exiting integrity attestation solutions, however, are not fully compatible with IoT devices. For example, both hardware and software implementations of the widely-used Trusted Platform Module (TPM) suffer from significant power and cost overhead. This has motivated the emergence of IoT-optimized integrity attestation solutions that do not rely on TPM (Broström et al., 2018). Firmware-level security for more resourceful devices is not straightforward either. Particularly, being an integral hub for many IoT services, smartphones and their operating systems (OS) are subject to *security heterogeneity* complications. This implies that each of the many IoT services that a smartphone hosts demands unique security services. To address this problem, the study conducted in (Wessel et al., 2015) suggests a low-overhead OS-level isolation mechanism that can decouple the resources of secure and non-secure applications. To achieve maximum security, the proposed technique uses both hardware and software isolation, implying that hardware modifications to the device are required (although as simple as using a memory card or pairing a module using BLE). Smartphone-based IoT applications must also adhere to security services of their hosts' operating system, effectively. The literature particularly underlines proper device access privileges as many existing apps are *over-privileged* (Fernandes, Rahmati, Jung, & Prakash, 2017).

Indeed, the firmware is only a single component of IoT devices. Complementary measures are needed to secure devices and protect them from deliberate tampering or unintentional damages, whether the device is deployed on-site or off-site (to safeguard against insiders). Covering physical nodes in safe cases that limit unauthorized access can be a simple and effective (yet costly) approach that greatly enhances device-level security (Tedeschi, Mehnen, Tapoglou, & Roy, 2017). Another dimension of device security involves *provable data erasure*, a mechanism that guarantees sensitive data are indeed deleted and hence inaccessible in a node's memory. A scenario pertaining to provable data erasure involves a transmitter that requests the erasures and a receiver, which hosts the sensitive data and is expected to erase them without leaving any possibility of data recovery. The most straightforward approach requires the transmitter to send random packets that fill the receiver's memory and overwrites the sensitive data. This solution is straightforward but it incurs significant communication overhead. As an alternative, the study conducted in Ammar et al. (2018) proposes a software-based solution that stores the sensitive data in a secure isolated memory block. This eliminates the reliance on excessive package transmission. Additionally, a software-based approach is applicable to legacy IoT devices. To enhance the integrity of the device and improve its resistant against tampering, device-level Physically Unclonable Functions (PUFs) have been proposed as viable solutions. Manufacturing imperfections imply that every single IoT device has unique characteristics. PUFs utilize these device-specific imperfections to uniquely identify IoT nodes. A PUF can be viewed as an input-output module, which for a given input (often termed *challenge* or *query* in the literature), generates different outputs (often called *response*) across various devices. This exclusive output can be used (say) as the seed of a random number generator to construct secrete keys on demand, thereby eliminating any need for their secure storage. PUFs are typically based on circuit-level implementations, however, device-level solutions that utilize idiosyncrasies of energy harvesting units and sensors are also proposed in the literature (Labrado & Thapliyal, 2019). Aside from their many advantages, PUFs suffer from stability issues as challenge-response pairs can sometimes be inconsistent (Suzuki, Ueno, Homma, & Aoki, 2019). Nonetheless, the importance of PUFs in IoT security is expected to grow in the coming years.

Circuit-level security protects embedded chips of IoT devices. The attacks that target this level generally require more expertise and are relatively less straightforward to carry out. Additionally, as chips' functionality and structure differ significantly from application to application, circuit level attacks often evince an astonishing variety. This has motivated the emergence of various techniques that aim to counter (very) specific attacks. Within this inclusive bracket, side-channel attacks form a major category. Many circuit-level solutions are proposed to battle side-channel attacks. Perhaps the most uncomplicated solution is to randomize computations and control, hence decoupling power demand and memory access from the task and critical parameters. In addition to its simplicity, randomization can be completely software-based, which increases its applicability. The drawback is that it increases the computational load and can expedite the battery drain. Another effective countermeasure against side-channel attacks is to increase the area of the chip. This can be achieved by unrolling rounds of iterated block ciphers, which not only battles power-based side-channels attacks but also increases the throughput of the system albeit at the cost of the increased area (Singh et al., 2019). Using laser as an instrument for fault injection attacks has also been studied in the literature. When targeted at the chip, tuned laser beams can induce photocurrent in transistors and possibly alter their status, thereby sabotaging its normal operation. Laser attacks are not straightforward to carry out. They require expertise and equipment. They also involve thorough chip analyses, careful timing, and time-consuming laser tuning. Nonetheless, the results can be quite rewarding for adversaries as even changing a single bit in a security status register might be sufficient for circumventing (say) secure boot procedures (Vasselle, Thiebeauld, Maouhoub, Morisset, & Ermeneux, 2018). Covering sensitive areas of the chip with photosensitive materials is an effective way to detect and combat laser attacks. However, this change needs to be incorporated into the system from early design phases.

Considering the vital role of energy storage units in IoT, many adversaries use energy depletion and drain of battery attacks to cripple individual nodes or even an entire network. Energy depletion attacks interfere with device communications to intentionally increase their energy consumption cost. In a simple scenario, a simple transmitter is sufficient to keep the channel occupied. This increases the back-off periods and wake-up times of legitimate nodes. Jamming attacks with the intention of increasing the error rate are another archetypes of energy depletion attacks. To avoid detection, malicious transmitter can only operate when the network load increases. Random transmissions are also effective for evading detection. In general, frequency hopping (which reduces interference) and statistical tools that detect abnormal channel access behaviors are the main means against these attacks (Nguyen et al., 2019). Drain of Battery (DoB) attacks aim to reduce device lifetime by increasing its power dissipation rate. Unlike the energy depletion attacks, however, DOB can temporarily increase the device performance and network QoS (e.g., by increasing the transmission power to more than sufficient levels). This complicates their detection using conventional solutions. An effective countermeasure against DoB attacks must be implemented in device-level. Algorithms that monitor energy consumption irregularities can help detect DoB attacks although at the cost of added computational overhead (Shakhov & Koo, 2018).

4.1.2. *Mobile crowd-sensing security and privacy*

A major trend in smart city sensing context is the proliferation of smart portable devices, which has created myriad opportunities in the emerging Mobile Crowd-Sensing (MCS) platform. In MCS, citizens use the non-dedicated sensing capabilities of their smart devices (Habibzadeh, Qin, et al., 2017) and smart vehicles (Nunes, Moreira, Kimura, Sastry, & Mahmoodi, 2017) for either participatory or opportunistic data acquisition; MCS provides the foundation for *Sensing as a Service (SaaS)* framework. Securing MCS systems is a challenging task as not only they face all the security and privacy challenges of dedicated sensing but their unique structure also poses additional threats and vulnerabilities. Overall, the security and privacy concerns in MCS are multi-faceted and highly interwoven. However, they can be broadly associated with (i) compensation (ii) trustworthiness and reputation assessment, and (iii) sensing data leakage.

Compensation mechanisms to encourage citizens' participation impart additional security flaws (Zhang et al., 2016). Many existing implementations use auction-based recruiting mechanisms, where a server recruits devices with the lowest bids, subject to its quality requirements. Conventional auction-based solutions, however, can potentially lead to privacy leakage as each bid can reveal sensitive information about the participants. For example, participants closer to the point of interest tend to bid higher (as they provide higher quality data), which can potentially reveal their location. It is possible to use grouping and *k*-anonymity to battle these security flaws (Li, Jung, et al., 2018).

Whether monetary or not, blindly compensating all participants always leaves adversaries a chance to get rewarded for providing falsified information. This drawback has motivated the research for quantifying the reputation of participants and the trustworthiness of their submitted data. To this end, the *hard* and *soft reputation* metrics are introduced to estimate the trustworthiness of the sensing hardware and its user, respectively (Pouryazdan et al., 2016; Pouryazdan, Kantarci, Soyata, Foschini, & Song, 2017). This way, it is possible to make a distinction between hardware failures of genuine participants and the malicious intention of the adversaries. Hard and soft reputation can be quantified using either centralized or decentralized approaches. Trustworthy Sensing for Crowd Management (TSCM) compares current and past data to detect outliers and suspicious samples (Kantarci & Mouftah, 2014). Because TSCM relies on an archive of information, it typically entails a centralized implementation. Alternatively, voting-based solutions provide a basis for many decentralized reputation analyzers such as Social Network-Aided Trustworthiness Assurance (SONATA) (Kantarci, Carr, & Pearsall, 2016), where participants in a sub-network vote for the trustworthiness of their peers. SONATA also adjusts the voting powers of participants dynamically based on their current reputation, hence limiting the influence of adversaries.

Many existing solutions to gauging data trustworthiness (including the preceding works) are based on a common premise, where different weights are computed and assigned to each node. This effectively measures trustworthiness; nonetheless, sharing weights of individual nodes can lead to additional security repercussions because it gives servers an opportunity for manipulation attacks. Homomorphic encryption can remedy this problem but at a significant computation overhead. Furthermore, MCS generally involves a high-rate of duplicate packets. Encryption makes it difficult to effectively detect duplicates (Ni, Zhang, Yu, Lin, & Shen, 2018). Another approach is to relegate this task to individual devices. To this end, the server aggregates the data (in an encrypted environment) and transmits the result back to individual nodes. Each node can then compare its sample with aggregated results to measure its deviation (which can be used as the basis for updating weights) (Xu et al., 2017). This approach, however, can incur additional communication overhead. Another alternative is to decouple trustworthiness measurement and rewarding process to third parties; particularly, miners in a blockchain-based cryptocurrency can effectively perform these task. Nonetheless, *k*-anonymity is still required to prevent privacy leakage to miners (Wang et al., 2018).

The intricate interaction between users and their smart portable devices in MCS platforms also poses significant privacy concerns. Adversaries can use eavesdropping and traffic analysis to gain private information about participants, pinpoint their location, or record their private conversations. Particularly, many MCS systems are vulnerable to collusion attacks, where multiple adversaries share their resources to circumvent security mechanisms (He, Chan, & Guizani, 2015). Making the participants completely anonymous might not be an effective approach as it can complicate their reputation analysis; it is hard to assess the trustworthiness of a user without knowing them. For some sensitive data such as location-based information, frequently changing the pseudonyms (Beresford & Stajano, 2003) and adding noise and misleading information intentionally (Ghinita, 2013) can be effective against privacy leakage. Another effective solution is to minimize the data exchange between the cloud and the participants, which reduces the opportunities for data leakage. To this end, some researches propose the game-theory and fundamentals of the free market to create a self-regulatory bidding and task assignment procedure, which can run independently of the cloud (Pouryazdan, Fiandrino, et al., 2017). In these applications, QoS is the utility of the server, whereas rewards are user's utility. Any risk to undermine the participant's privacy can model the cost function. Monopoly and oligopoly models can be used to create a self-regulatory system; users and the server try to maximize their utility function while minimizing their cost (Liu, Zhou, Zhu, Zhou, & Lin, 2017). They will eventually settle in equilibrium without requiring any involvement from third-party or explicit communication. Finally, although cloaking mechanisms and *k*-means can reduce the chances of privacy leakage, they are not effective against inadvertent data leaks. For example, camera-based services must automatically use face detection algorithms to blur and protect the identity of bystanders (Li, Jeong, Shin, & Park, 2017). Table 2 provides a summary of MCS security and its various dimensions.

4.2. *Communication level vulnerabilities*

The communication level comprises a short and medium range

Table 2
Regardless of its complexity, security and privacy protection in MCS applications includes three major dimensions. Oftentimes, the security of one dimension complicates the security of others; implying that designers should maintain a subtle tradeoff to achieve maximum security.

Dimension: Description	Solutions	Shortcomings
Recruitment &Compensation: Bids causing privacy leakage	Blockchain-based Compensation Cloaking (e.g., *k*-anonymity)	Cloaking Interference with Accurate Compensation & Location-based Services
Trustworthiness &Reputation Assessment: Participants submitting falsified or inaccurate information	History-based Analysis (e.g., TSCM), Voting-based Analysis (e.g., SONATA), (Additive) Homomorphic Encryption	Weights Causing Privacy Leakage Communication & Computation Overhead, Manipulation Attacks by Server
Sensing Data Leakage: Advertent/inadvertent privacy leaks	Anonymity Mechanisms Minimizing Data Exchange (Game-Theory Models)	Complicating Reputation Analysis Due to Anonymity Not Effective Against Inadvertent Privacy Leaks

network that allows the sensors to transmit their data to a gateway or cloudlet (Powers et al., 2015). Similar to sensors, these networks are used on-site and suffer from the same limitations such as meager power availability. Therefore, the networks connecting sensors and gateways are typically short-range, multi-hop, and low-rate, which allows them to manage their power consumption. The gateways are typically more powerful computers and have access to Internet, through which the data are transferred to and from the cloud. The network between the sensors and the gateways is sometimes considered as a part of the data acquisition level because the communication and sensor modules are typically implemented within the same device. Therefore, it is difficult to physically separate them. However, as their functionality is logically different, we assume them separate and group all the communication modules as a part of the communication level.

