IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON CHALLENGES AND OPPORTUNITIES OF BIG DATA AGAINST CYBER CRIME

Received June 14, 2018, accepted June 23, 2018, date of publication July 11, 2018, date of current version September 7, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2853985

Security and Privacy in Smart Cities: Challenges and Opportunities

LEI CUI[1,2], (Student Member, IEEE), GANG XIE[1,3], YOUYANG QU[2], (Student Member, IEEE), LONGXIANG GAO[2], (Senior Member, IEEE), AND YUNYUN YANG[1]

[1]College of Electrical and Power Engineering, Taiyuan University of Technology, Taiyuan 030024, China
[2]School of Information Technology, Deakin University, Burwood, VIC 3125, Australia
[3]School of Electronic Information Engineering, Taiyuan University of Science and Technology, Taiyuan 030024, China

Corresponding author: Gang Xie (xiegang@tyut.edu.cn)

This work was supported by the Shanxi Scholarship Council of China funded by Research Project under Grant 2016-044.

ABSTRACT Smart cities are expected to improve the quality of daily life, promote sustainable development, and improve the functionality of urban systems. Now that many smart systems have been implemented, security and privacy issues have become a major challenge that requires effective countermeasures. However, traditional cybersecurity protection strategies cannot be applied directly to these intelligent applications because of the heterogeneity, scalability, and dynamic characteristics of smart cities. Furthermore, it is necessary to be aware of security and privacy threats when designing and implementing new mechanisms or systems. Motivated by these factors, we survey the current situations of smart cities with respect to security and privacy to provide an overview of both the academic and industrial fields and to pave the way for further exploration. Specifically, this survey begins with an overview of smart cities to provide an integrated context for readers. Then, we discuss the privacy and security issues in current smart applications along with the corresponding requirements for building a stable and secure smart city. In the next step, we summarize the existing protection technologies. Finally, we present open research challenges and identify some future research directions.

INDEX TERMS Smart city, Internet of Things, security, privacy.

I. INTRODUCTION

In the past two decades, the concept of ''smart city'' has attracted increasing attention in both academic and industrial fields because of its strong realistic requirement and practical background in an increasingly urbanized world. According to the latest United Nations Population Fund, more than half of the world's population now lives in urban areas, and it is predicted that approximately 66 percent of the world's population will live in an urban environment by 2050 [1], resulting in excessive burdens to the climate, energy, environment, and living conditions.

Aiming to mitigate these challenges and improve the well-being of citizens, create economic development and manage modern cities in a sustainable and intelligent way, a growing number of cities worldwide have started to develop their own smart strategies. In 2017, Cisco announced a one billion dollar investment in smart cities. As the world's most populous nation, China alone has more than 200 smart city projects in progress [2]. Predictably, the infrastructure of a city is embedded with billions of devices that can be mutually beneficial for the citizens by means of various applications, such as smart transportation, smart government, smart healthcare, smart environments, and smart homes.

However, the creation of these smart applications may also pose numerous security and privacy problems due to the vulnerabilities commonly existing in each layer of a smart system. Attacks, such as the unauthorized access, Sybil, and denial of service (DoS), can degrade the quality of intelligent services [3]. For example, in 2015, nearly 230 thousand citizens living in Ukraine suffered a long period of electricity disconnection because the power grid system was attacked by hackers [4]. In addition, data over-collection by service providers and some third parties subjects residents to privacy threats [5].

Many protection methods (e.g., encryption, biometrics, anonymity) are widely applied in different application fields. Unfortunately, these methods are not sufficient for the smart city environment. The main reason is that most of the sensors and devices have limited computational power, so only simple cryptography algorithms can be used directly [6].

TABLE 1. Comparison of related surveys from the perspective of enabling technologies.

Reference	Cryptography	Blockchain	Biometrics	Machine Learning	Data Miniing	Game Theory	Ontology	Non-Technical
Gharaibeh et al. [9]	✓	✓	0	✓	0	0	0	0
Eckhoff et al. [10]	✓	0	✓	0	✓	0	0	0
Zhang et al. [3]	✓	0	✓	0	0	0	0	0
Kitchin et al. [81]	✓	0	0	0	✓	0	0	✓
Sicari et al. [7]	✓	0	✓	0	✓	0	0	0
This work	✓	✓	✓	✓	✓	✓	✓	✓

These ineffective measures indirectly pose serious threats to the whole system. In addition, compared with conventional computing systems, the heterogeneity, scalability and dynamic characteristics of IoT systems subject smart applications to high security and privacy risks. Furthermore, with the rapid development of information technologies such as machine learning and data mining, attackers have become ''smarter'' and have developed the ability to bypass the current attack detection mechanisms. These challenges motivate us to review the already applied and developed technologies in terms of protecting smart cities and to attempt to provide potential research opportunities for the readers to further study this promising and practical field.

During the past few years, several surveys have been conducted in this field, most of which are focused on the overall IoT ecosystem. For example, Sicari *et al.* [7] presented an overview of the current issues and solutions in IoT systems, including security, privacy and trust. Nia and Jha [8] recently discussed security issues on the edge-side layer of IoT. By contrast, the quantity of survey papers on smart city security and privacy is still limited. In 2017, a comprehensive survey conducted by Gharaibeh *et al.* [9] highlighted the achievements of smart cities and then discussed existing security issues from a data-centric perspective. Focusing on the security and privacy problems, Zhang *et al.* [3] provided a taxonomy of different security solutions with respect to different smart applications. Eckhoff and Wagner [10] conducted a survey of nine specific technologies for protecting privacy in a smart city contest.

Our survey is different from the existing ones because it is a survey conducted from the viewpoint of related disciplines. To reflect the novelty of this survey, we present a comparison in Table 1. The contributions of this work are listed as follows.

- We provide an extensive overview of protection methods for securing smart cities from the perspectives of different disciplines, including the latest developed or applied mechanisms and theories.
- We evaluate the availability of state-of-the-art protection technologies for smart cities and present some open issues that have limited effective countermeasures.
- We identify future research opportunities corresponding to the current challenges and the up-to-date security requirements, which can contribute to the construction of more secure, privacy protected and stable smart cities.

The rest of this paper is structured as follows. Section II provides an overview of the architecture, applications and characteristics of smart cities. In Section III, we identify security and privacy issues as well as some updated threats generated by emerging smart applications. The corresponding requirements for smart cities are provided in Section IV. The security and privacy technologies employed for smart cities are investigated with respect to different disciplines in Section V. Challenges and potential opportunities based on our understanding are provided in Section VI. Finally, we summarize and conclude the study in Section VII.

II. SMART CITY OVERVIEW

As the features of smart cities are closely related to the security requirements and challenges presented in the following sections and because most of the protection methods introduced in Section IV were developed based on the specific scenarios of different smart applications, it is necessary to introduce the characteristics, architecture, and common applications of smart cities to provide an integrated context and enable readers to easily understand the main contents of this survey.

