Security and Privacy in Smart City Applications: Challenges and Solutions

Kuan Zhang∗, Jianbing Ni∗, Kan Yang∗, Xiaohui Liang†, Ju Ren‡, and Xuemin (Sherman) Shen∗
∗Department of Electrical and Computer Engineering, University of Waterloo, Canada
†Department of Computer Science, University of Massachusetts at Boston, USA
‡School of Information Science and Engineering, Central South University, China
Email:{k52zhang, j25ni, k62yang, sshen}@uwaterloo.ca, Xiaohui.Liang@umb.edu, ren_ju@csu.edu.cn

Abstract—With the flourish and advancement of the Internet of Things (IoT), smart city has become an emerging paradigm, consisting of ubiquitous sensing, heterogeneous network infrastructure, intelligent information processing and control systems. Smart city can real-timely monitor the physical world in people’s daily life and provide intelligent services to both citizens and travelers regarding transportation, healthcare, environment, entertainment and energy. However, security and privacy concerns are prone to raise, since smart city applications not only collect a wide range of privacy-sensitive information from people and their living circle, but also control city facilities and influence people’s life. In this article, we investigate security and privacy in smart city applications. Specifically, we first introduce the promising smart city applications and architecture. Then, we discuss several security and privacy challenges in these applications. Some research efforts are subsequently presented to address these security and privacy challenges for intelligent healthcare, transportation and smart energy. Finally, we point out some open issues and pose future research directions to provide security and privacy in smart city applications.

I. INTRODUCTION

With the rising economy and social transformation, people have been moving from country to cities, resulting in the largest wave of urbanization throughout the world. By 2030, the urban population is estimated to reach 5 billion (about 60% of the world population), which produces massive opportunities for the economic and social development of cities [1]. Due to the ever-growing demands from citizens, the development of fundamental infrastructure and policies are not correspondingly ensured. Moreover, the unplanned and overfast urban growth brings excessive burden to climate, energy, environment and even living. These problems slow down the sustainable development of urban cities in consequence. To mitigate the problems from rapid urbanization, it is urgent to improve governance and service delivery, offer swift seamless mobility, and achieve easy access to urban public facilities, affordable housing, quality healthcare, education and living in the highly populated area [2]. A special spotlight covering urbanization trends in innovative management of urban operations and a variety of “smart” services to citizens, visitors and the government to satisfy the ever-increasing and diverse demands [3]. The advancement and flourish of smart city shed light on the materializing these value-added services and tackling the problems of urbanization.

As an emerging paradigm, smart city leverages a variety of promising techniques, such as the Internet of Things (IoT), cyber physical system, big data analysis and real-time control, to enable intelligent services and provide comfortable life for citizens [4]. It integrates ubiquitous sensing components, the heterogeneous network infrastructure and powerful computing systems to sense the physical changes from cities and feedback to the physical world. Specifically, RFID devices, sensors and versatile wearable devices are promoted to offer real-time monitoring and ubiquitous sensing, from energy to environments, from road traffic to healthcare, from home area to public venues, etc. Then, this sensing information is transmitted to a control center via heterogeneous networks. This control center takes comparative advantages of powerful computing systems, such as cloud server, to process and analyze the collected data. Fueled by human intelligence, the control center makes optimal decisions and manipulates the urban operations via feedback components, such as actuators [3]. Having the advanced information, communication and control technologies as backbones, smart city can offer various applications, including intelligent transportation, smart energy, intelligent healthcare and smart home. This up-and-coming connected city cannot only timely identify the demands from people and city, but also manipulate the urban operations to improve the urban living quality in an intelligent and sustainable way. It is expected that the global smart city market would exceed $1,200 billion by 2020, which is almost tripled compared with that in 2014 [1].

When cities become smarter, people may suffer from a series of security and privacy threats due to the vulnerabilities of smart city applications [5]. For example, malicious attackers may generate false data to manipulate sensing results such that services, decisions and control in smart city are influenced and not “intelligent” enough. Moreover, these malicious attackers could also launch denial-of-service attacks, disrupting the sensing, transmission and control to degrade the quality of intelligent services in smart city. In addition, the pervasive video surveillance in smart city captures a tremendous number of images or video clips, which may be utilized to infer citizen’s trajectory and inherently endanger their privacy. The home area information collected and managed by smart home applications may pave the way of disclosing residence’s highly privacy-sensitive lifestyle and even causing economic loss. Although some off-the-shelf techniques (encryption, authentication, anonymity, etc.) and policies might be directly applied to avert these problems [5], the emerging “smart” attackers could still infer and violate privacy in many other ways,
such as side channel attack and cold boot attack [6]. Without sufficient security and privacy protections, users may refrain from accepting smart city, which would remain as a far-off futuristic idea.