Communication security is arguably the most well-studied security challenge in smart city and IoT. Although this has made it easy to improve the security of this level by employing off-the-shelf techniques, it has also made it the target for many cyberattacks, as its strength and weaknesses are better known in comparison to other levels. Furthermore, in many smart city applications, the communication level joins non-IoT local networks at some point. Therefore, compromising a node through network attacks can endanger other non-IoT devices that share the networking infrastructure, including laptops and smartphones. IoT wireless networks are usually attacked by eavesdropping, jamming, and message injection. As discussed in (Kolias, Stavrou, Voas, Bojanova, & Kuhn, 2016), WiFi is vulnerable to man-in-the-middle attacks. This attack is typically defined as the *manipulation* of the messages from a sender to a receiver by an adversary, which is left unnoticed by both ends (Krimmling & Peter, 2014) (and hence it is alternatively referred to as *manipulation* attacks (Suo, Wan, Zou, & Liu, 2012)). ZigBee, too, is prone to replay attacks as it lacks a robust mechanism to evaluate the freshness of packets (Kolias et al., 2016). Both ZigBee and WiFi are very common in smart city implementations.

Smart city communication implementations are oftentimes vulnerable to manipulation attacks. Particularly, those targeting the network layer right after the introduction of a new device are known to be very effective. The mobile and distributed nature of IoT further exacerbates this vulnerability, as it substantially complicates the successful verification of end devices (Covington & Carskadden, 2013). Man-in-the-Middle attacks primarily exploit the inherent weakness of the session key establishment process in smart city applications. Ye, Zhu, Wang, Malekian, and Qiao-min (2014) propose a secure access control method to establish the session key according to the authentication of mutuality between the sender-receiver pairs. The proposed methodology is based on Elliptic Curve Cryptography (ECC). It restricts data transmission to genuine nodes that have undergone a two-stage authentication. Data is particularly vulnerable during its transmission from the network edge to the cloud servers. Systematic approaches are, therefore, required to ensure the security of information. A highly abstract three-component architecture consisting of a (i) perception layer, (ii) network layer, and (iii) application layer can combat these vulnerabilities (Puthal, Nepal, Ranjan, & Chen, 2016). Designing a system at such an abstract level makes it compatible with many IoT applications. However, every design process must address the nuances of each application (See Section 5 for more details).

An effective security and privacy preserving initiative must include all network layers. Encryption can be used to validate both the authenticity—to detect spoofing—and integrity (Zhou, Cao, Dong, & Vasilakos, 2017). Encryption techniques, however, cannot provide immunity against side-channel attacks. Additionally, running robust encryption on resource-limited devices is challenging. One promising solution is Advanced Encryption Standard (AES) as its required energy consumption and memory usage are economical, thereby making it suitable for 8-bit microcontrollers (Honan, Page, Kocabas, Soyata, & Kantarci, 2016); particularly, many chips benefit from dedicated AES modules that accelerate encryption and decryption. Alternatively, Elliptic Curve Cryptography can provide very robust security while using less memory. This reduction in memory usage is achieved by using smaller keys. However, it does not support processing encrypted data (they must be first decrypted) (Kocabas et al., 2016).

The communication level of the majority of IoT application includes an *adaption* layer that provides compatibility with IP. IPv6 over Low power Wireless Personal Area Network (6LoWPAN) protocol is a widespread selection. It provides multiple security configurations to preserve authentication, encryption, and confidentiality (Habibzadeh, Soyata, Kantarci, Boukerche, & Kaptan, 2018; Hennebert ö Santos, 2014). 6LoWPAN is also compatible with IPSec, which can provide security, regardless of whether the application layer includes any security mechanism or not (Hennebert & Santos, 2014). In the Application layer, the Constrained Application Protocol (CoAP) is mostly used in smart city and IoT applications, as it provides efficient compatibility for HTTP and the web. To ensure security and privacy CoAP uses Datagram Transport Layer Security (DTLS) and IPsec. DTLS is similar to TLS, but it is designed for UDP, which makes it more IoT-friendly. The authors in (Singh, Pasquier, Bacon, Ko, & Eyers, 2016), suggest that all data transfers in a smart city application must be protected by TLS, including data transfers among the servers—even if they are operated by the same provider.

4.3. Data processing and storage level vulnerabilities

Many smart city services are cloud-based, meaning that the data of in-field sensors is eventually transmitted to a centralized server. Cloud-based servers are preferred because (i) they are powerful and can perform complicated algorithms, (ii) they can be scaled to meet the ever-changing requirements of a smart city, and (iii) cloud is always available (Singh et al., 2016). Cloud servers must provide real-time services to a large number of clients, simultaneously. Therefore, they are typically designed to be resourceful. As the power, size, and computational capabilities of cloud servers are not a limiting factor in this level, it is suggested that, whenever possible, advanced and complicated security and privacy measures should be implemented (Zhou et al., 2017). Cloud-based servers are the convergence point of all the data collected in a smart city application; thus, any security breach can endanger the privacy and safety of a large number of users, and can subsequently lead to more severe and larger scale consequences. This is in contrast to security threats of data acquisition and communication levels, which can impact only a user or a small group of them. As the result, the importance of security in cloud servers cannot be emphasized enough.

Servers in a cloud-based smart city application are prone to different attacks, such as DoS, malicious data injection, spoofing, and data leakage (Zhang, Ni, et al., 2017). It is possible to improve the immunity of the system against such attacks by using commonly used techniques such as *encryption*, *anonymity*, and *access control* (Zhang, Ni, et al., 2017). However, the inherent characteristics of IoT raise multiple challenges in deploying such off-the-shelf techniques. Advanced data encryption is an effective way to provide security and privacy; although, it is normally not possible to process encrypted data. In private servers, where the servers are owned and controlled by only one smart city provider, this limitation does not raise serious concerns. However, many smart city applications rely on public servers to benefit from the advantage of scale and reduce their costs. Public servers typically provide multiple services to different clients simultaneously. Therefore, decrypting data before processing can expose them to attacks and leakage (Kocabas et al., 2016; Singh et al., 2016; Zhang, Ni, et al., 2017). *Fully homomorphic encryption* (Honan et al., 2016; Kocabas et al., 2013; Page, Kocabas, Soyata, Aktas, & Couderc, 2014) can address the requirement. It enables servers to apply algorithms to encrypted data, without first requiring them to be decrypted. However, homomorphic encryption is still mostly considered as an untrodden field. Unfortunately, current homomorphic algorithms suffer from a significant performance penalty, which makes them impractical in many applications. Furthermore, cryptography does not improve the immunity of the system against hardware and side-channel attacks such as timing attacks, power attacks, and cache attacks (Kocabas et al., 2016). Nonetheless, techniques such as Montgomery's multiplication (Koc, Acar, & Kaliski, 1996) and randomizing computations (Okeya & Sakurai, 2002) can enhance the system's robustness against these threats.

The anonymity of users can be protected by conventional methods such as pseudonyms. However, the system must be able to identify the users in case of a dispute (Zhou et al., 2017). Furthermore, some smart city service providers might intentionally gather information about their users for either future use or selling to third parties. Many smart city applications require flexible file sharing platforms. Conventional solutions that involve public/private key schemes are not applicable to these modern scenarios as they require an additional copy of data for every data access request (Kocabas et al., 2016). Clearly, in applications such as smart healthcare with intricate data access patterns, these solutions can become prohibitively complicated. Attribute-Based Encryption (ABE) must be used in these cases (Kocabas et al., 2016).

The dynamic nature of the smart cities requires a continuous *authentication* and verification method for participating devices. This nontrivial problem can be best addressed by employing hybrid solutions, which combine novel conceptual designs—such as defining social relations between the nodes, identifying behavioral patterns, etc.—with conventional biometrics-based authentication techniques. Defining relations among smart objects (first introduced in the work by Holmquist et al. (2001)) is perceived as socialization of smart objects. A conceptual review of the IoT-social network integration is presented in (Ding, Shi, & Liu, 2010), which can form a basis for continuous and/or behavior-based authentication in smart city applications. An example study of such authentication mechanisms based on the social interactions of users is conducted in (An, Gui, Zhang, & Jiang, 2011). Despite its negative impact on performance, biometric authentication remains a viable solution for secure and continuous authentication. Biometric-based solutions authenticate users using either their physiological (e.g., fingerprint and facial features) or behavioral biometrics (e.g., gait and handwriting) (Sultana, Paul, & Gavrilova, 2014). When conducted *implicitly*, behavioral authentication paves the way for robust, convenient, and non-invasive authentication. For example, users can be authenticated by analyzing their interactions with smartphones, web browsing habits, and location history (De Luca, Hang, Brudy, Lindner, & Hussmann, 2012; Feng et al., 2012; Gascon, Uellenbeck, Wolf, & Rieck, 2014; Khan, Atwater, & Hengartner, 2014; Khan & Hengartner, 2014). As opposed to authentication by (say) fingerprint scanning, behavioral solutions do not require users' explicit attention, hence the term *implicit* authentication.

Various studies conducted in the literature prove the applicability of behaviometrics-based authentication to a diverse range of applications. For example, the authors in Crandall and Cook (2013) show that this technique can substantially facilitate the interaction between users and their surrounding in smart environment implementations. In another study (Budurusubmi & Yau, 2015), the authors enable smartphone user to unlock their devices by analyzing their touchscreen gesture patterns. Similar studies are conducted in the literature to investigate the growing role of behavioral authentication in smart cities (Batty et al., 2012; Khatoun and Zeadally, 2016).

In Anjomshoa, Aloqaily, Kantarci, Erol-Kantarci, and Schuckers (2017), the authors study the behavioral patterns of mobile users on several various social network platforms with the aim of continuously verifying users on their smart handheld devices. The main motivation of this idea is that users' mobile devices can be recruited for large-scale non-dedicated sensing campaigns. Fig. 3 presents a minimalist view of the system architecture. The authors aim at mitigating the drawbacks and/or inconvenience of the conventional verification schemes such as pin codes/passwords or fingerprints/face recognition. The former category faces inevitable security vulnerabilities as mentioned by many researchers (Zhang & Li, 2011) whereas the improved security introduced by the latter comes at the expense of implementation cost (Dantcheva, Elia, & Ross, 2016; Liu-Jimenez, Sanchez-Reillo, & Fernandez-Saavedra, 2011; Meng, Wong, Furnell, & Zhou, 2015; Poursaberi et al., 2013). The mobile behaviometric framework monitors and assesses social activity on mobile devices through newly introduced sociability metrics.

5. Domain-specific security challenges of smart city applications

As almost all smart city applications share the same stratum, they remain susceptible to the same vulnerabilities (as discussed in Section 4). However, the nuances of each application also entail domain-specific considerations. This section is dedicated to studying these particularities. Because the concept of the smart city encompasses a wide range of applications, a thorough study of each possible domain exceeds the scope of this paper. Nonetheless, the included applications form (arguably) the backbone of the smart city. Additionally, each application, in the context of this section, should be envisioned in a broad concept. For example, the provided discussion on smart homes remains fairly applicable to smart buildings and smart environments as well.

5.1. Smart health

The traditional healthcare typically requires the physical presence of patients in hospitals. The patients first need to be hospitalized, where the professional and trained staff can monitor their biomarkers and assess their health status (Honan et al., 2016; Page et al., 2015). This rather *archaic* approach fails to provide real-time and continuous monitoring, which is a requirement for successfully diagnosing and remedying chronic diseases such as cardiovascular disorders, diabetes, and hypertension (Honan et al., 2016). The design of a reliable system that can provide real-time, personalized, and clinical-grade digital health information has been addressed by creating *smart*—or equivalently *digital*—health (Shishvan et al., 2018). The progress in smart health is mostly due to recent innovations in the CPS arena; as devices have become inexpensive, non-invasive, bio-compatible and accurate enough for personal and clinical use, their application in an IoT-based CPS becomes feasible. Further contributing to the realization of smart healthcare, the advances in Wireless Body Area Networks (WBAN)

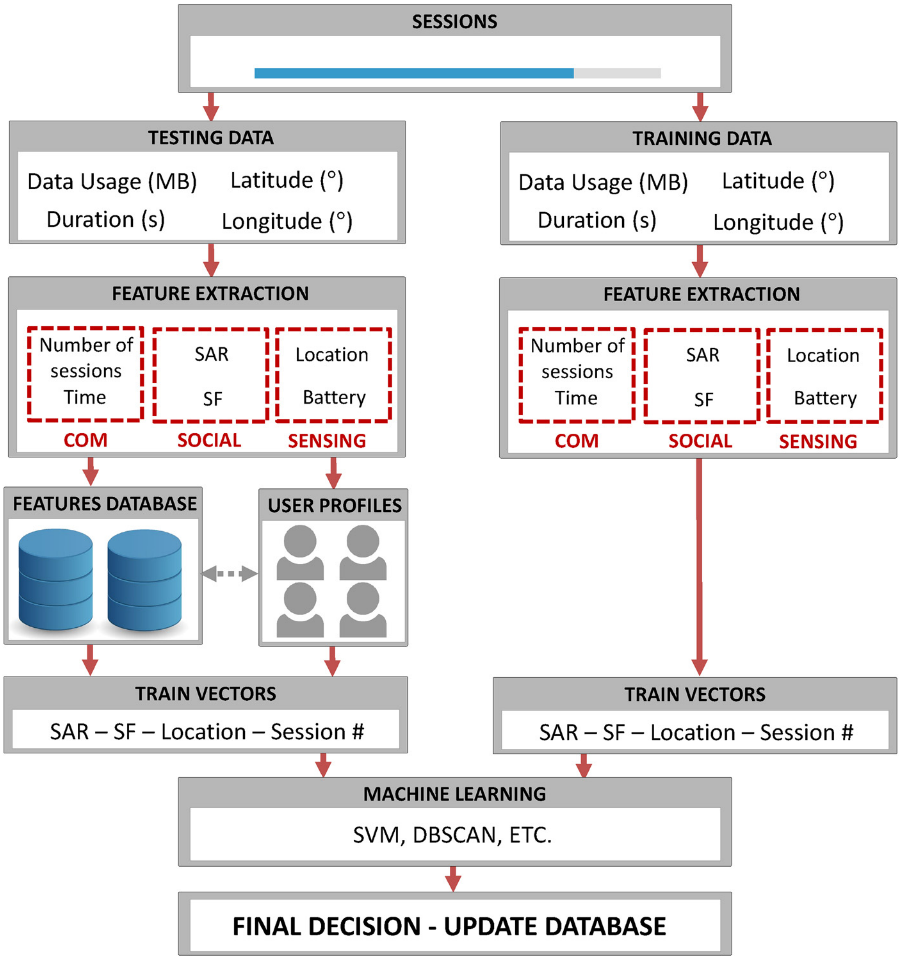

Fig. 3. Continuous behavioral authentication mechanism developed in (Anjomshoa et al., 2017) encompasses five modules for monitoring, data acquisition, normalization, training, and verification.