A. IOT ARCHITECTURE FOR SMART CITIES

To keep up with the development of smart cities, multiple architectures have been designed [11]. However, to the best of our knowledge, there is no uniform IoT architecture. As the emphasis of this work is to summarize security and privacy issues in smart cities, the architecture described here is based on the well-known three-layer architecture and the generally accepted architecture proposed in [105]. As shown in Fig. 1, the architecture can be divided into four layers; a brief introduction is provided in the following.

Perception layer, also called the sensing layer, recognition layer or the edge layer, is the lowest layer of the architecture. The perception layer is mainly used for data collection from things (e.g., heterogeneous devices, WSNs and sensors) in the real world and transmitting the acquired information to the network layer for further processing.

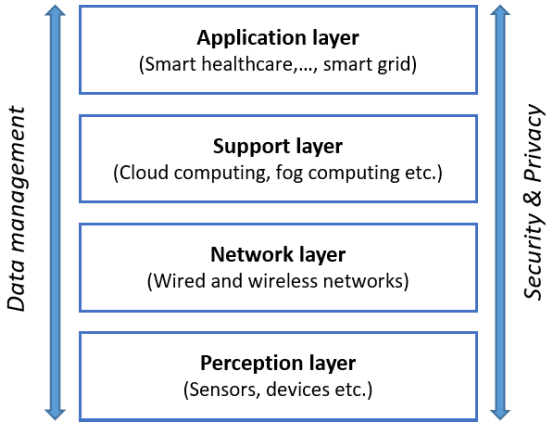


FIGURE 1. IoT-based architecture for a smart city.

Network layer is the core layer in the IoT architecture that depends on basic networks, such as the Internet, WSNs, and communications networks. The responsibility of this layer is to transmit the data collected by the perception layer and to connect smart things, network devices, and servers.

Support layer, which works very closely with the application layer, provides support for the requirements of diversified applications via intelligent computing techniques (e.g., cloud computing, edge computing, fog computing).

Application layer, as the top layer, is responsible for providing intelligent and practical services or applications to users based on their personalized requirements. We provide a detailed description in the following subsection.

B. APPLICATIONS

One objective of building smart cities is to benefit residents with respect to different aspects that are closely related to the living standards of residents, such as energy, environment, industry, living, and services. We illustrate the emerging intelligent applications of smart cities in Fig. 2 and describe them in detail as follows.

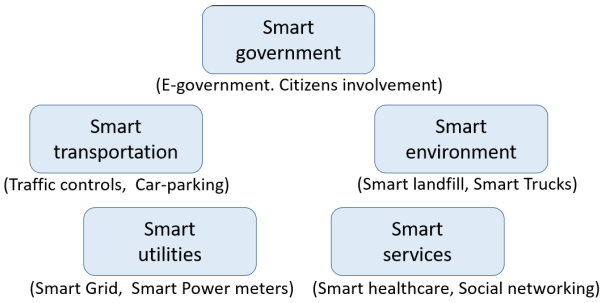


FIGURE 2. Applications in smart cities.

1) SMART GOVERNMENT

Smart government plays a crucial role in a smart city. The purpose of smart government is to better serve citizens and communities by interconnecting data, institutions, proceedings, and physical infrastructures based on information technology [12]. In addition, smart governance enables citizens to get involved in public decisions and city planning [13], which can improve the efficiency while simultaneously increasing information transparency. For example, e-government allows individuals to utilize governmental services online, such as applying for a conference center, paying for bills and reporting problems.

2) SMART TRANSPORTATION

Smart transportation aims to provide a ''smarter'' usage of transport systems. Specifically, intelligent transport networks can better serve the public by enhancing safety, speed and reliability [14]. By using transport-oriented mobile applications, consumers can easily plan their schedules while finding the most economic and fastest routes. Other common applications in smart transport facilities are driver's passports, license recognition systems, car-parking searching and prediction [15].

3) SMART ENVIRONMENT

Smart environment can contribute substantially in terms of building a sustainable society. Specifically, by adopting technical management tools, a smart city has the ability to monitor energy consumption, air quality, the structural reliability of buildings, and traffic congestion and to address pollution or waste efficiently [16]. Ideally, novel environmental sensor networks may even have the ability to predict and detect natural disasters in the future [17].

4) SMART UTILITIES

Smart utilities enable smart cities to reduce the overconsumption of resources such as water and gas and to improve economic growth and contribute to environmental protection. Smart metering, as a practical smart utility application, is widely applied in smart grids to monitor the distributed energy resources [18]. In addition, smart water meters [19] and smart light sensors [20] are used to manage resources and reduce energy loss.

5) SMART SERVICES

Smart services benefit citizens in many aspects. For example, intelligent healthcare applications can timely monitor people's health conditions via wearable devices and medical sensors [21]. Furthermore, some smart services can create comfortable, intelligent and energy-saving living environments, such as through the remote control of home appliances. Last but not the least, social networking, entertainment, smart shopping and other smart services have considerably improved the convenience of people's daily lives.

C. CHARACTERISTICS

It is important to understand the differences between the aforementioned smart applications and traditional ones. Moreover, the characteristics (as illustrated in Fig. 3) of smart cities should be considered and combined before developing any new security or privacy protection method.

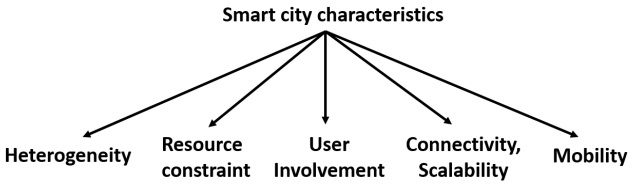


FIGURE 3. Characteristics of smart cities.

1) HETEROGENEITY

In IoT-based systems, high heterogeneity is the most distinguishing characteristic, which means the systems are independent, distributed, being stored or used by different users. It also refers to the wide variety of IoT nodes, communication protocols and technologies, mobility means, diverse hardware performances, platforms, etc. [22]. To the best of our knowledge, there is no uniform definition of smart city, and the IoT architecture varies by smart city. Therefore, the lack of a common security framework and service is another major problem.

2) RESOURCE CONSTRAINTS

Most IoT devices are resource constrained, which means not only limited memory, battery capacity and processing capabilities, but also constrained network interfaces due to low-power radio standards. To be more specific, cheaper, smaller, but energy deficient embedded devices are widely applied in smart cities. Typically, the random-access memory and storage capacities of these devices are limited, with 8-bit or 16-bit microcontrollers. The wireless networks equipped with IEEE 802.15.4 radio lead to low data rates and frame sizes (20-250 kb/s and up to 127 octets, respectively) [23].