These emerging trends motivate our research in investigating the not-for-profit global initiative of security and privacy for smart city. In this article, we first introduce smart city applications and a heterogeneous architecture. Then, we discuss several challenging security and privacy issues, including privacy leakage, secure information processing, and dependability in control. Some innovative research efforts are presented to address these challenges in various smart city applications. Finally, we point out several open research directions and outlook the smart city from the security and privacy perspective.

II. SMART CITY APPLICATIONS AND ARCHITECTURE

As smart city connects the physical world and information world, many intelligent applications are emerging from local to global, from sensing to control, as shown in Fig. 1. In this section, we introduce smart city applications and the heterogeneous architecture.

A. Smart City Applications

Smart city applications benefit people and the city in a variety of aspects: energy, environment, industry, living and services. We introduce several key applications as follows.

1) Smart Energy: Exploiting the widely deployed sensors to monitor the energy generation, transmission, distribution and consumption, smart energy [7] leverages utility usage, electric vehicle charging, smart grid, etc. It cannot only reduce the energy consumption in many aspects, but also prevent blackout of power grid and failure of individual energy usage.

2) Smart Environment: Smart environment is promoted to support the comfortable climate and sustainable environment for smart city. Ubiquitous sensing and intelligent climate management are jointly applied in smart environment applications [4]. They can monitor waste gas, greenhouse gas, city noise, air and water pollution, forest condition, etc., to afford the intelligent and sustainable development.

3) Smart Industry: With the main driver of industrial sustainable development in smart city, smart industry rolls out to optimize the industrial production and manufacture, while achieving efficiency and robustness. On one hand, it curtails the material and resource consumption (e.g., labor, time and production lines) during the industrial process; on the other hand, it prevents the industrial waste heat and waste gas from excessive emission. Both sensing and control are equally arresting components in smart industry, which requires real-time feedback and precise operations. Finally, servo actuators, motors and robots are adopted to enable precise control and operations in consequence of smart industry.

4) Smart Living: In home areas, smart living offers intelligent management of various appliances and utility to create comfortable home and improve the energy efficiency simultaneously [6]. It can enable remote control of home appliances, climate adjustment, energy saving, surveillance, entertainment and education. In the community (or building) wide, smart living applications also intelligently manage waste recycling, social network and parking to provide a smart community (or building) with comfortable life, intimate service, wonderful experience, sustainable environment and energy.

5) Smart Service: Smart service enables the public facilities and services to benefit people in a wide range of aspects [1]. For example, intelligent transportation [8] can help citizens and travelers to avoid road traffic congestion, enable road navigation, discover points of interests, manage the travel planning, etc. The road traffic information can be collected by the deployed sensors, camera at the intersections, GPS, smart-
phones from people on the road, etc. The control center adjusts travelers’ road plans and feedbacks to their smartphones or GPS. In addition, the road traffic can be adjusted by managing the traffic light and public transportation tools, such as bus, train and shared bicycle.

To provide quality healthcare, intelligent healthcare enables continuous health monitoring and timely diagnosis (including health warning) to the people in smart city [9]. It relies on wearable devices and medical sensors to measure users’ health conditions, and sends health data to the processing unit for doctor’s further diagnosis. It also provides easy access to user’s historical comprehensive health information, considerably increasing the chance to diagnose chronic or infectious diseases in the early stage. In addition, intelligent healthcare contains various health-related applications, such as home care, emergency alarm, intelligent fitness and training.

B. Smart City Architecture

To achieve ubiquitous sensing and finesse city management, smart city manipulates the information sensed from the physical world, the information transmitted in the communication world and the information processed in the information world for intelligent services. It incorporates sensing components, heterogeneous network infrastructure, processing unit, control and operating components as shown in Fig. 2.

1) Sensing Components: Sensing components exploit wearable devices, industrial sensors and smart devices, e.g., smartphones, smart meters and video surveillance camera [4] to measure the information from the physical world and transmit this information to the processing unit for decision making. In other words, sensing components are the bridge connecting the physical world and information world. The sensing devices are either deployed by the government, departments and companies, or carried by users as discussed in Section II-A. In addition, due to the limitations of device size, battery and processing capabilities, these resource-constrained sensing devices usually pre-process or compress the real-time and granular data before sending to the network.