(Habibzadeh et al., 2018) have removed many obstacles against low-cost, reliable, and ubiquitous communications. Additionally, modern data analytics and machine learning can analyze and correlate collected data to assist medical personnel with decision-making and provide real-time and personalized recommendations to users. Smart health systems can now reliably measure cardiovascular parameters (Mahbub et al., 2017; Rachim & Chung, 2016), blood pressure (Kachuee, Kiani, Mohammadzade, & Shabany, 2017), respiration variables (Liu, Cao, Tang, Wen, & Guo, 2016; Reyes, Reljin, Kong, Nam, ö Chon, 2017), etc. Non-invasive commercial products such as Apple watch (Apple Inc., 2017a) and Fitbit (FitBit Inc., 2017) can provide fitness related information. More technical sensors and devices such as MC10 (MC10 Inc., 2017) products can also provide clinical grade information.

Parallel to the evolution of smart healthcare systems, threats and attacks that target users' privacy have also increased in complexity and frequency. Two mega-trends transpiring in the field can be primarily associated with these developments. First, the ever-increasing application of sundry implantable, wearable, and ambient sensors increases the odds of sensitive data leakage (Piwek, Ellis, Andrews, & Joinson, 2016). These vulnerabilities span almost all smart healthcare services, from clinical devices (e.g., privacy vulnerabilities of some cardiac devices exposed in 2017 by the Food and Drug Administration (FDA Safety Communication, 2018)) to casual fitness sensors such as smartwatches and fitness bands (e.g., BLE-based communication can be compromised to reveal sensitive information about users' physical activities (Das, Pathak, Chuah, & Mohapatra, 2016)). Second, the *cloudification* of smart healthcare not only creates a centralized single point of failure but also enables adversaries to gain valuable insight by taking advantage of data fusion (Zhou et al., 2017). For example, in the recent incident reported in Rogers (2018), the publication of seemingly unimportant data of an activity tracking application (collected from smart wearables) led to an unexpected data leakage about sensitive locations such as military bases.

Cyber attacks that target smart health systems can easily lead to privacy violation of the patients, as health data is very sensitive. Due to this sensitivity, the Health Insurance Portability and Accountability Act (HIPAA) 104th Congress Public Law 191, 1996 mandates smart healthcare services providers to respect and protect the privacy of their patients (Ara, Al-Rodhaan, Tian, & Al-Dhelaan, 2017; Kocabas et al., 2013). Hence, it is critical to ensure that the new innovations in smart healthcare field meet the requirements of HIPAA (The reader should be aware of ongoing efforts to relax HIPAA requirements, with the intent of reducing regulations and motivating innovation and production (Knopf, 2019)).

A major complication in smart healthcare applications stems from the large number of stakeholders and their indeterministic roles. The personal data of the patients must be shared with hospitals, physicians, specialists, pharmacies, insurance companies, etc. Additionally, some constituents of smart healthcare (e.g., first responders) require on-demand and temporary privileges. This complication entails two requirements. First, the existing data must be digitized in a standard format (to generate electronic health records or EHR) and second, the EHRs must be securely and effectively shared with multifarious constituents of smart healthcare. HIPAA-compatible standards such as OpenEHR and Health Level Seven International (HL7) can address the former requirements, although their variety still raises interoperability concerns (Blobel, 2018). The latter requirement is typically fulfilled by novel data sharing protocols as conventional file sharing mechanisms are ineffectual in the dynamic environment of smart healthcare.

A typical EHR may include comprehensive information about a patient. A secure model should allow access only to the portion that is relevant to the requester's role. This, however, should not limit a stakeholder's ability to search the entire record for relevant information. Attribute-based decryption (ABE) is an effective approach to provide diverse access control privileges, which makes it particularly applicable to cloud-based smart healthcare scenarios. In ABE, the owner of the data (e.g., the patient) determines access policies based on attributes and relationships. The users can access an entry in EHR if their attributes match the designated policy. This is an effective solution when attributes and relations are static. However, it fails to provide *justified* temporary access to new users (e.g., allowing access to first responders during an emergency). Therefore, access control should be “self-adaptive” and differentiate between normal and emergency situations. A self-adaptive system involves a master key that is shared with the patient and their emergency contacts. The emergency units need to communicate with these emergency contacts to obtain the password and gain access to complete health record of the patient (Yang, Zheng, Guo, Liu, & Chang, 2019).

Notwithstanding its remarkable performance for protecting on-cloud data, ABE computational complexity makes it inapplicable to WBAN technologies, which constitute the front-end of smart healthcare. In these scenarios, it might be productive to revert to more conventional solutions augmented with new improvements. Particularly, for WBANs, identity-based access control provides a practical balance between simplicity and security. Additionally, efficient Certificateless Signcryption (SLSC) can further reduce the energy consumption and computational demands of the algorithm. SLSC also benefits from the advantage of improved security, as the service provider only dispenses partial keys (hence eliminating the need for a completely trustful server) (Li, Han, & Jin, 2018).

ABE and identity-based access control can deliver access management for the back and front-end of smart healthcare, respectively. Both of these solutions, however, rely on central servers, which impedes their applicability to ever-growing distributed implementations. Blockchain-based access control is a nascent technology that aims to address this limitation. Rather than storing the entire EHR on the blockchain, the existing works merely employ it as an access control mechanism (meaning that the blockchain only stores references to data), which enables the data owners (e.g., the patients) to have complete control over sharing their information. This reduces the storage overhead of the blockchain but creates a weak link in the central node that stores the EHR of a patient. Despite its increasing popularity, blockchain is not a panacea for EHR sharing. The platform remains always vulnerable to 51% attacks. Additionally, tracking the transactions of a user can reveal their visiting patterns, hence compromising their privacy. Blockchain-based access control is also inherently complicated. This adds to the access delay and can result in inconvenience for users (Dagher, Mohler, Milojkovic, & Marella, 2018). Table 3 lists some of the major challenges in healthcare security. These challenges involve various domains of the healthcare; the most important of which are listed in the table.

5.2. Smart transportation

The main purpose in smart transportation (also called *intelligent* transportation) is to improve the safety of roads and to provide a more convenient driving experience (Habibzadeh, Qin, et al., 2017), using either dedicated (Datondji, Dupuis, Subirats, & Vasseur, 2016) or crowd sensing (Calabrese, Colonna, Lovisolo, Parata, & Ratti, 2011). It involves various aspects of transportation. Smart parking services address the challenge of finding a vacant parking spot in busy cities (Chatzigiannakis, Vitaletti, & Pyrgelis, 2016). Smart driving applications employ various technologies to assess and evaluate the status of the road and assist the driver accordingly with the goal to prevent accidents and improve the safety of the passengers and other drivers (Teichmann, Weber, Zoellner, Cipolla, & Urtasun, 2016). Some smart driving technologies also analyze the status of the driver to detect if they are sleepy, stressful, or distracted (Yamaguchi & Sakakima, 2007). Other systems aim to improve public transportation and provide citywide services, which allow them to guarantee the smooth flow of traffic (Brisimi, Cassandras, Osgood, Paschalidis, & Zhang, 2016). Smart transportation can also overlap with smart healthcare, where traffic manipulation is used to minimize the response time of emergency units. It can assist law enforcement in addressing traffic incident disputes (Wu & Horng, 2017). Because fixed sensors can only provide highly localized information, many smart transportation systems include a large number of non-dedicated sensors in their front-end (Habibzadeh, Qin, et al., 2017). Moreover, a substantial portion of the sensors used in smart transportation is incorporated within the vehicles, which implies a mobile and highly dynamic framework. Smart transportation also involves infrastructure sensors and actuators that facilitate the interaction between vehicles and roads. Infrastructure units must reliably serve multiple clients simultaneously, which increases their computational and energy-consumption requirements. Hence, they are either implemented as grid-connected or self-sufficient devices with energy harvesting capabilities (Habibzadeh, Hassanalieragh, Ishikawa, Soyata, ö Sharma, 2017; Habibzadeh, Hassanalieragh, Soyata, & Sharma, 2017c, 2017).

The highly dynamic characteristics of some of the smart transportation services require flexible and ad hoc architecture. Within the core of this architecture lies the Vehicular Ad Hoc Network (VANET). It allows Vehicle-to-Vehicle (V2V) communication and utilizes Road Side Units (RSU) (Rajput, Abbas, Eun, & Oh, 2017) for Vehicle-to-Infrastructure (V2I) data exchange. Such communication provides a basis, upon which vehicles can coordinate their behavior to maximize safety and improve traffic flow based on the condition of the infrastructure. Not unlike the smart healthcare that generally revolves around an individual (WBAN), smart transportation services ultimately involve individual vehicles. Vehicles, however, are significantly more resourceful than smart wearables, which implies more opportunities for advanced on-site data processing. This resource abundance of on-vehicle nodes paves the way for *agile* communication services (using *cognitive radio*), which are crucial for overcoming many existing challenges of V2V communication (e.g., heterogeneity) (Ding, Zhang, Cai, & Fang, 2018). The proliferation of smart vehicles is currently the major driving force in the growth of smart transportation. The threats against smart vehicles can be categorized based on their vulnerability (Baig et al., 2017). Physical threats target the electronic control unit of vehicles to gain unauthorized access to data or sabotage the operation of the vehicle. Interception attacks intercept the data transmission within the vehicle or between the vehicle and the cloud. The reliance on communication technologies and operating systems such as Android Auto or Apple's CarPlay leaves smart vehicles susceptible to known vulnerabilities of these systems.

Although privacy leakage—especially for location data—is important in smart transportation, it is not as disquieting as in smart health applications. Instead, the ramifications of the cyber attacks on smart transportation mostly include safety concerns and economic losses. For example, it is shown that radio signals can interfere with the smart vehicle braking system, which directly threatens the safety of the occupants and other drivers. Furthermore, an attack on public transportation systems—such as the one on the Bay Area Rapid Transit (BART) (Bay Area Rapid Transit, 2017)—may inflict substantial financial losses. Adversaries can generate falsified data to manipulate the traffic to their advantage, which hints at the significance of evaluating data trustworthiness and authentication in smart transportation (Guo et al., 2017). These attacks, when transpired in the intricate ecosystem of smart transportation, are particularly difficult to detect and

Table 3
Some major challenges in smart healthcare security and privacy along with domains they affect.

Challenges	Domain	Trends	Comments
Data Sensitivity/Multi-Faceted Heterogeneity in Privacy &Security Requirements/Number and Dynamic Roles of Stakeholders	Structure & Architecture	Cloudification, Edge-Computing, &Hybrid Architectures	Cloudification increases latency, limits scalability, and creates single-point-of-failure. Edge-computing causes availability issues and is not compatible with many existing data analytics algorithms.
	Access Control	Attribute-Based &Identity-based Access Control	These are used for back- and front-end respectively. ABAC entails a central implementation. It does not provide emergency access privileges, effectively and burdens the front-end. ABAC has also poor scalability.
	Data Sharing & Semantic Extraction	Standardized EHR, Blockchain, &Natural language Processing (NLP)	NLP is used to process unstructured data such as EHR. EHR standards (e.g., OpenEHR) promise good inter-family interoperability while meeting many requirements for secure information sharing regulations. However, different formats of different standards are not typically compatible.

countervail. This mirrors the significance of Intrusion Detection Systems (IDS), which are critical to smart transportation security. There are two general approaches to IDSs. The common implementations use a database of known attacks and their signature to detect irregularities in the network's behavior. This *signature*-based solution is very effective against known vulnerabilities but falls short of protecting the system from zero-day threats. Alternatively, *anomaly detection*-based solutions analyze the current status of the system to detect irregularities. This can provide security against zero-day attacks albeit the overall accuracy is typically lower. Various implementations for IDS have been proposed in the literature. Some adopt the principles of game theory to model the intricate competition between the defender and adversary. These two agents typically aim to maximize their utility while considering the optimal response of their competitors. Game theoretic solutions are applicable to distributed architectures and are proven efficacious in the context of large-scale systems (Sedjelmaci, Hadji, & Ansari, 2019). However, their performance remains reliant on various assumptions e.g., the rules of the game and whether or not the adversaries are cooperative. Hybrid machine learning (ML) techniques that integrate multiple ML algorithms are also proven effective (Aloqaily, Otoum, Ridhawi, & Jararweh, 2019). ML-based approaches, however, rely on feature extraction techniques which pose two major challenges. First, extracting the most salient features is oftentimes complicated. Second, adversaries can eventually learn the relevant features and engineer their attacks accordingly (Diro & Chilamkurti, 2018a). The growing deep learning (DL) techniques can mitigate this drawback as they operate on raw data. Additionally, DL-based IDSs are more robust against zero-day attacks (as DL is more tolerant of small changes in data than ML) (Diro & Chilamkurti, 2018b). Nonetheless, DL algorithms require large and high-quality training datasets (van der Heijden, Dietzel, Leinmller, & Kargl, 2019).