3) MOBILITY

Urban mobility has been seen as an important engine for the growth and progress of modern cities. In smart cities, mobility refers not just to the movement within a city and the delivery of goods from one place to another destination, it also means technologies like citywide wireless communication and real-time monitoring of the traffic flow, as well as the flexible reactions to problems. In addition, mobility in smart cities is customized through the well-developed communication infrastructure.

4) CONNECTIVITY AND SCALABILITY

Connectivity enables any device to connect to the smart world. It is the most basic feature for a successful smart city and has been regarded as fundamental to moving smart city plans forward [24]. At the same time, scalability is an apparent feature in smart city scenarios. Smart cities are rapidly developing from small to large, resulting in explosive growth in both data and network traffic. Therefore, a smart city is not able to operate well without scalable systems and mechanisms.

5) USER INVOLVEMENT

The definition of a smart city is not just about cutting-edge technologies and infrastructures, human factors (learning, creativity, and education) are also essential for the development of smart cities [25] since the main purpose of building smart cities is to serve residents. Furthermore, citizens' involvement can improve the quality of those smart applications. For example, an initial understanding of their requirements and concerns regarding security will result in the best outcome in terms of protection strategies.

III. SECURITY AND PRIVACY ISSUES IN SMART CITIES

Although the aforementioned developments in smart cities have contributed considerably to the improvements of the whole society, almost every smart application is vulnerable hacking through up-to-date attacks, such as background knowledge attacks, collusion attacks, Sybil attacks, eavesdropping attacks, spam attacks, likability attacks, inside curious attacks, outside forgery attacks, and identity attacks [81], [100].

In recent years, significant problems have been found in different application scenarios. For example, the smart metering infrastructure in smart grids can monitor the private lives of residents, including their living habits and working hours [101]. Similarly, in the context of smart homes and healthcare, device manufacturers and service providers may gain access to the sensitive data [104]. In addition, the large amount of trajectory information collected by smart mobility applications can be used to infer the location and mobility patterns of a user [102]. In addition to these problems, the following items are the latest issues generated by the rapidly developing smart applications.

A. BOTNET ACTIVITIES IN IOT-BASED SMART CITIES

The recently emerged IoT botnets have posed serious threats to IoT systems. A representative example is the Mirai botnet, which can infect devices (e.g., IP cameras, webcams, printers, DVRs, and routers), spread infection to many heterogeneous IoT devices, and finally cause a DDoS against target servers [106]. Compared with computers and smart phones, IoT devices are often designed with poor security or even none at all. Unfortunately, this danger was not realized until the second half of 2016. Therefore, much more work is needed, and the security community should develop novel defences. Otherwise, this new normal of DDos attacks will have a destructive impact on the IoT-enabled ecosystem [97].

B. THREATS OF DRIVERLESS CARS IN SMART CITIES

High-tech companies have spent billions of dollars developing autonomous vehicles (AVs), aiming to reduce traffic accidents and to build a cleaner and smarter society [103]. However, this rapidly growing application has been seen as a major security issue because once an AV is hacked, both life safety and data privacy will be threatened [107]. Specifically, hackers can exploit security bugs to conduct remote attacks, such as applying the brakes, shutting down the engine and controlling the steering. In addition, the massive personal data collected by the computer system of a self-driving vehicle may cause significant privacy issues.

C. PRIVACY ISSUES OF VIRTUAL REALITY IN SMART CITIES

In technology-driven smart cities, virtual reality (VR) technology has been embraced by various organizations and entities, such as city planning departments, healthcare service providers and the engineering industry sector. However, the sensitive information shared with third parties, the unencrypted communications between VR devices, and the data stored by sensors all pose threats of privacy leakage [109]. Unfortunately, because these new applications are rushed to market, designers and users have not made appropriate and comprehensive privacy considerations.

D. THREATS POSED BY AI IN SMART CITIES

AI systems play indispensable roles in various smart applications, such as automatic control of trading systems, home appliances and pacemakers. However, the growing use of AI also poses security risks. For example, service providers and device manufactures can use data mining technologies to excessively analyze personal data and to extract sensitive information that exceed the primary objectives of the related services [90]. Furthermore, attackers with knowledge of AI are also getting smarter [91]. Hackers may understand how ML-based protection mechanisms were trained or designed so that they are able to adopt targeted approaches to weaken the training effects and to reduce the reliability of the algorithms.

IV. SECURITY REQUIREMENTS

Considering the characteristics of IoT devices, the complex environment of smart cities, and the security and privacy threats mentioned earlier, the remainder of this section focuses mainly on identifying the requirements related to securing smart cities.

A. AUTHENTICATION AND CONFIDENTIALITY

Authentication is a basic requirement for different layers of a smart system and is needed to prove identities and ensure that only authorized clients can access services across a heterogeneous system [26]. Specifically, IoT devices deployed in smart cities can authenticate the network, other nodes, and the messages from management stations. Furthermore, since the quantity of authentication data is growing explosively in smart cities, it is important to develop advanced technologies to guarantee real-time and precise authentication.

The purpose of confidentiality is to prevent information from passive attacks or being exposed to the wrong source. In IoT-based applications, attackers are assumed to have the ability to eavesdrop on communication or to access devices. Therefore, to protect the confidentiality of information transmission between nodes, encryption-based technologies are widely applied to build reliable communication and storage systems [27].

It is notable that transparency and reliability are two factors that make the design of identification and authentication methods difficult [28].

B. AVAILABILITY AND INTEGRITY

In general, availability means that devices and services should be available when needed. Corresponding to our topic, smart systems or applications should have the ability to maintain effective functioning even when under attack. Moreover, since these devices are susceptible to attacks, a smart system must be able to detect any abnormal conditions and have the ability to stop further damage to the system. Resilience is regarded as the attack-resistance ability of a system that can tolerate various faults and failures caused by attacks and large-scale disasters. Protection mechanisms should have strong robustness and the ability to continue learning adaptively to cope with the increasingly intelligent attacks.

It is also important to ensure the integrity of both IoT devices and the data exchanged between devices and the cloud. Because data are exchanged across many devices in an overall smart application, the data are easily tampered with during the transmission process if they are not well protected. Some methods such as firewalls and protocols can manage data traffic in IoT communications, but they cannot guarantee the integrity at endpoints because of the low computational power of most IoT devices.

C. LIGHTWEIGHT INTRUSION DETECTION AND PREDICTION

According to the vulnerabilities of the devices and networks deployed in a smart city, a smart system can be seen as secure only if it has the ability to monitor its operation conditions and to detect any abnormal events in a timely manner. The traditional intrusion detection system (IDS) is widely used in three approaches: misuse detection, anomaly detection, and specification-based detection [29]. However, in the heterogeneous and complex smart city ecosystem, the simple adaptation of a global IDS solution is not flexible and is unrealistic [30]. In addition, because most of the sensors and devices are resource-constrained, lightweight intrusion detection methods must be developed.