2) Heterogeneous Networks: With the coexistence of massive sensing devices and various applications [9], the sensing information is collected in different ways such that the heterogeneous network infrastructure plays an instrumental role of supporting smart city. Heterogeneous networks incorporate cellular network, Wireless Local Area Networks (WLANs), Wide Area Network (WAN), Device-to-Device (D2D) communications, millimeter wave communications, sensor networks, etc., and enables the seamless switch among different types of networks. Heterogeneous networks represent the communication world in smart city to connect the physical world and information world.

3) Processing Unit: The processing unit exploits the powerful cloud computing servers, abundant database and dedicated control systems to analyze and process the collected sensing information from the physical world for decision making. The processing unit manages the information world in smart city. Authorized entities, such as the government, hospital, in-
industrial factory, users, etc., have certain privilege and authorization to access the collected information. They can also determine the requirements or policies for decision making and control in smart city.

4) Control and Operating Components: Leveraging the optimization and decision from the processing unit, smart city feedbacks to manipulate the physical world via the control and operating components, such as servo actuator or smartphones. These control and operating components optimize and make adjustments to the physical world such that the quality living can be offered in smart city. They also implement the two-way flow of smart city, i.e., sensing and control. This two-way flow cannot only acquire the knowledge about the physical world, but also monitor and manage every device or component in smart city to make it operate properly and “smart”.

III. SECURITY AND PRIVACY ISSUES IN SMART CITY

Although cities are seeking to become “smarter”, smart city applications raise a series of concerns and challenges in terms of security and privacy. As an information and networking paradigm, smart city should be able to defend the involved information from unauthorized access, disclosure, disruption, modification, inspection, and annihilation. Underlying security and privacy requirements, including confidentiality, integrity, non-repudiation, availability, access control and privacy [5], should be satisfied in the information, communication and physical worlds. Besides these general requirements, securing smart city still faces a set of unique challenges. One hand, smart city collects granular-scale and privacy-sensitive information from people’s life and environment; on the other hand, it processes this information, manipulates and impacts people’s life. Due to these unique characteristics, security and privacy issues become challenging and prevent smart city from being tempting enough to encourage more use.

A. Privacy Leakage in Data Sensing

Smart city is vulnerable to privacy leakage and information inferring by outside attackers, since private information is collected, transmitted and processed. The disclosed privacy in smart city may contain user’s identity and location in transportation, health condition in healthcare, lifestyle inferred from intelligent surveillance, smart energy, home and community, etc. It would be a major oversight to disclose this privacy-sensitive information to untrusted or unauthorized entities in both physical world and communication world. To preserve user privacy during data sensing, some off-the-shelf security and privacy techniques, such as encryption, anonymity and access control, can be applied [10] and [11]. Martinez et al. [5] propose a set of privacy concepts and general privacy requirements towards smart city applications. The privacy of identity, query, location, footprint and owner is identified and provided with some basic ideas to solve the general problems.

However, a portion of private information may still be unconsciously disclosed to untrusted entities. For example, intelligent surveillance may capture citizen’s daily life hint, style or even privacy, although it is originally designed for monitoring criminal behaviors in real and cyber world. Similarly, smart home also utilizes surveillance camera to detect theft or abnormal events. The intruded attackers in smart home may acquire private information about the home area, which is prejudicial to residence’s privacy. Most existing security and privacy protections [10] are developed against the outside eavesdroppers and attackers. But the potential inside attackers, such as agents, employees and security guards who can access surveillance records, may either steal user’s data or leave a gap for outside attackers. In addition, the data in smart city are in a highly granular scale and of diverse types such that the privacy requirements vary with different types. It is challenging to develop adjustable privacy protection mechanisms in smart city to balance the trade off between privacy and efficiency.

B. Privacy and Availability in Data Storage and Processing

As smart city takes the comparative advantages of powerful cloud servers on data storage and processing in the information world, it faces security threats due to the untrusted cloud servers. If the smart city data are in clear text during the storage and processing, they are directly revealed to the cloud server [12]. An alternative is to encrypt the smart city data and send ciphertexts to the cloud server for storage and processing [13]. Although this method prevents the untrusted cloud server from directly accessing the collected data, the cloud server cannot process the encrypted data and perform effective analytical operations for smart city applications. The latest breakthrough on fully homomorphic encryption sheds light on the processing, such as summation and comparison, over encrypted data. The computational overhead poses another impending challenge in terms of efficiency, especially when massive data are involved in smart city.