Location-based services are inherent to smart transportation applications, which inevitably raises privacy concerns. The existing solutions for protecting users' location privacy offer a trade-off between computation and communication requirements. Pseudonyms are arguably the most widely used approach. However, pseudonym management is typically centralized, which raises concerns about its scalability and latency; especially considering the increasing number of connected vehicles. Distributed pseudonym management systems that utilize edge-computing can mitigate this problem (Kang, Yu, Huang, & Zhang, 2018). Spatial cloaking (e.g., *k*-Anonymity and *l*-diversity) adds to communication's overhead, while homomorphic encryption complicates computations (Lin, Niu, Li, & Atiquzzaman, 2019). VANETs are also susceptible to a diverse range of cyber attacks. Intercepting or eavesdropping attacks may steal some of the critical information about the vehicle and its driver because beacons transmitted by each vehicle contain a unique ID and location-related information (Rajput et al., 2017). Table 4 summarizes IDS and privacy of location-related data as the major security and privacy dimensions of smart transportation along with some suggested solutions.

5.3. Smart grid

Smart grid applications improve the efficiency of power generation, distribution, and consumption, which not only reduces costs but also decreases pollution and retards the climate change. A modern smart grid application must be particularly compliant with renewable energy sources and energy storage blocks. They must provide tools for handling complex modern smart grids, self-healing feature, and compatibility with emerging electric vehicles (Eder-Neuhauser, Zseby, & Fabini, 2016). Three objectives can be enumerated for smart grid services: (Chu & Iu, 2017) (i) converting the currently centralized energy network to a more decentralized system, (ii) improving network management and monitoring in order to add to the system's resilience, and (iii) analyzing the bulk of information system-wide to improve efficiency and prevent blackouts. Example applications of smart grid include pricing in real-time, managing demand, and distributed generation—which is also an implication of the propagation of renewable energies. Making the grid decentralized also increases its resilience against different types of attacks, natural disasters, and human errors (Eder-Neuhauser et al., 2016).

Advanced Measuring Infrastructure (AMI) is a key component of the smart grid. It facilitates the interaction between consumers and operators. Consumers benefit from AMI as it allows them to accurately monitor their consumption and take full advantage of dynamic pricing policies. It benefits operators by enabling them to automatize meter readings, which improves accuracy and reduces costs. At the heart of the smart grid, the Supervisory Control and Data Acquisition (SCADA) manages the entire network. It collects AMI's data, processes them, and makes decisions to adjust the grid based on its real-time status (Tan, De, Song, Yang, & Das, 2017).

Similar to other smart city services, smart grid applications are highly dependent on communication technologies (Kalalas, Thrybom, & Alonso-Zarate, 2016) (especially, technologies such as power line communication, ZigBee, IEEE 802.11 h, Bluetooth, etc. (Habibzadeh et al., 2018)). Making the grid *intelligent* and integrating it with the cyber world renders the system vulnerable to various cyber attacks threatening the system's availability, integrity, and privacy. At the lowest level (data acquisition level), the smart grid CPSs are prone to attacks that manipulate the readings of smart meters and pricing policies (energy theft). Moreover, as power consumption can reveal valuable information about the occupants of a building, their habits, and their lifestyle, privacy-violating attacks such as eavesdropping and intercepting are also important in a smart grid. The existing countermeasures against energy theft can be broadly categorized into state-based, game theory-based, and data analytics-based solutions. State-based solutions use state equations to model energy consumption. This way, possible biases in state estimators (e.g., Kalman filter) can be

Table 4
Two dimensions of security and privacy are particularly important in smart transportation systems. This table tabulates the main trends in each solution.

Challenges	Domain	Trends	Comments
High-Accuracy/Highly Dynamic/ Low-Latency &Delay-Intolerance	Intrusion Detection Systems (IDS)	Game-theoric Models, Machine Learning, &Deep Learning Models	The performance of models that use game theory mostly depends on their assumptions about the game rules. Similarly, the performance of ML solutions highly depends on proper feature extraction, which is not straightforward. DL requires a large amount of training data.
	Location Data Privacy	Pseudonyms, Cloaking, & Homomorphic Encryption	Pseudonyms management is centralized, which causes additional latency. Cloaking techniques cause communication overhead while Homomorphic encryption is computationally expensive.

interpreted as power consumption irregularity, which can potentially imply malicious activity (Salinas & Li, 2016). This is an effective approach but sometimes it requires multi-sensor data fusion (McLaughlin, Holbert, Fawaz, Berthier, & Zonouz, 2013), which can incur additional installation costs. Alternatively, the interaction between energy companies and energy thefts can be modeled as a game to structure an inexpensive energy theft detection mechanism. The performance of these solutions, however, mostly relies on the game rules (e.g., defining utility functions), which are oftentimes not easy to determine (Jokar, Arianpoo, & Leung, 2016). Many emerging studies use ML and DL to detect irregular energy consumption (Yip et al., 2017). These algorithms typically deliver impressive accuracy; however, they require high-quality training data. Additionally, ML algorithms oftentimes fail to differentiate between malicious users and innocuous events (such as new tenants in of a building); therefore, they suffer from high false positive rates. To protect users' privacy during processing, FHE can be applied (Yao et al., 2019).

Smart grid cybersecurity should equally emphasize both software and hardware aspects, thereby providing communication and device security. Fulfilling this vital requirement demands early countermeasure against cyber attacks. This is, however, not an easy task to undertake as the extent of smart grid systems (which may even span an entire country) provides ample attack opportunities for adversaries (Kabalci, 2016). Furthermore, even a relatively small subset of compromised devices are adequate to disturb the delicate balance of the smart grid and, hence, causing a domino-like chain of failures. These complications give rise to attack prevention, detection and mitigation models. Reducing the communication between the field (home area networks and building area networks) and the control center lowers the chances for privacy leakage and possible cyber attacks. This can be achieved by localizing some of the computations to field devices and hence making them more independent; building area networks can provide some level of management to locally distribute the load among home area networks by estimating their expected demand. In many cases, the deviation from the expected load can be handled by redistributing the load among different home area networks without involving the control center. This effectively increases the immunity of the system against outsider attacks (Abdallah & Shen, 2017). Attack detection in the context of the smart grid oftentimes involves evaluating data for anomalies and inconsistencies (falsified data do not comply with physical rules of electric circuits). Conventional detection solutions utilize these anomalies to expose attacks, where the deviation in key parameters of the grid (e.g., power and phase) passes a given threshold (meaning that deviations are inexplicable using physical rules, even after accounting for expected noise). This approach, however, fails to detect stealth attacks, where the adversary, aware of the network's topology and status, ensures that data manipulations do not violate the system's norms. This necessitates more powerful tools for anomaly detection. Both supervised and unsupervised solution can surmount these complexities, although the scale of the smart grid causes dimensionality issues (principal component analysis is shown to be effective to battle this problem) (Esmalifalak, Liu, Nguyen, Zheng, & Han, 2017). Machine learning solutions utilize past smart grid data to develop statistical models, which can later be used to detect outliers. A cyber attack involves compromised nodes that aim to undermine the integrity and availability of the system. An attack mitigation model employs trusted nodes to counterbalance the wrongdoings of adversaries. These interactions between two competing entities naturally lead to game-theoretic solutions that can approximate the complex nonlinear behavior of participants without having full knowledge of their action-taking process (Srikantha & Kundur, 2016).

The scale and complexity of the smart grid, coupled with the sheer number of stakeholders involved, significantly complicate the intrusion detection problem. Cyber attacks are getting more insidious, where adversaries perform their attack in extended time frames to gradually infiltrate the network. As mentioned in the preceding discussion, this hints at the importance of modern intrusion detection systems (IDS) in the context of the smart grid. An alternative to game-theoretic solutions, immune theory and principles of artificial immune systems provide a solid basis for the development of an effective IDS. Such systems include antigens and detectors—typically categorized as immature, mature, and memory detectors,—which can identify and neutralize intrusions. The remarkable performance of these systems, however, stems from their ability to dynamically evolve, which renders them effective against unknown threats as well. The proper execution of this methodology hinges on establishing an information library. The content of this library along with the detected attacks is then used to alarm the system manager (Liu, Yang, Zhang, Chen, & Zeng, 2011). Artificial immune systems, however, are a growing field. Therefore, their applicability to real-world scenarios is not completely known (Pump, Ahlers, & Koschel, 2018).

Forestalling *spoofing* cannot be assured by solely relying on conventional encryption and authentication techniques. Instead, it requires more comprehensive solutions. SVELTE (Raza, Wallgren, & Voigt, 2013) is proposed as a real-time intrusion detection system for the IoT to detect sinkhole and selective forwarding attacks. SVELTE was initially designed for a Low-power Wireless Personal Area Networks with IPv6 (6LoWPAN) (Kushalnagar, Montenegro, & Schumacher, 2007) that uses message security technologies to provide end-to-end message security. The main components of SVELTE include: (i) 6LowPAN Mapper (6Mapper), which collects data about the status and performance of the network and uses RPL to establish links and routes among nodes, (ii) intrusion detection, which secures the network against intrusions, and (iii) distributed firewall, which controls the traffic to and from the network and blocks malicious packets. In case no particular implementation of IDS can fulfill the requirements of an application, hybrid solutions are also proposed in the literature (Krimmling & Peter, 2014) (Table 5). Table 5 tabulates the major security dimensions of the smart grid, as well as some typical challenges and prominent solutions.

5.4. Smart home

The smart home ecosystem involves smart appliances, which primarily focus on providing convenience, e.g., smart refrigerators that can keep track of users' shopping list. Many smart home services involve improving energy consumption (which implicitly binds them with the smart grid). Smart Heating, Ventilation, and Air Conditioning (HVAC) systems fall into this category (Yan, Zeng, Liang, He, & Li,

Table 5
Privacy and Security of smart grid systems include two major dimensions to battle energy theft and stealth insidious attacks.

Challenges	Domain	Trends	Comments
DDoS Attacks/Large Scale/ Stealth Attacks	Energy Theft	State-based, Game Theory-based, ML &DL-based Detection	State-based solutions do not require extensive data selection but the may incur an additional cost. Game theory is inexpensive but relatively less effective. ML and DL require training data and can introduce privacy concerns.
	Attack Prevention, Detection, &Mitigation	Game-Theory, ML &DL, Artificial Immune Systems	Game-theory based solutions are effective against stealth attacks as they can curb the damages. Machine learning based systems require training datasets that are inclusive enough for overcoming heterogeneity. artificial immune systems are not applied to real-world applications, hence, their applicability is doubtful.

2017). Some applications provide security services e.g., home access control through doors and windows, break-in detection, and fire detection systems (Jose & Malekian, 2017). An interesting application is when the smart home and smart health meet. For example, a home-wide fall detection service can detect fall incidents for the elderly (Stone & Skubic, 2015). Notwithstanding these multifarious advantages, the widespread adoption of smart home technologies still faces many challenges. Particularly, security and privacy concerns are known to be a major hindrance (Wilson, Hargreaves, & Hauxwell-Baldwin, 2017). Social implications of smart homes also require further investigation, as these technologies can sway the control to tech-savvy residents or even third-parties (Gram-Hanssen & Darby, 2018).

Generally, smart home applications are cloud-based. Numerous frameworks such as Home Kit (Apple Inc., 2017b), SmartThings (Samsung Electronics Co., 2017), and Weave (Google Inc., 2017) can provide various ready-to-use smart home services without requiring a complicated and costly setup (Fernandes, Rahmati, Jung, et al., 2017). This reliance on various cloud-based services and technologies, however, inevitably leads to excessive fragmentation, which evinces itself in sensing, communication, security, and processing dimensions of smart home systems. Circumventing this heterogeneity is a major unresolved challenge in smart home technology. A suggested solution utilizes hierarchical cloud architecture to consolidate the services of independently-operated cloud servers. This solution involves a mediator, which dispenses commands and requests among various independent servers and enables them to remain synchronized. By identifying the relationships among various security feature, ontology-based security is used to ensure security interoperability (Tao, Zuo, Liu, Castiglione, & Palmieri, 2018). The dependence on the cloud, however, brings about a major reliability ramification; being the single point of failure, any accidental or intentional interruption in the cloud's operation can render the smart home unavailable and leave it susceptible to security threats. In-home processing services can mitigate this vulnerability. This approach involves a local processing hub that remains constantly in sync with the cloud. Upon any interruption in connectivity with the cloud, this hub assumes control of the smart home to provide basic services (e.g., maintaining the operation of surveillance systems or safety sensors) (Doan, Safavi-Naini, Li, Avizheh, & Fong, 2018).

Making homes *smart* has exposed them to new threats; in addition to conventional security vulnerabilities, smart homes are now prone to cyber attacks and cyber thieves. Constituting the communication framework of the system, many smart home services also share the weaknesses of wireless LAN protocols (WLAN), implying their vulnerability against routing and wormhole attacks (Jose & Malekian, 2017). Particularly, data leakage can reveal information about the residents' lifestyle. For example, it is possible to use the data of an IR sensor to determine when residents are home. For applications that primarily target security, sabotaging the system can compromise the security of the entire home. Even more disturbing is that some available smart home devices fail to adopt even the most fundamental communication security services (which are, thanks to existing off-the-shelf solutions, relatively easier to implement in comparison to say hardware security.) These devices are typically shipped with simple default passwords, which many users neglect to alter. Even in the presence of strong passwords, spoofing and firmware attacks can compromise the equipment (Ling et al., 2017).