Prediction and knowing about incoming threats in advance is better than detection and recovery after an attacks. Xynos *et al.* [31] found that many intrusion prediction systems (IPS) failed to detect and prevent attacks, with a high failure rate, especially for web-based applications. Similarly, one study focused on smart grids indicated that many harmful attacks are caught off guard, which means that it is too late to take measures after detecting the attack, and current security protection strategies are unable to provide sufficient protection for a smart grid [32].

Therefore, it is of great importance to develop intelligent IPS systems to achieve security situation awareness and to automatically predict various attacks on smart applications.

D. PRIVACY PROTECTION

Privacy and security are closely related; all the requirements presented before can affect privacy protection. The necessity of this subsection is to include some security prerequisites that were not covered by previous subsections.

In smart city scenarios, in addition to some common harms, such as packet interception in communication, malware in mobile devices and applications, hacking on servers and falsification permission, sensitive data leakage, whether intentional or unintentional, is the main cause of privacy breaches. In 2017, a comprehensive survey [3] reported that four sources of data can be used to hack privacy, namely, observable data, repurposed data, published data, and leaked data, which contains large amount of users' sensitive information. To avoid misuse by unauthorized persons, adequate and effective countermeasures, such as encryption methods and anonymous mechanisms, and some novel techniques, such as differential privacy [33], must be applied.

Sometimes, the privacy of citizens can be breached even though a system is secure and not harmed by offenders. One potential way for this to occur is the powerful data mining algorithms. With these mining tools, some service providers and third parties can easily discover consumers' personal information, for example, the example provided by [34]. Accordingly, privacy preserving data mining (PPDM) strategies must be employed.

It is also worthwhile to note that the adoption of only technical solutions is not sufficient, although they have some positive effects. Other means of protection, such as governance, education, and policies, should also be implemented [81].

V. CURRENT SECURITY AND PRIVACY PROTECTION TECHNOLOGIES

In this section, we highlight critical insights into current and potential technologies used to handle security and privacy threats in the smart city environment. Table 2 shows the technical examples used in this section from the perspectives of different disciplines.

A. CRYPTOGRAPHY

Cryptographic algorithms are the backbone of security and privacy protection for the services of smart applications because they avoid the access of distrusted parties during the data life circle of storing, processing and sharing. In this subsection, we attempt to summarize the current cryptographic tools applied to smart systems and to highlight some novel and promising technologies.

Traditional algorithm and encryption standards are not completely suitable for resource-constrained devices because of the computational complexity and energy consumption [22]. Therefore, lightweight encryption has become a basic requirement for applying cryptographic technologies in practice. In 2016, Mahmood *et al.* [42] developed a lightweight authentication mechanism for an IoT scenario that can protect end-to-end users' communications from DDoS attacks. Recently, a novel lightweight authentication protocol was proposed by Li *et al.* [43] by adopting a public key encryption scheme and aiming to secure smart city applications.

It is notable that homomorphic encryption (HE), which enables computations on encrypted data and chains different services together without exposing sensitive data, has attracted increasing attention. For example, HE can be used to protect electricity consumption aggregation in a smart grid system [36], to protect privacy for healthcare monitoring [44], and to solve cloud computing security issues [45]. However, although full HE witnessed some breakthroughs in recent years, the high computational expense remains a restriction of the method.

Zero-knowledge proofs, first introduced by Goldwasser *et al.* [46], is another method applied in the cryptographic domain to enable one party to prove something to other parties without conveying any other information. Zero-knowledge proofs can be used to handle authentication issues. For example, Dousti and Jalili [38] used zero-knowledge proofs to develop an efficient authentication protocol for smart cards.

B. BLOCKCHAIN

Although the blockchain technique is a specific technology rather than a discipline, we use this subsection to introduce it because of the substantially increasing interest around it in recent years. A comprehensive survey in this field was conducted in 2016 by Christidis and Devetsikiotis [47], who verified the realizability of applying blockchian to the IoT domain and indicated its significant application value in the developing IoT ecosystem.

The decentralized feature of blockchain enables applications to operate in a distributed manner, which is the main reason behind the popularity of many blockchain-based IoT applications. For example, in 2016, Biswas and Muthukkumarasamy [48] developed a blockchain-based security framework that can both guarantee the communication security of devices in a smart city and improve the reliability and efficiency of the system. Similarly, in 2017, Dorri *et al.* [39] integrated blockchian technology into a smart home scenario, and the newly developed framework can achieve the goal of confidentiality, integrity, and availability. Another recent study conducted by Lei *et al.* [40] addressed the security issues in vehicular communication systems through the blockchain structure.

Sharma *et al.* [49] indicated that existing clouds cannot satisfy the new requirements of future scalable IoT networks. They made use of blockchain's advantages in combination with fog computing and software defined networking (SDN) technology to develop a novel distributed architecture that satisfies the required design principles, such as resilience, efficiency, adaptability, scalability, and security.

Clearly, although blockchain technology has become a hot topic in recent years and has resulted in more reliable and convenient applications, it is still at a quite early stage in the IoT era. We need to take steps to better utilize this technology to settle serious privacy and security concerns.

C. BIOMETRICS

In IoT-based systems, biometrics are widely for authentication. Specifically, this technology can be used to

TABLE 2. Examples of security and privacy protection methods in smart cities.

Disciplines	Year	References	Applications scenario	Technologies
Cryptography	2017	[35]	Smart transportation	Two-level authentication key exchange scheme
	2016	[36]	Smart grid	Homomorphic encryption
	2017	[37]	Smart shopping	RFID
	2016	[38]	Smart card	Zero-knowledge proofs
Blockchain	2017	[39]	Smart home	Blockchain-based smart home architecture
	2017	[40]	Smart transportation	Network topology and decentralized blockchain-based framework
	2017	[49]	IoT architecture	Distributed architecture based on blockchain technique and fog computing
Biometrics	2016	[41]	Mobile sensors	Cascading bandpass filter for noise cancellation
	2017	[51]	Storage devices	Biometric based authentication and key negotiation protocol
ML and DM	2017	[56]	Wi-Fi networks	Deep feature learning
	2015	[57]	Smartphone	SVM-based authentication system
	2017	[58]	Mobile devices	Bayesian linear regression model
	2017	[64]	Social networking	Privacy preserving k-means clustering
Game theory	2017	[68]	Low-resource IoT devices	Nash Equilibrium
	2016	[69]	Honeypot-enabled networks	Bayesian game of incomplete information
	2016	[71]	Wireless networks	Zero-sum game
Ontology	2016	[77]	Smart home	Layered cloud architectural mode based on ontology
	2017	[79]	Mobile computing	Context-aware and personalized privacy control
	2017	[82]	IoT architecture	Semantic-ontology-based situation reasoning method

automatically recognize a person through unique behavioral and biological characteristics. The bio-data are extracted from fingerprints, faces, voices, handwritten signatures and so on. One method worth mentioning here is brainwave-based authentication [50], which can achieve a high degree of authentication accuracy while simultaneously guaranteeing efficiency.

To protect the confidential information of users in storage devices, a key negotiation and mutual authentication protocol was proposed by Amin *et al.* [51]. The novel protocol not only effectively defeats security attacks but also maintains an acceptable communication cost and overhead in comparison with other related systems.

Another characteristic to note is that if these bio-based methods are not appropriately used, the risk of privacy leakage will increase. Natguanathan *et al.* [52] reported that we need to develop privacy-preserving biometric schemes (PPBSs), such as the work performed by Wang *et al.*, [53]. They also indicated the promising future of using biometrics in other applications, such as e-business.

D. MACHINE LEARNING AND DATA MINING

Based on the current practical situations, machine learning (ML) technologies have been employed to improve the efficiency of intrusion detection systems, which is one of the most commonly used security infrastructures to protect networks from attacks. Wireless sensor network (WSNs) the key component of the smart world, have received increasing attention. A comprehensive survey [54] indicated three advantages of adopting machine learning technologies to secure WSNs and summarized different ML algorithms. Luo *et al.* [55] proposed a machine-based scheme to secure data sensing and fusion in WSNs. Moreover, a recent study [56] developed a novel feature extraction and selection model to detect attacks in Wi-Fi networks, which has a high detection rate.

In addition to network-centric security methods, a few user-centric ML technologies have been applied in recent years to analyze, predict and make personalized decisions. The rapidly expanding sensor networks and smartphones have subjected citizens to many privacy and security concerns. Lee and Lee [57] adopted SVM to design a multi-sensor-based authentication system for smartphone users. The key idea was to learn users' behavior patterns and corresponding environmental features. In 2017, researchers [58] developed a novel permission mechanism for mobile platforms based on ML technology. However, similar efforts, such as [59] and [60], have a common problem, that is, the data used for analysis cannot avoid of the subjectiveness of participants and may not sufficient reflect the situation in a real IoT environment.

We note that many defense strategies can be strengthened by ML technologies. Shamshirband *et al.* [61] introduced a game theoretic model through ML to detect and prevent intrusions in WSNs. Biggio *et al.* [62] reviewed the current situation of the biometric security systems from the perspective of adversarial ML.

In the field of data mining (DM), a comprehensive survey conducted by Tsai *et al.* [63] indicated that vast quantities of data collected by many sensors and devices around consumers are used to mine new regulations and information to provide better services. However, some security and privacy concerns result from DM technologies because of the sensitive information, such as users' locations and behavioral patients, may be disclosed. To mitigate this problem, some privacy preserving data mining (PPDM) technologies have been developed in recent years [5], [64].

E. GAME THEORY

Game theory, a powerful mathematical tool, has been successfully applied in the fields of cybersecurity and privacy protection and in various application scenarios [65].

A comprehensive survey conducted by Do *et al.* [66] reported the characteristics of the game-theoretical approach and its advantages in comparison with traditional defense mechanisms, which are described below.

1) Proven mathematics;
2) Reliable defense;
3) Timely action;
4) Distributed solutions.

Predictably, interest in using game theory to address security and privacy issues in IoT-based applications has increased in recent years. For example, Abass *et al.* [67] developed novel attack analyzing strategies for cloud storage by evolutionary game theory. In another recent work, Sedjelmaci *et al.* [68] targeted low-powered devices and proposed a lightweight anomaly detection technique that both guarantees accuracy and reduces energy consumption.

Focusing on communication security issues in networks, La *et al.* [69] formulated a game theoretic model to study the attack and defense problem in honeypot-enabled networks. The model has potential to be adapted to new emerging IoT applications, such as smart healthcare, smart buildings, and sensor networks. Similarly, a recent paper written by Wang *et al.* [70] introduced a honeypot game to address attack problems in advanced metering infrastructure networks. Another work conducted by Xiao *et al.* [71] adopted a zero-sum game to detect spoofing attacks in wireless networks.

With respect to privacy issues, many studies develop mechanisms by combining game theory with other privacy protection technologies, such as k-anonymity [72] and differential privacy [73]. In addition, game theory is an effective tool to balance protection intensity and data utility, as in the approach proposed by Xu *et al.* [74] in 2015.

Although fewer studies have applied game theory to a specific smart city application, many technologies have been developed within the scope of IoT security, and we believe that with the rapid evolution of the everything-connected smart cities, game-theoretic approaches will play a significant role in solving some new security and privacy issues of this smart era.

F. ONTOLOGY

Ontology, one of the major branches of philosophy, has been identified as a promising tool to address heterogeneous issues, especially for unstructured data, knowledge and configurable systems. The main purpose of employing ontology is to better understand, describe, and reuse some formally represented knowledge and to search for new knowledge and isolate inconsistencies.

The aforementioned inherent features have advanced many ontology-based efforts to resolve security and privacy problems, such as cyber attack detection and security risk management [75], [76]. However, the application of ontology to the IoT domain is an emerging area, and only a few related efforts can be found recent years. Tao *et al.* [77] developed a novel ontology-based security management model in the domain of smart homes that enables smart devices to interact more effectively and improves the security of the system. Also applied to smart homes, Mohsin *et al.* [78] proposed an ontology-driven security analysis framework to support capturing consistencies automatically in the process of interactions.

As noted previously that mobile phones are the pivot of a smart city, Kim *et al.* [79] designed an ontology-based model called QoPI to characterize, represent, and manage users' personalized and dynamic privacy-control patterns under mobile computing situations. From the perspective of trust, Lee *et al.* [80] provided a novel definition of "trust ontology" and used it to measure the trustworthiness among content providers and consumers according to the preferences, purposes and perspectives of users.

One obvious limitation of the current ontology-based studies in terms of IoT security is that most of them focus on a specific application scenario or requirement and lack a unified model, which affects their application value. Attempting to solve this problem, in 2017, Xu *et al.* [82] proposed a semantic-ontology-based situation reasoning method that provides a more comprehensive view of the security situation while simultaneously improving the ability for emergency response. Unfortunately, this method only focuses on the network layer of the IoT architecture and cannot address the overall security problems.

G. NON-TECHNICAL SUPPLEMENTS

The application of technical solutions alone is not sufficient for protection. The existing technology limitations can be mitigated by the reinforcement of the related policy, regulation, governance, education and so on [81].

From the perspective of governance and politics, according to [83], sound governance is critical to creating a reliable smart system. Walravens [84] argued that governments have the responsibility to carefully consider which data can be opened and who has the right to access the data. Similarly, Batty *et al.* [85] indicated that regulations enforced by the government must protect data and model development under a smart city framework.

Training directed at improving the related skills of manufacturers, service providers, and users is also important [86]. For example, application designers should gain the ability to develop stable and resilient coding through training. Vendors are responsible for updating firewalls to fix vulnerabilities. Furthermore, device manufacturers should enhance the overall level of safety and quality standards as much as possible.