Fulfilling privacy and security requirements of smart homes typically revolves around standard cryptography including TLS and SSL. These solutions, however, can be quite expensive for resource-constrained smart home devices. Many lightweight key-establishment mechanisms based on symmetric encryption are proposed to address this drawback. However, they typically rely on trusted centralized providers, which is not a valid assumption in many smart home services. Additionally, encryption can complicate data query and data processing (Poh, Gope, & Ning, 2019). Particularly, in the context of smart homes, users' privacy is often threatened by eavesdropping. Adversaries can trace data streams to their individual source devices (by simply monitoring IP address or using ML). They can monitor the activities of these devices to infer householder's habits and lifestyles. An individual device might not reveal much information but fusing data from multiple sensors can pose a serious threat to privacy. Hence, it is important to make devices *unidentifiable* and employ mechanisms to preempt unauthorized data fusion (Kumar, Braeken, Gurtov, Iinatti, & Ha, 2017). The study conducted in (Apthorpe, Reisman, & Feamster, 2017) proposes four practices to minimize privacy leakage in smart home applications, particularly when subject to eavesdropping and analysis by last-mile entities. The first practice is a preventive method to minimize the outgoing traffic of smart devices (e.g., using a firewall). However, many devices require Internet connectivity to function (in fact, many smart home devices are over-privileged. They need cloud connectivity even though it is not critical to their operation). The second practice recommends encryption of DNS queries as they contain information about devices' identities. ML technique can still identify devices even if DNS queries are encrypted although with much higher difficulty for adversaries. The third suggestion recommends VPNs for data encryption and aggregating multiple data streams into a single one, which can make devices less identifiable. Finally, traffic shaping and injection (where devices use random delays to make their activities look more sporadic or sending decoy traffic) is effective against eavesdroppers.

Unlike other smart city applications that are administrated by professionals, householders are typically the managers of smart home devices. However, typical householders may lack the technical understanding of cyber-security. Additionally, different residents might have different priorities and interpretation of their security and privacy (Zeng, Mare, & Roesner, 2017). Hence, protecting device security becomes very crucial in the smart home context. Especially, firmware updates and platform attestation mechanisms are very important. If the device resources are limited, *delta updates* must be implemented, where only a portion of the firmware is changed. This also ensures device stability (Lin & Bergmann, 2016). However, secure boot and delta updates must be added in the design phase and many existing products lack such crucial features (Heartfield et al., 2018). Table 6summarizes the major privacy and security aspects of smart homes.

5.5. Public safety and emergency management

Public safety services focus on protecting people's security,

Table 6
Two major dimensions of smart home security and privacy considerations.

Challenges	Domain	Trends	Comments
DDoS Attacks/Large Scale/Stealth Attacks	Privacy Leakage	Standard Cryptography, Lightweight Cryptography (Symmetric Encryption), VPN &Traffic Shaping	Standard Cryptography is effective but it is often too computationally demanding for smart home devices. Proposed lightweight cryptography-based solution typically rely on trusted servers which are not always available. Traffic Shaping is effective against eavesdropping but can incur communication and latency overhead.
	Device-Level Security & System Management	Secure Boot, Firmware Integrity Attestation, &Regular Security Updates Self-Configurable Security	Householders in charge of smart home devices oftentimes lack technical knowledge of cybersecurity. Hence, devices must be regularly updated and self-configured for optimal security. However, these features must be integrated into the device from early design phases. Many existing products fail to comply with these requirements.

especially during abnormal situations such as natural disasters, attacks, riots, etc. It is important to provide supportive services shortly after a disaster. It is possible that in a disastrous situation, the backbone network is interrupted and hence the communication is not feasible (Habibzadeh, Xiong, et al., 2017). A substitute is needed in such cases to enable firefighters, police, and medical staff to communicate (Habibzadeh, Xiong, et al., 2017). Isolated E-UTRAN Operation for Public Safety (IOPS) is proposed for this purpose, which allows public safety users to communicate, even in the absence of connectivity between access points and the backhaul network (Oueis, Conan, Lavaux, Stanica, & Valois, 2017). Even if there is no infrastructure, it is possible to use easy-to-deploy access points to create a network or alternatively Software Defined Radio (SDR) networks can be employed to quickly create an LTE network—or any other type of communication such as WiFi. These deployable nodes can harvest their own power from the environment to minimize their dependence on any infrastructure (Habibzadeh, Xiong, et al., 2017).

Public safety is highly dependent on the data generated by IoT nodes. Due to its purpose (protecting public security), any successful attack can have devastating consequences. Moreover, in the case of non-natural attacks (man-made), it is possible that attackers also target the public safety infrastructure. Therefore, securing smart city public safety services is critical. Particularly, IoT-based public safety is vulnerable to unauthorized access (Butun, Erol-Kantarci, Kantarci, & Song, 2016). This vulnerability is escalated with the scale and during disasters when an alternative IoT infrastructure is quickly deployed to replace the dysfunctional one. Furthermore, the cloud-access authentication is extremely important, as public safety services typically collect sensitive information about the city and citizens. Other security-related challenges in IoT public safety authorized data sharing and data storage (Butun et al., 2016).

6. Summary and concluding remarks

The concept of modern smart city reaches far beyond what discussed in this paper. The smart city now plays an integral role in the economy, government, tourism, education, etc. Part of these emerging services can be subsumed under traditional applications. For example, smart homes are closely entangled with smart building and smart environments (e.g., smart classrooms (Kim, Soyata, & Behnagh, 2018)). This integration of services can be associated with two different attributes of smart cities. First, no concise definition of these services exists, which enables researchers to liberally interpret the domain of their application. Second, fueled by advancements in big data analytics, an emerging branch of smart city comingles once stand-alone applications to consolidated ecosystems. Electric vehicles link the smart grid with smart transportation and, less directly, with the smart home and smart healthcare (via energy management systems and traffic control for emergency situations).

This unification of services brings about various security ramifications. The dynamic and heterogeneous nature of the smart city renders traditional digital forensics ineffective, e.g., it can become difficult to determine the jurisdiction of various entities over the data as it travels through various states, countries, and organizations (Baig et al., 2017). The increasing reliance of companies on advanced cryptography also entangles digital forensics; it improves users' privacy but makes it difficult to resolve legal disputes (Baig et al., 2017). Also inherent in this unified structure is the inexorable *security disparity* among various stakeholders. Data circulates through various public and private sectors, with different security and privacy guidelines. This requires a need for secure data *mashup* techniques that enable various organizations to combine their datasets. Existing mashup solutions, however, face numerous challenges (e.g., combining data increases its dimensionality, which potentially undercuts privacy protecting solutions such as *k*-anonymity.) (Braun, Fung, Iqbal, & Shah, 2018). The increasing influence of smart city technology also furthers the pull of governments and corporations. This underlines the importance of *transparency*. It is critical to somehow incentivize these entities to keep their customers informed about the purpose and extent of data mining. The utilization of data by corporations and governments should be hence contingent upon users' consent. This is, however, not straightforward as, in many cases, users are not even aware of data collections or may not find it worthwhile to actively consent every instance of data usage (Eckhoff & Wagner, 2018). This hints at research opportunities for continuous and unobtrusive consenting techniques. In addition to the increasing data dimensionality, combining various applications into a coherent service increases the number of stakeholders. The perception of knowledge among these diverse stakeholders varies based on their interests. This substantially convolutes data presentation in cross-domain smart city services.

The recent technological advances in the radii of the smart city also bring about unanticipated security threats. Botnets, artificial intelligence, smart vehicles, and virtual reality each imparts additional security challenges (Cui, Xie, Qu, Gao, & Yang, 2018). Botnets can effectively launch DDoS attacks. AI empowers adversaries to extract sensitive knowledge from ostensibly insensitive data. Furthermore, the reliance of machine learning algorithm on input data (oftentimes in an unpredictable fashion) renders them vulnerable against data manipulation attacks, where adversaries can generate seemingly genuine input that deceives the algorithm (Fernandes, Rahmati, Eykholt, & Prakash, 2017). Smart vehicles' dependence on ICT and electronic devices gives adversaries the opportunity to seize control of the vehicle, jeopardizing the privacy and safety of occupants and other drivers. Virtual reality applications often tend to deprioritize privacy (Cui et al., 2018).

Not all vulnerabilities can be associated with software/hardware deficiencies. In fact, an all-inclusive security framework should also emphasize human errors (whether intentional or not). It is critical to unambiguously define security roles of individuals (particularly, in city administration, cybersecurity officers can often be subject to lay-offs to reduce expenses). Cities should also value security leadership and form and maintain specialized security teams to carry out routine security measures such as training, firmware updates, developing emergency response plans, maintaining communications with different vendors and services providers, etc. (Kitchin & Dodge, 2017).

There are nascent innovations in the literature that can potentially mitigate the challenges described in the section. Blockchain, coupled with software-defined networks (SDN), can significantly *virtualize* the platform, hence contributing to the practicality of decentralized implementations. In the heart of a hybrid SDN/blockchain architecture, a number of resourceful devices (controlled by SDN for increased resilience) assume the role of miners to verify transactions and form blocks. They are also responsible for performing advanced data processing. Local servers in the edge of the network provide preliminary processing and security services to end-devices in their proximity, thereby cutting the distance between end-devices and the processor (not unlike cloudlets) (Sharma & Park, 2018). From another standpoint, the game theory is increasingly being used in the context of smart city security. The applications of game theory do not limit to containing cyberattacks (See Section 5.2). It can also be used to study the effects of government's policies on corporates' decision to invest in security and privacy features of their products (for example, paying premiums for security features vs. monetarily penalizing vendors for cyber attacks and security breaches) (Li & Liao, 2018). Ontology, when applied in the context of the smart city, can help with battling many challenges of data presentation and knowledge sharing. Ontology provides a formal representation of concepts and describes the existing relations among them. This formal structuring of the domain into various components (e.g., smart city into *smart* and *city*, city into *stakeholders* and *outcome*, outcome into *sustainability*, *resilience*, *life quality*, and so on (Ramaprasad, Sánchez-Ortiz, & Syn, 2017)) makes it interpretable by computers, which in turn can provide query services to users, enabling them to extract relevant knowledge. Recommended by World Wide Web Consortium (W3C), Semantic Sensor Network (SSN) ontology receives raw (even real-time) data from sensors and converts them to interoperable semantics (Daniello, Gaeta, & Orciuoli, 2018) (refer to Gyrard, Zimmermann, and Sheth (2018) for further information). The evolution of authentication and authorization is also expected to transform the smart city. They are mostly driven forward by advances in emerging behavioral and biometrics-based techniques, where resilient and strong verification can be implemented by employing two-factor and three-factor authentication (e.g., using conventional passwords, smart cards, and biometrics) (Mishra, Chaturvedi, & Mukhopadhyay, 2015; Zhang, Zhu, ö Tang, 2017). Although effective, such solutions complicate the authentication process, which can become prohibitive for certain users of the smart city (the elderly and the disabled). They also fail to provide continuous authentication. These limitations give rise to an emerging research field, which aims to provide non-invasive and user-friendly authentication based on information gathered by cameras, RF sensors, RFID, etc. (Kumar, Braeken, Liyanage, & Ylianttila, 2017).

The preceding paragraphs clearly show that the implementation of secure smart cities requires a holistic approach. In parallel to technological efforts to improve the security of all software and hardware components of the smart city, citizens, governments, and policymakers should join forces to address many unresolved and under-discussed challenges in the field. This paper aims to show that only the combined efforts of these various entities can provide adequate momentum to the realization of sustainable and secure smart city ecosystems. To this end, this manuscript presents a bifocal view of the field, starting with a thorough discussion on the potential security and safety implications for critical infrastructures as well as the resulting policy implications at the city, regional, national and global scales. The paper also provides a review of privacy and security vulnerabilities imparted by the generic architecture of the smart city, followed by a study of specificity of most common applications in the smart city.

Declarations of interest

None declared.

References

104th Congress Public Law 191 (1996). *Health insurance portability and accountability act of 1996.* Accessed 28.07.17 https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

Abdallah, A., & Shen, X. (2017). Lightweight security and privacy preserving scheme for smart grid customer-side networks. *IEEE Transactions on Smart Grid, 8*(3), 1064–1074. https://doi.org/10.1109/TSG.2015.2463742.

Abendroth, B., Kleiner, A., & Nicholas, P. (2017). *A scalable systems approach for critical infrastructure security.* Accessed 21.07.17 https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf.

Aloqaily, M., Otoum, S., Ridhawi, I. A., & Jararweh, Y. (2019). An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks, 90*, 101842. https://doi.org/10.1016/j.adhoc.2019.02.001 recent advances on security and privacy in Intelligent Transportation Systems, http://www.sciencedirect.com/science/article/pii/S1570870519301131.

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144–166.

Ammar, M., Daniels, W., Crispo, B., & Hughes, D. (2018). SPEED: Secure provable erasure for class-1 IoT devices. *Proceedings of the eighth ACM conference on data and application security and privacy* (pp. 111–118). . https://doi.org/10.1145/3176258.3176337.