Education programmes aim to enrich citizens' knowledge of how smart applications operate and how to protect themselves [87]. However, the effectiveness remains a challenge. Aleisa and Renaud [88] found that although some users know the potential harms of privacy leakage, they ignore the concerns to take advantage of the convenience.

VI. CHALLENGES AND FUTURE DIRECTIONS

We have discussed current security and privacy protection technologies for smart cities. Many novel countermeasures have recently been proposed in various fields. Unfortunately, according to the updated threats and security requirements we noted earlier, it is reasonable to conclude that more effective protection methods must be developed to keep pace with the rapid growth of smart cities. The following items are promising opportunities and research directions based on our investigation.

A. IOT-BASED NETWORK SECURITY IN SMART CITIES

The IoT can be seen as a network of networks, in which heterogeneous networks, such as the Internet, smartphone networks, social networks, and industrial networks, are interconnected and integrated [94]. Under this type of complex environment, novel effective technologies are needed to cope with the latest challenges [95]. For example, an understanding of malware propagation characteristics in IoT-based infrastructures, modeling of the spread patterns of information in wireless sensor networks, and the development of effective prevention strategies are of great significance [98].

B. SECURITY AND PRIVACY ISSUES IN FOG-BASED SYSTEMS

As an emerging technology to implement smart cities, Fog-based structures present new security challenges because the operation environments of distributed Fog systems are more vulnerable to attacks than centralized clouds [108]. Compared with Clouds, Fog systems are small, resulting in their limited ability to protect themselves. In addition, as Fog nodes are close to end users, they provide precious opportunities to protect the privacy of consumers before personal sensitive data leave the edge. Therefore, the protections of smart devices in Fog-based smart systems should receive much more attention [96].

C. USER-CENTRIC AND PERSONALIZED PROTECTION METHODS

In user-centric smart cities, consumers should have the right to delete or move data from one service provider to any other service provider at any time [89]. Moreover, people's preferences towards security and privacy must be considered since attitudes and requirements can vary by person. Moreover, the growing number of configurable privacy settings makes it difficult for users to align their settings with their actual preferences [99]. Therefore, the development of user-friendly protection assistants that can both improve the security and comfort of various smart applications is promising.

D. DATA MINIMIZATION TOWARDS SMART APPLICATIONS

The task of ''data minimization'' is two-fold. One is to minimize the amount of data collected, used, and stored by IoT applications, which requires not only technical guarantees but also reinforcement from related governance and politics. The other is how to minimize the knowledge discovered. Specifically, service providers can only discover knowledge limited to the boundaries of their primary objectives and are unable to mine any other sensitive information from citizens without their permission [93].

E. LIGHTWEIGHT SECURITY SOLUTIONS

Although various novel mechanisms have been developed in recent years, the direct application of some of these mechanisms is unrealistic. The limited processing abilities and energy sources of sensors and devices make it possible for only basic and weak preserving algorithms to be implemented. Consequently, to satisfy the strong mobility, flexibility, dynamic and low-cost requirements, further research is required to develop lightweight countermeasures to minimize overhead while simultaneously guaranteeing protection.

F. THEORETICAL COMPLEMENT

Smart applications are being talked everywhere, and nearly every country has smart projects under development. However, no uniform concept of a smart city, including its definition and architecture, exists. Consequently, many of the developed security protection mechanisms and network protocols focus mainly on a specific area, which means they cannot be incorporated into and shared among the entire smart city environment. Therefore, additional theoretical studies are a necessary foundation to reduce the barriers to securing smart cities.

VII. SUMMARY

The widespread use of smart applications has caused many security and privacy issues. The development of more advanced protection models and frameworks is essential and highly demanded in both industrial and academic fields. Motivated by these factors, we surveyed the latest efforts and advances in countermeasures from the perspectives of different disciplines. We also discussed up-to-date issues and open challenges that have emerged in recent years to lay a foundation for further studies. Various protection mechanisms and strategies have been developed in recent years. However, there is a long way to go to satisfy the multiple security requirements of these rapidly developing smart applications. It is reasonable to predict that in the following few years, mitigating the presented challenges will be the primary task of smart city-related studies.

REFERENCES

[1] Department of Economiical and Social Affairs, *World Urbanization Prospects: The 2014 Revision, Highlights*. New York, NY, USA: United Nations Population Division, 2014.
[2] Y. Li, Y. Lin, and S. Geertman, ''The development of smart cities in China,'' in *Proc. 14th Int. Conf. Comput. Urban Planning Urban Manage.*, 2015, pp. 7–10.
[3] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, ''Security and privacy in smart city applications: Challenges and solutions,'' *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.
[4] K. Zetter, ''Inside the cunning, unprecedented hack of ukraine's power grid,'' *Wired*, Mar. 2016. [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedentedhack-ukraines-power-grid/

[5] L. Li, R. Lu, K.-K. R. Choo, A. Datta, and J. Shao, "Privacy-preserving-outsourced association rule mining on vertically partitioned databases," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1847–1861, Aug. 2016.

[6] B. Alomair and R. Poovendran, "Efficient authentication for mobile and pervasive computing," *IEEE Trans. Mobile Comput.*, vol. 13, no. 3, pp. 469–481, Mar. 2014.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[8] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct./Dec. 2017.

[9] A. Gharaibeh *et al.*, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[10] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2017.

[11] I. Yaqoob *et al.*, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017.

[12] J. R. Gil-Garcia, "Towards a smart state? Inter-agency collaboration, information integration, and beyond," *Inf. Polity*, vol. 17, nos. 3–4, pp. 269–280, 2012.

[13] S. Alawadhi and H. J. Scholl, "Smart governance: A cross-case analysis of smart city initiatives," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 2953–2963.

[14] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of Things is the backbone," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, Jul. 2016.

[15] E. Vlahogianni, K. Kepaptsoglou, V. Tsetsos, and M. Karlaftis, "A real-time parking prediction system for smart cities," *J. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 192–204, 2016.

[16] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[17] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," in *Proc. ASE BigData SocialInform.*, 2015, Art. no. 28.

[18] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renew. Sustain. Energy Rev.*, vol. 57, pp. 302–318, May 2016.

[19] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in *Proc. IEEE 13th Int. Conf. Ind. Inform. (INDIN)*, Jul. 2015, pp. 993–998.

[20] M. Magno, T. Polonelli, L. Benini, and E. Popovici, "A low cost, highly scalable wireless sensor network solution to achieve smart LED light control for green buildings," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2963–2973, May 2015.

[21] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.

[22] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[23] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the Internet of Things," *IEEE Commun. Mag.*, vol. 50, no. 12, pp. 144–149, Dec. 2012.