An, J., Gui, X., Zhang, W., & Jiang, J. (2011). Nodes social relations cognition for mobility-aware in the internet of things. *International conference on internet of things (iThings/CPSCom), 4th international conference on cyber, physical and social computing* (pp. 687–691).

Angrishi, K. (2017). *Turning internet of things (IoT) into internet of vulnerabilities (IoV): IoT botnets.* arXiv preprint arXiv:1702.03681.

Anjomshoa, F., Aloqaily, M., Kantarci, B., Erol-Kantarci, M., & Schuckers, S. (2017). Social behaviometrics for personalized devices in the internet of things era. *IEEE Access, 5*, 12199–12213. https://doi.org/10.1109/ACCESS.2017.2719706.

Apple Inc (2017a]). *Apple watch.* Accessed 28.07.17 https://www.apple.com/watch/.

Apple Inc (2017b]). *IOS home.* Accessed 29.07.17 https://www.apple.com/ios/home/.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). *Closing the blinds: Four strategies for protecting smart home privacy from network observers.* arXiv preprint arXiv:1705.06809.

Ara, A., Al-Rodhaan, M., Tian, Y., & Al-Dhelaan, A. (2017). A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems. *IEEE Access, 5*, 12601–12617. https://doi.org/10.1109/ACCESS.2017.2716439.

Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99–109. https://doi.org/10.1109/TMSCS.2015.2498605.

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., et al. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation, 22*, 3–13. https://doi.org/10.1016/j.diin.2017.06.015http://www.sciencedirect.com/science/article/pii/S1742287617300579.

Baker, A. B., Eagan, R. J., Falcone, P. K., Harris, J. M., Herrera, G. V., Hines, W. C., et al. (2019). *A scalable systems approach for critical infrastructure security.* Sandia National Laboratories.

Balte, A., Kashid, A., & Patil, B. (2015). Security issues in internet of things (IoT): A survey. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(4).

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.

Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., et al. (2012). Smart cities of the future. *The European Physical Journal Special Topics, 214*(1), 481–518.

Bay Area Rapid Transit (2017). *About BART.* Accessed 08.10.17 https://www.bart.gov.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive computing, 2*(1), 46–55.

Blobel, B. (2018). Interoperable ehr systems-challenges, standards and solutions. *EJBI, 14*(2), 10–19.

Braun, T., Fung, B. C., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society, 39*, 499–507. https://doi.org/10.1016/j.scs.2018.02.039http://www.sciencedirect.com/science/article/pii/S2210670717310272.

Brisimi, T. S., Cassandras, C. G., Osgood, C., Paschalidis, I. C., & Zhang, Y. (2016). Sensing and classifying roadway obstacles in smart cities: The street bump system. *IEEE Access, 4*, 1301–1312.

Broström, T., Zhu, J., Robucci, R., & Younis, M. (2018). Iot boot integrity measuring and reporting. *SIGBED Review, 15*(5), 14–21. https://doi.org/10.1145/3292384.3292387.

Budurusubmi, A. B., & Yau, S. S. (2015). An effective approach to continuous user authentication for touch screen smart devices. *IEEE international conference on software quality, reliability and security (QRS),* 219–226.

Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Communications Magazine, 54*(4), 47–53. https://doi.org/10.1109/MCOM.2016.7452265.

Cabaj, K., & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: The case of cryptowall. *IEEE Network, 30*(6), 14–20. https://doi.org/10.1109/MNET.2016.1600110NM.

Calabrese, F., Colonna, M., Lovisolo, P., Parata, D., & Ratti, C. (2011). Real-time urban monitoring using cell phones: A case study in rome. *IEEE Transactions on Intelligent Transportation Systems, 12*(1), 141–151.

Cerrudo, C. (2015). An emerging us (and world) threat: Cities wide open to cyber attacks. *Securing Smart Cities*.

Chatzigiannakis, I., Vitaletti, A., & Pyrgelis, A. (2016). A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Computer Communications, 89*, 165–177.

Chu, C. C., & Iu, H. H. C. (2017). Complex networks theory for modern smart grid applications: A survey. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7*(2), 177–191. https://doi.org/10.1109/JETCAS.2017.2692243.

Conti, G., Cross, T., & Raymond, D. (2015). *Pen testing a city*. https://www.blackhat.com/docs/us-15/materials/us-15-Conti-Pen-Testing-A-City.pdf.

Covington, M. J., & Carskadden, R. (2013). Threat implications of the internet of things. *2013 5th international conference on cyber conflict (CyCon)* (pp. 1–12).

Crandall, A. S., & Cook, D. J. (2013). *Behaviometrics for identifying smart home residents. Human aspects in ambient intelligence*. Springer55–71.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access, 6*, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014http://www.sciencedirect.com/science/article/pii/S2210670717310685.

Daniello, G., Gaeta, M., & Orciuoli, F. (2018). An approach based on semantic stream reasoning to support decision processes in smart cities. *Telematics and Informatics, 35*(1), 68–81. https://doi.org/10.1016/j.tele.2017.09.019http://www.sciencedirect.com/science/article/pii/S0736585317304768.

Dantcheva, A., Elia, P., & Ross, A. (2016). What else does your biometric data reveal? A survey on soft biometrics. *IEEE Transactions on Information Forensics and Security, 11*(3), 441–467.

Das, A. K., Pathak, P. H., Chuah, C.-N., & Mohapatra, P. (2016). Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. *Proceedings of the 17th international workshop on mobile computing systems and applications* (pp. 99–104). . https://doi.org/10.1145/2873587.2873594.

Data Breach Investigations Report (2018). *Executive summary*. Accessed 16.02.19 https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

Datondji, S. R. E., Dupuis, Y., Subirats, P., & Vasseur, P. (2016). A survey of vision-based traffic monitoring of road intersections. *IEEE Transactions on Intelligent Transportation Systems, 17*(10), 2681–2698.

De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and I know it's you!: Implicit authentication based on touch screen patterns. *Proceedings of the SIGCHI conference on human factors in computing systems. ACM,* 987–996.

Ding, L., Shi, P., & Liu, B. (2010). The clustering of internet, internet of things and social network. *2010 3rd international symposium on knowledge acquisition and modeling (KAM)* (pp. 417–420).

Ding, H., Zhang, C., Cai, Y., & Fang, Y. (2018). Smart cities on wheels: A newly emerging vehicular cognitive capability harvesting network for data transportation. *IEEE Wireless Communications, 25*(2), 160–169. https://doi.org/10.1109/MWC.2017.1700151.

Diro, A., & Chilamkurti, N. (2018a]). Leveraging LSTM networks for attack detection in fog-to-things communications. *IEEE Communications Magazine, 56*(9), 124–130. https://doi.org/10.1109/MCOM.2018.1701270.

Diro, A. A., & Chilamkurti, N. (2018b]). Distributed attack detection scheme using deep learning approach for internet of things. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043http://www.sciencedirect.com/science/article/pii/S0167739X17308488.

Doan, T. T., Safavi-Naini, R., Li, S., Avizheh, S. M. V. K., & Fong, P. W. L. (2018). Towards a resilient smart home. *Proceedings of the 2018 workshop on IoT security and privacy* (pp. 15–21). . https://doi.org/10.1145/3229565.3229570.

Dwyer, A. (2018). The NHS cyber-attack: A look at the complex environmental conditions of WannaCry. *RAD Magazine, 44*.

Eckhoff, D., & Wagner, I. (2018). Privacy in the smart city applications, technologies, challenges, and solutions. *IEEE Communications Surveys Tutorials, 20*(1), 489–516. https://doi.org/10.1109/COMST.2017.2748998.

Eder-Neuhauser, P., Zseby, T., & Fabini, J. (2016). Resilience and security: A qualitative survey of urban smart grid architectures. *IEEE Access, 4*, 839–848. https://doi.org/10.1109/ACCESS.2016.2531279.

Ehrenfeld, J. M. (2017). Wannacry, cybersecurity and health information technology: A time to act. *Journal of Medical Systems, 41*(7), 104.

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.

Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., & Han, Z. (2017). Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal, 11*(3), 1644–1652. https://doi.org/10.1109/JSYST.2014.2341597.

FDA Safety Communication (2018). *Cybersecurity vulnerabilities identified in St. Jude medical's implantable cardiac devices and merlin@home transmitter: FDA safety communication.* Accessed 12.03.18 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.

Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y., et al. (2012). Continuous mobile authentication using touchscreen gestures. *2012 IEEE conference on technologies for Homeland security (HST)* (pp. 451–456).

Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017a]). Security implications of permission models in smart-home application frameworks. *IEEE Security Privacy, 15*(2), 24–30. https://doi.org/10.1109/MSP.2017.43.

Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017b]). Internet of things security research: A rehash of old ideas or new intellectual challenges? *IEEE Security Privacy, 15*(4), 79–84. https://doi.org/10.1109/MSP.2017.3151346.

FitBit Inc (2017). *Fitbit flex wireless activity & sleep wristband.* Accessed 28.07.17 https://www.fitbit.com/flex.

Francescani, C. (2016). *Ransomware hackers blackmail U.S. Police departments.* Accessed 16.02.19 https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746.

Gallagher, S. (2016). *Ransomware locks up San Francisco public transportation ticket machines: Some systems now restored; attacker demanded $73,000.* Accessed 21.07.17 https://arstechnica.com/security/2016/11/san-francisco-muni-hit-by-black-friday-ransomware-attack/.

Gascon, H., Uellenbeck, S., Wolf, C., & Rieck, K. (2014). *Continuous authentication on mobile devices by analysis of typing motion behavior. Sicherheit.* Citeseer1–12.

Ghinita, G. (2013). Privacy for location-based services. *Synthesis Lectures on Information Security, Privacy, & Trust, 4*(1), 1–85.

Goldfinch, S. (2007). Pessimism, computer failure, and information systems development in the public sector. *Public Administration Review, 67*(5), 917–929.

Google Inc (2017). *Weave, google developers.* Accessed 29.07.17 https://developers.google.com/weave/.

Gram-Hanssen, K., & Darby, S. J. (2018). Home is where the smart is? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science, 37*, 94–101. https://doi.org/10.1016/j.erss.2017.09.037http://www.sciencedirect.com/science/article/pii/S2214629617303213.

Guo, L., Dong, M., Ota, K., Li, Q., Ye, T., Wu, J., et al. (2017). A secure mechanism for big data collection in large scale internet of vehicle. *IEEE Internet of Things Journal, 4*(2), 601–610. https://doi.org/10.1109/JIOT.2017.2686451.

Gyrard, A., Zimmermann, A., & Sheth, A. (2018). Building IoT-based applications for smart cities: How can ontology catalogs help? *IEEE Internet of Things Journal, 5*(5), 3978–3990. https://doi.org/10.1109/JIOT.2018.2854278.

Habibzadeh, M., Qin, Z., Soyata, T., & Kantarci, B. (2017). Large scale distributed dedicated- and non-dedicated smart city sensing systems. *IEEE Sensors Journal (JSEN), 17*(23), 7649–7658. https://doi.org/10.1109/JSEN.2017.2725638.

Habibzadeh, M., Hassanalieragh, M., Ishikawa, A., Soyata, T., & Sharma, G. (2017a]). Hybrid solar-wind energy harvesting for embedded applications: Supercapacitor-based system architectures and design tradeoffs. *IEEE Circuits and Systems Magazine (MCAS), 17*(4), 29–63. https://doi.org/10.1109/MCAS.2017.2757081.

Habibzadeh, M., Xiong, W., Zheleva, M., Stern, E. K., Nussbaum, B. H., & Soyata, T. (2017b]). Smart city sensing and communication sub-infrastructure. *IEEE midwest symposium on circuits and systems (MWSCAS)* (pp. 1159–1162). . https://doi.org/10.1109/MWSCAS.2017.8053134.

Habibzadeh, M., Hassanalieragh, M., Soyata, T., & Sharma, G. (2017c]). Solar/wind hybrid energy harvesting for supercapacitor-based embedded systems. *IEEE midwest symposium on circuits and systems (MWSCAS)* (pp. 329–332). . https://doi.org/10.1109/MWSCAS.2017.8052927.

Habibzadeh, M., Hassanalieragh, M., Soyata, T., & Sharma, G. (2017d]). Supercapacitor-based embedded hybrid solar/wind harvesting system architectures. *Proceedings of the 30th IEEE international system-on-chip conference (SOCC)* (pp. 215–220). . https://doi.org/10.1109/SOCC.2017.8226043.

Habibzadeh, M., Soyata, T., Kantarci, B., Boukerche, A., & Kaptan, C. (2018). Sensing, communication and security planes: A new challenge for a smart city system design. *Computer Networks (COMNET)*. https://doi.org/10.1016/j.comnet.2018.08.001.

Hampton, N., & Baig, Z. A. (2015). *Ransomware: Emergence of the cyber-extortion menace*.

He, D., Chan, S., & Guizani, M. (2015). User privacy and data trustworthiness in mobile crowd sensing. *IEEE Wireless Communications, 22*(1), 28–34.

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., et al. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security, 78*, 398–428. https://doi.org/10.1016/j.cose.2018.07.011http://www.sciencedirect.com/science/article/pii/S0167404818304875.

Heeks, R., & Bhatnagar, S. (1999). *Understanding success and failure in information age reform. Reinventing government in the information age: International practice in IT-enabled public sector reform, vol. 1*, 49–74.

Hennebert, C., & Santos, J. D. (2014). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet of Things Journal, 1*(5), 384–398. https://doi.org/10.1109/JIOT.2014.2359538.