[24] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[25] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proc. 12th Annu. Int. Digit. Government Res. Conf., Digit. Government Innov. Challenging Times*, 2011, pp. 282–291.

[26] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.

[27] V. Angelakis, E. Tragos, H. C. Pöhls, A. Kapovits, and A. Bassi, *Designing, Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions*. Springer, 2017.

[28] Z.-K. Zhang, M. C. Y. Cho, and S. Shieh, "Emerging security threats and countermeasures in IoT," in *Proc. 10th ACM Symp. Inf., Comput. Commun. Secur.*, 2015, pp. 1–6.

[29] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1223–1237, 3rd Quart., 2013.

[30] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 656–666.

[31] K. Xynos, I. Sutherland, and A. Blyth, "Effectiveness of blocking evasions in intrusion prevention system," Univ. South Wales, Wales, U.K., Tech. Rep., 2013, pp. 1–6.

[32] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big data analysis based security situational awareness for smart grid," *IEEE Trans. Big Data*, to be published. [Online]. Available: https://ieeexplore.ieee.org/document/7587350/

[33] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography* (Lecture Notes in Computer Science), vol. 3876, S. Halevi and T. Rabin, Eds. Berlin, Germany: Springer, 2006, pp. 265–284.

[34] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, Oct. 2014.

[35] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2017.

[36] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 396–405, Jan. 2016.

[37] R. Li, T. Song, N. Capurso, J. Yu, J. Couture, and X. Cheng, "IoT applications on secure smart shopping system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1945–1954, Dec. 2017.

[38] M. S. Dousti and R. Jalili, "An efficient statistical zero-knowledge authentication protocol for smart cards," *Int. J. Comput. Math.*, vol. 93, no. 3, pp. 453–481, 2016.

[39] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[40] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 1832–1843, Dec. 2017.

[41] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.

[42] Z. Mahmood, H. Ning, and A. Ghafoor, "Lightweight two-level session key management for end user authentication in Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Dec. 2016, pp. 323–327.

[43] N. Li, D. Liu, and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Trans. Sustain. Comput.*, vol. 2, no. 4, pp. 359–370, Oct./Dec. 2017.

[44] M. S. H. Talpur, M. Z. A. Bhuiyan, and G. Wang, "Shared–node IoT network architecture with ubiquitous homomorphic encryption for healthcare monitoring," *Int. J. Embedded Syst.*, vol. 7, no. 1, pp. 43–54, 2014.

[45] I. Jabbar and S. Najim, "Using fully homomorphic encryption to secure cloud computing," *Internet Things Cloud Comput.*, vol. 4, no. 2, pp. 13–18, 2016.

[46] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, 1989.

[47] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

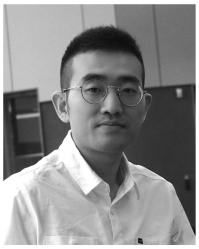
[48] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun.*, Dec. 2016, pp. 1392–1393.

[49] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[50] L. Zhou, C. Su, W. Chiu, and K.-H. Yeh, "You think, therefore you are: Transparent authentication system with brainwave-oriented bio-features for IoT networks," *IEEE Trans. Emerg. Topics Comput.*, to be published. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8057810/

[51] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," *IEEE Trans. Consum. Electron.*, vol. 63, no. 1, pp. 53–61, Feb. 2017.
[52] I. Natgunanathan, A. Mehmood, Y. Xiang, G. Beliakov, and J. Yearwood, "Protection of privacy in biometric data," *IEEE Access*, vol. 4, pp. 880–892, 2016.
[53] Y. Wang, J. Wan, J. Guo, Y.-M. Cheung, and P. C. Yuen, "Inference-based similarity search in randomized Montgomery domains for privacy-preserving biometric identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 7, pp. 1611–1624, Jul. 2017.
[54] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.
[55] X. Luo, D. Zhang, L. T. Yang, J. Liu, X. Chang, and H. Ning, "A kernel machine-based secure data sensing and fusion scheme in wireless sensor networks for the cyber-physical systems," *Future Gener. Comput. Syst.*, vol. 61, pp. 85–96, Aug. 2016.
[56] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 3, pp. 621–636, Mar. 2018.
[57] W.-H. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Feb. 2015, pp. 1–11.
[58] K. Olejnik, I. Dacosta, J. S. Machado, K. Huguenin, M. E. Khan, and J.-P. Hubaux, "SmarPer: Context-aware and automatic runtime-permissions for mobile devices," in *Proc. 38th IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 1058–1076.
[59] H. Lee and A. Kobsa, "Privacy preference modeling and prediction in a simulated campuswide IoT environment," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Mar. 2017, pp. 276–285.
[60] P. Wijesekera *et al.* (2017). "The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences." [Online]. Available: https://arxiv.org/abs/1703.02090
[61] S. Shamshirband, A. Patel, N. B. Anuar, M. L. M. Kiah, and A. Abraham, "Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks," *Eng. Appl. Artif. Intell.*, vol. 32, pp. 228–241, Jun. 2014.
[62] B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 31–41, Sep. 2015.
[63] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 77–97, 1st Quart., 2014.
[64] K. Xing, C. Hu, J. Yu, X. Cheng, and F. Zhang, "Mutual privacy preserving k-means clustering in social participatory sensing," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 2066–2076, Aug. 2017.
[65] S. Yu, "Big privacy: Challenges and opportunities of privacy study in the age of big data," *IEEE Access*, vol. 4, pp. 2751–2763, 2016.
[66] C. T. Do *et al.*, "Game theory for cyber security and privacy," *ACM Comput. Surv.*, vol. 50, no. 2, 2017, Art. no. 30.
[67] A. A. A. Abass, L. Xiao, N. B. Mandayam, and Z. Gajic, "Evolutionary game theoretic analysis of advanced persistent threats against cloud storage," *IEEE Access*, vol. 5, pp. 8482–8491, 2017.
[68] H. Sedjelmaci, S.-M. Senouci, and T. Taleb, "An accurate security game for low-resource IoT devices," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9381–9393, Oct. 2017.
[69] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1025–1035, Dec. 2016.
[70] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.
[71] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10037–10047, Dec. 2016.
[72] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2985–2993.
[73] M. Kearns, M. Pai, A. Roth, and J. Ullman, "Mechanism design in large games: Incentives and privacy," in *Proc. 5th Conf. Innov. Theor. Comput. Sci.*, 2014, pp. 403–410.
[74] L. Xu, C. Jiang, Y. Chen, Y. Ren, and K. J. R. Liu, "Privacy or utility in data collection? A contract theoretic approach," *J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1256–1269, Oct. 2015.
[75] A. Razzaq, Z. Anwar, H. F. Ahmad, K. Latif, and F. Munir, "Ontology for attack detection: An intelligent approach to Web application security," *Comput. Secur.*, vol. 45, pp. 124–146, Sep. 2014.
[76] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the Internet of Things," in *Proc. IEEE Int. Workshop Meas. Netw. (M&N)*, Oct. 2015, pp. 1–6.
[77] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Sep. 2016.
[78] M. Mohsin, Z. Anwar, F. Zaman, and E. Al-Shaer, "IoTChecker: A data-driven framework for security analytics of Internet of Things configurations," *Comput. Secur.*, vol. 70, pp. 199–223, Sep. 2017.
[79] S.-H. Kim, I.-Y. Ko, and S.-H. Kim, "Quality of private information (QoPI) model for effective representation and prediction of privacy controls in mobile computing," *Comput. Secur.*, vol. 66, pp. 1–19, May 2017.
[80] O.-J. Lee, H. L. Nguyen, J. E. Jung, T.-W. Um, and H.-W. Lee, "Towards ontological approach on trust-aware ambient services," *IEEE Access*, vol. 5, pp. 1589–1599, 2017.
[81] R. Kitchin, "Getting smarter about smart cities: Improving data privacy and data security," Dept. Taoiseach, Data Protection Unit, Dublin, Ireland, Tech. Rep., 2016.
[82] G. Xu, Y. Cao, Y. Ren, X. Li, and Z. Feng, "Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things," *IEEE Access*, vol. 5, pp. 21046–21056, 2017.
[83] A. Meijer and M. P. R. Bolívar, "Governing the smart city: A review of the literature on smart urban governance," *Int. Rev. Administ. Sci.*, vol. 82, no. 2, pp. 392–408, 2016.
[84] N. Walravens, "Mobile business and the smart city: Developing a business model framework to include public design parameters for mobile city services," *J. Theor. Appl. Electron. Commerce Res.*, vol. 7, no. 3, pp. 121–135, 2012.
[85] M. Batty *et al.*, "Smart cities of the future," *Eur. Phys. J. Special Topics*, vol. 214, no. 1, pp. 481–518, Nov. 2012.
[86] S. Misra, M. Maheswaran, and S. Hashmi, *Security Challenges and Approaches in Internet of Things*. Springer, 2017.
[87] W. Hurst, N. Shone, A. El Rhalibi, A. Happe, B. Kotze, and B. Duncan, "Advancing the micro-CI testbed for IoT cyber-security research and education," in *Proc. CLOUD Comput.*, 2017, p. 139.
[88] N. Aleisa and K. Renaud, "Yes, i know this IoT device might invade my privacy, but i love it anyway! A Study of Saudi Arabian Perceptions," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur. (IoTBDS)*, 2017, pp. 198–205.
[89] C. Perera, R. Ranjan, L. Wang, S. Khan, and A. Zomaya, "Privacy of big data in the Internet of Things era," *IEEE IT Prof. Mag.*, to be published.
[90] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.
[91] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An Internet of Things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.
[92] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.
[93] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing Internet of Things applications and platforms," in *Proc. 6th Int. Conf. Internet Things*, 2016, pp. 83–92.
[94] K. Xu, Y. Qu, and K. Yang, "A tutorial on the Internet of Things: From a heterogeneous network integration perspective," *IEEE Network*, vol. 30, no. 2, pp. 102–108, Mar. 2016.
[95] S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou, "Networking for big data: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 531–549, 1st Quart., 2016.
[96] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May/Jun. 2016.
[97] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
[98] S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 1, pp. 170–179, Jan. 2015.

[99] B. Liu *et al.*, "Follow my recommendations: A personalized privacy assistant for mobile app permissions," in *Proc. Symp. Usable Privacy Secur.*, 2016, pp. 1–16.
[100] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 3015–3045, 4th Quart., 2017.
[101] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1732–1745, 3rd Quart., 2014.
[102] Z. Ning, F. Xia, N. Ullah, X. J. Kong, and X. P. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.
[103] R. Petrolo, V. Loscrì, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, p. e2931, 2017.
[104] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. 7th Int. Symp. Parallel Archit., Algorithms Program. (PAAP)*, Dec. 2015, pp. 217–222.
[105] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. V5-376–V5-380.
[106] K. Angrishi. (2017). "Turning Internet of Things (IoT) into Internet of vulnerabilities (IoV): IoT botnets." [Online]. Available: https://arxiv.org/abs/1702.03681
[107] M. Hutson, "A matter of trust," *Science*, vol. 358, no. 6369, p. 1375, 2017.
[108] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.
[109] E. Baştuğ, M. Bennis, M. Médard, and M. Debbah, "Toward interconnected virtual reality: Opportunities, challenges, and enablers," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 110–117, Jun. 2017.



LEI CUI (S'17) received the B.S. degree from the College of Electrical and Power Engineering, Taiyuan University of Technology, China, in 2010. He is currently pursuing the Ph.D. degree with the School of Information Technology, Deakin University, Australia. His research interests include security and privacy issues in the IoT, social networks, and big data.

GANG XIE received the B.S. degree in control theory and the Ph.D. degree in circuits and systems from the Taiyuan University of Technology, China, in 1994 and 2006, respectively. He is currently the Vice President of the Taiyuan University of Science and Technology, China, and has also been a Professor of the Taiyuan University of Technology since 2008. He has authored over 100 papers and held five invention patents. His main research interests cover intelligent information processing, complex networks, and big data. He has received six provincial science and technology awards.

YOUYANG QU (S'17) received the B.S. and M.S. degrees from the Beijing Institute of Technology in 2012 and 2015, respectively. He is currently pursuing the Ph.D. degree with the School of Information Technology, Deakin University. His research interests focus on addressing security and privacy issues in social networks, cloud computing, IoT, and big data.

LONGXIANG GAO (SM'17) received the Ph.D. degree in computer science from Deakin University, Australia. He was a Post-Doctoral Research Fellow with IBM Research and Development, Australia. He is currently a Lecturer with the School of Information Technology, Deakin University. His research interests include data processing, mobile social networks, fog computing, and network security.

Dr. Gao has over 30 publications, including patents, monographs, book chapters, and journal and conference papers. Some of his publications have been published in the top venues, such as IEEE TMC, IEEE IoT, IEEE TDSC, and IEEE TVT. He received the 2012 Chinese Government Award for Outstanding Students Abroad (Ranked No.1 in Victoria and Tasmania consular districts). He is active in the IEEE Communication Society. He has served as the a TPC co-chair, a publicity co-chair, an organization chair, and a TPC member for many international conferences.

YUNYUN YANG received the B.Sc. degree in mathematics and applied mathematics from Xinzhou Teachers University, Xinzhou, China, in 2010, the M.Sc. degree in computer engineering from Yanshan University, Qinhuangdao, China, in 2013, and the Ph.D. degree from the College of Information Engineering, Taiyuan University of Technology, in 2017. She is currently a Teacher with the College of Electrical and Power Engineering, Taiyuan University of Technology. Her research interests include complex networks, big data, and machine learning.