Holmquist, L. E., Mattern, F., Schiele, B., Alahuhta, P., Beigl, M., & Gellersen, H.-W. (2001). Smart-its friends: A technique for users to easily establish connections between smart artefacts. *International conference on ubiquitous computing. Springer,* 116–122.

Honan, G., Page, A., Kocabas, O., Soyata, T., & Kantarci, B. (2016). Internet-of-everything oriented implementation of secure Digital Health (D-Health) systems. *Proceedings of the 2016 IEEE symposium on computers and communications (ISCC)* (pp. 718–725). . https://doi.org/10.1109/ISCC.2016.7543821.

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,* 612–625.

Internet of things privacy and security in a connected world. Accessed 21.07.17 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Jokar, P., Arianpoo, N., & Leung, V. C. M. (2016). Electricity theft detection in AMI using customers consumption patterns. *IEEE Transactions on Smart Grid, 7*(1), 216–226. https://doi.org/10.1109/TSG.2015.2425222.

Jose, A. C., & Malekian, R. (2017). Improving smart home security: Integrating logical sensing into smart home. *IEEE Sensors Journal, 17*(13), 4269–4286. https://doi.org/10.1109/JSEN.2017.2705045.

Kabalci, Y. (2016). A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews, 57*, 302–318. https://doi.org/10.1016/j.rser.2015.12.114http://www.sciencedirect.com/science/article/pii/S1364032115014975.

Kachuee, M., Kiani, M. M., Mohammadzade, H., & Shabany, M. (2017). Cuffless blood pressure estimation algorithms for continuous health-care monitoring. *IEEE Transactions on Biomedical Engineering, 64*(4), 859–869. https://doi.org/10.1109/TBME.2016.2580904.

Kalalas, C., Thrybom, L., & Alonso-Zarate, J. (2016). Cellular communications for smart grid neighborhood area networks: A survey. *IEEE Access, 4*, 1469–1493. https://doi.org/10.1109/ACCESS.2016.2551978.

Kang, J., Yu, R., Huang, X., & Zhang, Y. (2018). Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems, 19*(8), 2627–2637. https://doi.org/10.1109/TITS.2017.2764095.

Kantarci, B., & Mouftah, H. T. (2014). Trustworthy sensing for public safety in cloud-centric internet of things. *IEEE Internet of Things Journal, 1*(4), 360–368.

Kantarci, B., Carr, K. G., & Pearsall, C. D. (2016). SONATA: Social network assisted trustworthiness assurance in smart city crowdsensing. *International Journal of Distributed Systems and Technologies (IJDST), 7*(1), 59–78.

Khan, H., & Hengartner, U. (2014). Towards application-centric implicit authentication on smartphones. *Proceedings of the 15th workshop on mobile computing systems and applications. ACM,* 10.

Khan, H., Atwater, A., & Hengartner, U. (2014). Itus: An implicit authentication framework for android. *Proceedings of the 20th annual international conference on mobile computing and networking. ACM,* 507–518.

Khatoun, R., & Zeadally, S. (2016). Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM, 59*(8), 46–57.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine, 55*(3), 51–59. https://doi.org/10.1109/MCOM.2017.1600297CM.

Kim, Y., Soyata, T., & Behnagh, R. F. (2018). Towards emotionally-aware AI smart classroom: Current issues and directions for engineering and education. *IEEE Access, 6*, 5308–5331. https://doi.org/10.1109/ACCESS.2018.2791861.

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security.* Data Protection Unit, Department of the Taoiseach.

Kitchin, R., & Dodge, M. (2017). The (in)security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology,* 1–19. https://doi.org/10.1080/10630732.2017.1408002.

Knopf, A. (2019). As hipaa changes loom, patients demand continued confidentiality for sud records. *Alcoholism & Drug Abuse Weekly, 31*(4), 1–3. https://doi.org/10.1002/adaw.32236.

Koc, C. K., Acar, T., & Kaliski, B. S. (1996). Analyzing and comparing montgomery multiplication algorithms. *IEEE Micro, 16*(3), 26–33.

Kocabas, O., Soyata, T., Couderc, J., Aktas, M. K., Xia, J., & Huang, M. (2013). Assessment of cloud-based health monitoring using homomorphic encryption. *Proceedings of the 31st IEEE international conference on computer design (ICCD)* (pp. 443–446). . https://doi.org/10.1109/ICCD.2013.6657078.

Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging security mechanisms for medical cyber physical systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB), 13*(3), 401–416. https://doi.org/10.1109/TCBB.2016.2520933.

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., & Kuhn, R. (2016). Learning internet-of-things security “hands-on”. *IEEE Security Privacy, 14*(1), 37–46. https://doi.org/10.1109/MSP.2016.4.

Krimmling, J., & Peter, S. (2014). Integration and evaluation of intrusion detection for CoAP in smart city applications. *2014 IEEE conference on communications and network security (CNS)* (pp. 73–78).

Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., & Ha, P. H. (2017a]). Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security, 12*(4), 968–979. https://doi.org/10.1109/TIFS.2016.2647225.

Kumar, T., Braeken, A., Liyanage, M., & Ylianttila, M. (2017b]). Identity privacy preserving biometric based authentication scheme for naked healthcare environment. *2017 IEEE international conference on communications (ICC),* 1–7. https://doi.org/10.1109/ICC.2017.7996966.

Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). *IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals, Tech. Rep.* IETF.

Lévy-Bencheton, C., & Darra, E. (2015). *Cyber security for smart cities – An architecture model for public transport.* https://doi.org/10.2824/846575.

Labrado, C., & Thapliyal, H. (2019). Design of a piezoelectric-based physically unclonable function for IoT security. *IEEE Internet of Things Journal, 6*(2), 2770–2777. https://doi.org/10.1109/JIOT.2018.2874626.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly, 35*(1), 151–160. https://doi.org/10.1016/j.giq.2017.10.006 internet Plus Government: Advancement of Networking Technology and Evolution of the Public Sector. http://www.sciencedirect.com/science/article/pii/S0740624X16302155.

Li, Y., Jeong, Y., Shin, B., & Park, J. H. (2017). Crowdsensing multimedia data: Security and privacy issues. *IEEE MultiMedia, 24*(4), 58–66. https://doi.org/10.1109/MMUL.2017.4031306.

Li, F., Han, Y., & Jin, C. (2018a]). Cost-effective and anonymous access control for wireless body area networks. *IEEE Systems Journal, 12*(1), 747–758. https://doi.org/10.1109/JSYST.2016.2557850.

Li, T., Jung, T., Qiu, Z., Li, H., Cao, L., & Wang, Y. (2018b]). Scalable privacy-preserving participant selection for mobile crowdsensing systems: Participant grouping and secure group bidding. *IEEE Transactions on Network Science and Engineering,* 1. https://doi.org/10.1109/TNSE.2018.2791948.

Liao, K., Zhao, Z., Doupe, A., & Ahn, G. J. (2016). Behind closed doors: Measurement and analysis of cryptolocker ransoms in bitcoin. *2016 APWG symposium on electronic crime research (eCrime),* 1–13. https://doi.org/10.1109/ECRIME.2016.7487938.

Lin, H., & Bergmann, N. W. (2016). Iot privacy and security challenges for smart home environments. *Information, 7*(3), https://doi.org/10.3390/info7030044https://www.mdpi.com/2078-2489/7/3/44.

Lin, J., Niu, J., Li, H., & Atiquzzaman, M. (2019). A secure and efficient location-based service scheme for smart transportation. *Future Generation Computer Systems, 92*, 694–704. https://doi.org/10.1016/j.future.2017.11.030http://www.sciencedirect.com/science/article/pii/S0167739X17317235.

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security vulnerabilities of internet of things: A case study of the smart plug system. *IEEE Internet of Things Journal, 4*(6), 1899–1909. https://doi.org/10.1109/JIOT.2017.2707465.

Liu, C., Yang, J., Zhang, Y., Chen, R., & Zeng, J. (2011). Research on immunity-based intrusion detection technology for the internet of things. *2011 seventh international conference on natural computation (ICNC), Vol. 1* (pp. 212–216).

Liu, X., Cao, J., Tang, S., Wen, J., & Guo, P. (2016). Contactless respiration monitoring via off-the-shelf WiFi devices. *IEEE Transactions on Mobile Computing, 15*(10), 2466–2479. https://doi.org/10.1109/TMC.2015.2504935.

Liu, B., Zhou, W., Zhu, T., Zhou, H., & Lin, X. (2017). Invisible hand: A privacy preserving mobile crowd sensing framework based on economic models. *IEEE Transactions on Vehicular Technology, 66*(5), 4410–4423. https://doi.org/10.1109/TVT.2016.2611761.

Liu, W., Gu, C., Qu, G., & ONeill, M. (2018). Approximate computing and its application to hardware security. *Cyber-physical systems security. Springer,* 43–67.

Liu-Jimenez, J., Sanchez-Reillo, R., & Fernandez-Saavedra, B. (2011). Iris biometrics for embedded systems. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 19*(2), 274–282.

Logota, E., Mantas, G., Rodriguez, J., & Marques, H. (2014). Analysis of the impact of denial of service attacks on centralized control in smart cities. *International wireless internet conference. Springer,* 91–96.

Maciag, M., & Wogan, J. (2017). With less state aid, localities look for ways to cope. *Governing, 30*, 32–37.

Mahbub, I., Pullano, S. A., Wang, H., Islam, S. K., Fiorillo, A. S., To, G., et al. (2017). A low-power wireless piezoelectric sensor-based respiration monitoring system realized in cmos process. *IEEE Sensors Journal, 17*(6), 1858–1864. https://doi.org/10.1109/JSEN.2017.2651073.

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). Wannacry-a year on. *BMJ: British Medical Journal (Online), 361*.

Mathews, L. (2018). *Ransomware that hit Atlanta's computers destroyed police evidence.* Accessed 16.02.19 https://www.forbes.com/sites/leemathews/2018/06/08/ransomware-that-hit-atlantas-computers-destroyed-police-evidence/#2143b552112d.

MC10 Inc (2017). *Wearable healthcare technology & devices watch.* Accessed 28.07.17 https://www.mc10inc.com.

McLaughlin, S., Holbert, B., Fawaz, A., Berthier, R., & Zonouz, S. (2013). A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE Journal on Selected Areas in Communications, 31*(7), 1319–1330.

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268–1293.

Mishra, D., Chaturvedi, A., & Mukhopadhyay, S. (2015). Design of a lightweight two-factor authentication scheme with smart card revocation. *Journal of Information Security and Applications, 23*, 44–53. https://doi.org/10.1016/j.jisa.2015.06.001http://www.sciencedirect.com/science/article/pii/S221421261500023X.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack. *International Journal, 8*(5).

Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586–602.

Nam, T., & Pardo, T. A. (2011). Smart city as urban innovation: Focusing on management, policy, and context. *Proceedings of the 5th international conference on theory and practice of electronic governance. ACM,* 185–194.

National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis (2015). *The future of smart cities: Cyber-physical infrastructure risk.* Accessed 21.07.17 https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf.

Nguyen, V., Lin, P., & Hwang, R. (2019). Energy depletion attacks in low power wireless networks. *IEEE Access, 7*, 51915–51932. https://doi.org/10.1109/ACCESS.2019.2911424.

Ni, J., Zhang, K., Yu, Y., Lin, X., & Shen, X. S. (2018). Providing task allocation and secure deduplication for mobile crowdsensing via fog computing. *IEEE Transactions on Dependable and Secure Computing,* 1. https://doi.org/10.1109/TDSC.2018.2791432.

Nunes, D. F., Moreira, E. S., Kimura, B. Y., Sastry, N., & Mahmoodi, T. (2017). Attraction-area based geo-clustering for LTE vehicular CrowdSensing data offloading. *Proceedings of the 20th ACM international conference on modelling, analysis and simulation of wireless and mobile systems* (pp. 323–327). . https://doi.org/10.1145/3127540.3127576.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace.* Symantec Corporation.

Okeya, K., & Sakurai, K. (2002). *On insecurity of the side channel attack countermeasure using addition-subtraction chains under distinguishability between addition and doubling.*

Information security and privacy. Springer63–70.

Oueis, J., Conan, V., Lavaux, D., Stanica, R., & Valois, F. (2017). Overview of LTE isolated E-UTRAN operation for public safety. *IEEE Communications Standards Magazine, 1*(2), 98–105. https://doi.org/10.1109/MCOMSTD.2017.1600875.

Pagano, M. A., & Hoene, C. W. (2018). *City budgets in an era of increased uncertainty: Understanding the fiscal policy space of cities.* Washington, DC: Brookings Institution. https://www.brookings.edu/wp-content/uploads/2018/07/20180718_Brookings-Metro_City-fiscal-policy-Pagano-Hoene-final.pdf.

Page, A., Kocabas, O., Soyata, T., Aktas, M. K., & Couderc, J. (2014). Cloud-based privacy-preserving remote ECG monitoring and surveillance. *Annals of Noninvasive Electrocardiology (ANEC), 20*(4), 328–337. https://doi.org/10.1111/anec.12204.

Page, A., Hassanalieragh, M., Soyata, T., Aktas, M. K., Kantarci, B., & Andreescu, S. (2015). Conceptualizing a real-time remote cardiac health monitoring system. In T. Soyata (Ed.). *Enabling real-time mobile cloud computing through emerging technologies* (pp. 1–34). IGI Global. https://doi.org/10.4018/978-1-4666-8662-5.ch001 Ch. 1.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. *PLOS Medicine, 13*(2), 1–9. https://doi.org/10.1371/journal.pmed.1001953.

Poh, G. S., Gope, P., & Ning, J. (2019). Privhome: Privacy-preserving authenticated communication in smart home environment. *IEEE Transactions on Dependable and Secure Computing,* 1. https://doi.org/10.1109/TDSC.2019.2914911.

Poursaberi, A., Vana, J., Mracek, S., Dvora, R., Yanushkevich, S. N., Drahansky, M., et al. (2013). Facial biometrics for situational awareness systems. *IET Biometrics, 2*(2), 35–47.

Pouryazdan, M., & Kantarci, B. (2016). The smart citizen factor in trustworthy smart city crowdsensing. *IT Professional, 18*(4), 26–33.

Pouryazdan, M., Fiandrino, C., Kantarci, B., Kliazovich, D., Soyata, T., & Bouvry, P. (2016). Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric internet-of-things (IoT) applications. *IEEE GLOBECOM workshops,* 1–6. https://doi.org/10.1109/GLOCOMW.2016.7848915.

Pouryazdan, M., Kantarci, B., Soyata, T., Foschini, L., & Song, H. (2017a]). Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing. *IEEE Access, 5*, 1382–1397. https://doi.org/10.1109/ACCESS.2017.2660461.

Pouryazdan, M., Fiandrino, C., Kantarci, B., Soyata, T., Kliazovich, D., & Bouvry, P. (2017b]). Intelligent gaming for mobile crowd-sensing participants to acquire trust-worthy big data in the internet of things. *IEEE Access, 5*(1), 22209–22223. https://doi.org/10.1109/ACCESS.2017.2762238.

Powers, N., Alling, A., Osolinsky, K., Soyata, T., Zhu, M., Wang, H., et al. (2015). The cloudlet accelerator: Bringing mobile-cloud face recognition into real-time. *Globecom workshops (GC Wkshps)* (pp. 1–7). . https://doi.org/10.1109/GLOCOMW.2015.7414055.

Pump, R., Ahlers, V., & Koschel, A. (2018). State of the art in artificial immune-based intrusion detection systems for smart grids. *2018 second world conference on smart trends in systems, security and sustainability (WorldS4),* 119–126. https://doi.org/10.1109/WorldS4.2018.8611584.

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to networking cloud and edge datacenters in the internet of things. *IEEE Cloud Computing, 3*(3), 64–71.

Rachim, V. P., & Chung, W. Y. (2016). Wearable noncontact armband for mobile ECG monitoring system. *IEEE Transactions on Biomedical Circuits and Systems, 10*(6), 1112–1118. https://doi.org/10.1109/TBCAS.2016.2519523.

Rajput, U., Abbas, F., Eun, H., & Oh, H. (2017). A hybrid approach for efficient privacy-preserving authentication in VANET. *IEEE Access, 5*, 12014–12030. https://doi.org/10.1109/ACCESS.2017.2717999.

Ramaprasad, A., Sánchez-Ortiz, A., & Syn, T. (2017). A unified definition of a smart city. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, P. Parycek, H. J. Scholl, & D. Trutnev (Eds.). *Electronic government* (pp. 13–24). Cham: Springer International Publishing.

Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad Hoc Networks, 11*(8), 2661–2674.

Reuben, K. (2011). *Municipal budget shortfalls.* Accessed 16.02.19 https://www.taxpolicycenter.org/taxvox/municipal-budget-shortfalls.

Reyes, B. A., Reljin, N., Kong, Y., Nam, Y., & Chon, K. H. (2017). Tidal volume and instantaneous respiration rate estimation using a volumetric surrogate signal acquired via a smartphone camera. *IEEE Journal of Biomedical and Health Informatics, 21*(3), 764–777. https://doi.org/10.1109/JBHI.2016.2532876.

Rogers, J. (2018). *Fitness tracking data on strava app reveal US military bases details, sparking security concerns.* Accessed 19.03.18 http://www.foxnews.com/tech/2018/01/29/fitness-tracking-data-on-strava-app-reveal-us-military-bases-details-sparking-security-concerns.html.

Salinas, S. A., & Li, P. (2016). Privacy-preserving energy theft detection in microgrids: A state estimation approach. *IEEE Transactions on Power Systems, 31*(2), 883–894. https://doi.org/10.1109/TPWRS.2015.2406311.

Samsung Electronics Co (2017). *SmartThings, Add a little smartness to your things.* Accessed 29.07.17 https://www.smartthings.com.

Sedjelmaci, H., Hadji, M., & Ansari, N. (2019). Cyber security game for intelligent transportation systems. *IEEE Network,* 1–7. https://doi.org/10.1109/MNET.2018.1800279.

Shakhov, V., & Koo, I. (2018). Depletion-of-battery attack: Specificity, modelling and analysis. *Sensors, 18*(6), https://doi.org/10.3390/s18061849http://www.mdpi.com/1424-8220/18/6/1849.

Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems, 86*, 650–655. https://doi.org/10.1016/j.future.2018.04.060http://www.sciencedirect.com/science/article/pii/S0167739X1830431X.

Shishvan, O. R., Zois, D., & Soyata, T. (2018). Machine intelligence in healthcare and medical cyber physical systems: A survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2018.2866049.

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported internet of things. *IEEE Internet of Things Journal, 3*(3), 269–284. https://doi.org/10.1109/JIOT.2015.2460333.

Singh, A., Chawla, N., Ko, J. H., Kar, M., & Mukhopadhyay, S. (2019). Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes. *IEEE Internet of Things Journal, 6*(1), 421–434. https://doi.org/10.1109/JIOT.2018.2861324.

Smith, K. L. (2017). *The inconvenient truth about smart cities.* Accessed 16.02.19 https://blogs.scientificamerican.com/observations/the-inconvenient-truth-about-smart-cities/.

Soyata, T., Muraleedharan, R., Funai, C., Kwon, M., & Heinzelman, W. (2012). Cloud-vision: Real-time face recognition using a mobile-cloudlet-cloud acceleration architecture. *Proceedings of the 17th IEEE symposium on computers and communications (ISCC)* (pp. 59–66). . https://doi.org/10.1109/ISCC.2012.6249269.

Soyata, T., Copeland, L., & Heinzelman, W. (2016). RF energy harvesting for embedded systems: A survey of tradeoffs and methodology. *IEEE Circuits and Systems Magazine (MCAS), 16*(1), 22–57. https://doi.org/10.1109/MCAS.2015.2510198.

Soyata, T. (2018). *GPU parallel program development using CUDA.* Taylor and Francis.

Srikantha, P., & Kundur, D. (2016). A der attack-mitigation differential game for smart grid security analysis. *IEEE Transactions on Smart Grid, 7*(3), 1476–1485. https://doi.org/10.1109/TSG.2015.2466611.

Stewart, J. (2016). *San Franciscos transit hack couldve been way worse – And cities must prepare.* Accessed 21.07.17 https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare/.

Stone, E. E., & Skubic, M. (2015). Fall detection in homes of older adults using the microsoft kinect. *IEEE Journal of Biomedical and Health Informatics, 19*(1), 290–301. https://doi.org/10.1109/JBHI.2014.2312180.

Sultana, M., Paul, P. P., & Gavrilova, M. (2014). A concept of social behavioral biometrics: Motivation, current developments, and future trends. *International conf. on cyberworlds* (pp. 271–278).

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. *2012 international conference on computer science and electronics engineering (ICCSEE), Vol. 3* (pp. 648–651).

Suzuki, M., Ueno, R., Homma, N., & Aoki, T. (2019). Efficient fuzzy extractors based on ternary debiasing method for biased physically unclonable functions. *IEEE Transactions on Circuits and Systems I: Regular Papers, 66*(2), 616–629. https://doi.org/10.1109/TCSI.2018.2869086.

Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K. (2017). Survey of security advances in smart grid: A data driven approach. *IEEE Communications Surveys Tutorials, 19*(1), 397–422. https://doi.org/10.1109/COMST.2016.2616442.

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems, 78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011http://www.sciencedirect.com/science/article/pii/S0167739X16305775.

Tedeschi, S., Mehnen, J., Tapoglou, N., & Roy, R. (2017). Secure IoT Devices for the Maintenance of Machine Tools. *Procedia CIRP, 59*, 150–155. https://doi.org/10.1016/j.procir.2016.10.002 proceedings of the 5th International Conference in Through-life Engineering Services Cranfield University, 1st and 2nd November 2016. http://www.sciencedirect.com/science/article/pii/S2212827116309878.

Teichmann, M., Weber, M., Zoellner, M., Cipolla, R., & Urtasun, R. (2016). *Multinet: Real-time joint semantic reasoning for autonomous driving.* arXiv preprint arXiv:1612.07695.

van der Heijden, R. W., Dietzel, S., Leinmller, T., & Kargl, F. (2019). Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys Tutorials, 21*(1), 779–811. https://doi.org/10.1109/COMST.2018.2873088.

Vasselle, A., Thiebeauld, H., Maouhoub, Q., Morisset, A., & Ermeneux, S. (2018). Laser-induced fault injection on smartphone bypassing the secure boot. *IEEE Transactions on Computers,* 1. https://doi.org/10.1109/TC.2018.2860010.

Wagstaff, K. (2013). *Big paydays force hospitals to prepare for ransomware attacks.* Accessed 16.02.19 https://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176.

Wang, J., Li, M., He, Y., Li, H., Xiao, K., & Wang, C. (2018). A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access, 6*, 17545–17556. https://doi.org/10.1109/ACCESS.2018.2805837.

Wessel, S., Huber, M., Stumpf, F., & Eckert, C. (2015). Improving mobile device security with operating system-level virtualization. *Computers & Security, 52*, 207–220. https://doi.org/10.1016/j.cose.2015.02.005http://www.sciencedirect.com/science/article/pii/S0167404815000206.

Whittaker, B. (1999). What went wrong? Unsuccessful information technology projects. *Information Management & Computer Security, 7*(1), 23–30.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy, 103*, 72–83. https://doi.org/10.1016/j.enpol.2016.12.047http://www.sciencedirect.com/science/article/pii/S030142151630711X.

Wu, H., & Horng, G. (2017). Establishing an intelligent transportation system with a network security mechanism in an internet of vehicle environment. *IEEE Access, 5*, 19239–19247. https://doi.org/10.1109/ACCESS.2017.2752420.

Xu, G., Li, H., Tan, C., Liu, D., Dai, Y., & Yang, K. (2017). Achieving efficient and privacy-preserving truth discovery in crowd sensing systems. *Computers & Security, 69*, 114–126. https://doi.org/10.1016/j.cose.2016.11.014 security Data Science and Cyber Threat Management, http://www.sciencedirect.com/science/article/pii/S0167404816301675.

Yamaguchi, M., & Sakakima, J. (2007). Evaluation of driver stress in a motor-vehicle driving simulator using a biochemical marker. *Journal of International Medical Research, 35*(1), 91–100.

Yan, J., Zeng, Q., Liang, Y., He, L., & Li, Z. (2017). Modeling and implementation of electroactive smart air-conditioning vent register for personalized HVAC systems. *IEEE Access, 5*, 1649–1657. https://doi.org/10.1109/ACCESS.2017.2664580.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Information Sciences, 479*, 567–592. https://doi.org/10.1016/j.ins.2018.02.005http://www.sciencedirect.com/science/article/pii/S0020025518300860.

Yao, D., Wen, M., Liang, X., Fu, Z., Zhang, K., & Yang, B. (2019). Energy theft detection with energy privacy preservation in the smart grid. *IEEE Internet of Things Journal,* 1. https://doi.org/10.1109/JIOT.2019.2903312.

Ye, N., Zhu, Y., Wang, R.-c., Malekian, R., & Qiao-min, L. (2014). An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics & Information Sciences, 8*(4), 1617.

Yip, S.-C., Wong, K., Hew, W.-P., Gan, M.-T., Phan, R. C.-W., & Tan, S.-W. (2017). Detection of energy theft and defective smart meters in smart grids using linear regression. *International Journal of Electrical Power & Energy Systems, 91*, 230–240. https://doi.org/10.1016/j.ijepes.2017.04.005http://www.sciencedirect.com/science/article/pii/S0142061516316386.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328.

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. *Thirteenth symposium on usable privacy and security ({SOUPS} 2017),* 65–80.

Zhang, H., & Li, M. (2011). Security vulnerabilities of an remote password authentication scheme with smart card. *2011 international conference on consumer electronics, communications and networks (CECNet)* (pp. 698–701).

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT security: Ongoing challenges and research opportunities. *2014 IEEE 7th international conference on service-oriented computing and applications*. https://doi.org/10.1109/SOCA.2014.58.

Zhang, X., Yang, Z., Sun, W., Liu, Y., Tang, S., Xing, K., et al. (2016). Incentives for mobile crowd sensing: A survey. *IEEE Communications Surveys Tutorials, 18*(1), 54–67. https://doi.org/10.1109/COMST.2015.2415528.

Zhang, L., Zhu, S., & Tang, S. (2017a]). Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. *IEEE Journal of Biomedical and Health Informatics, 21*(2), 465–475. https://doi.org/10.1109/JBHI.2016.2517146.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017b]). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine, 55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM.

Zhao, Y. L. (2013). *Research on data security technology in internet of things. Applied mechanics and materials, Vol. 433*, Trans Tech Publ1752–1755.

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine, 55*(1), 26–33. https://doi.org/10.1109/MCOM.2017.1600363CM.