Another challenging issue of securing smart city goes into data sharing and access control. For example, the road traffic data can be collected by the deployed camera or traveler’s smartphones and GPS in a crowdsourcing way. During the global road planning, it is challenging to define the access policy and enable privacy-preserving data sharing among the collaboration. Therefore, smart city data storage and sharing requires extensive research efforts.

C. Trustworthy and Dependable Control

Smart city, having a two-way control flow, relies on the control system and actuators to materialize the operations determined by the control center. The control and feedback systems in the physical world, especially public and industrial infrastructure, become the highly attractive targets for attackers, criminals and even terrorists [14]. Denial-of-service attacks, spoofing attack, malicious data injection, etc., would disrupt the smart city such that the management, control and operation are either in a biased and incorrect way, or disabled. Most of these malicious attacks and misbehaviors are detected based on the third party inspection and auditing. In [15], data integrity functionality and digital signatures are adopted in software defined networks to achieve data integrity, access control, etc. Meanwhile, trusted computing is a state-of-the-art solution to resists operating system and software framework alterations.
However, these schemes consumes a large latency and high false rate to detect ‘smart’ attacks in smart city. As dependability of control is considered as the topmost priority in smart city, the efficient and fast detection of malicious attacks and misbehaviors become challenging requires collaborative efforts among various parties and stakeholders.

IV. SECURITY SOLUTIONS FOR SMART CITY PARADIGMS

To materialize the notion of security and privacy in smart city, balanced and pragmatic solutions are desired. In this section, we introduce state-of-the-art security and privacy protection schemes for several emerging smart city paradigms, including intelligent healthcare, intelligent transportation, and smart grid.

A. Privacy-preserving Infection Spread Analysis for Intelligent Healthcare

Intelligent healthcare, fueled by connected biomedical sensors, health data storage and processing units, provides preventive, curative and palliative health services. It can collect a wide range of real-time health data from users, analyze and defend severe healthcare issues in city wide, such as infectious disease spread. Infectious diseases, e.g., Ebola, flu and acute respiratory infection, could be rapidly spread in the population via human to human contact, especially when the infected patients cough and sneeze around crowd. People having frequent contact or strong social relationships with the patient (e.g., students studying in the same classroom, and families living in the same house) is usually considered as being susceptible from the perspectives of biomedical and sociology. An old-fashioned prevention approach is to isolate the susceptible people for a certain period. However, this approach does not consider their health condition and infectivity such that it has a series of negative impacts, including massive healthcare expense, economic loss of the isolated people, and panic or anxiety among the society.

To tackle the infection spread problem, intelligent healthcare would provide efficient diagnosis and health condition (or emergency) warning, by real-timely analyzing the infectivity during the outbreak season. Suppose a junior school student Bob is continuously monitored from both health and social perspectives during the outbreak of infectious disease. Once Bob’s immunity strength goes very low and he frequently contacts an infected student, he may be inferred as a susceptible patient in the early stage. The spread of infectious disease depends on user’s social contact and health condition. Specifically, this spread process can be affected by several key factors of infection, i.e., infectivity of the infected patient, immunity strength of the contacted user, contact duration and social tie.

The fusion of social network data together with the real-time health data facilitates a novel paradigm of infection analysis, as shown in Fig. 3. On one hand, social network employs a variety of applications to mine users’ social contact during their social interactions. For example, Wechat friend discovery program can find users in the physical proximity and record social interactions; speech recognition can detect if some people cough or sneeze; face-tagging function can identify user’s face from images. On the other hand, wearable devices and medical sensors can measure user’s real-time health condition [3,9].

However, the health and social network data are collected by multiple independent service providers, such as hospital and social network vendors (e.g., Facebook and Wechat), respectively. The collaboration of these service providers is the key challenge of enabling this enhanced infection analysis, and poses a series of security issues. Both social and health cloud servers are considered to be honest-but-curious [5] in intelligent healthcare applications. To preserve user’s data privacy and achieve data availability, homomorphic encryption [9] can be adopted to make both social network and health data invisible to the untrusted cloud servers. The collaboration of different untrusted cloud servers is achieved via the authorized entity (i.e., hospital authorized by users as shown in Fig. 3). However, when the hospital queries the infected patient’s data on the social cloud server, the social cloud server may infer that the queried user is infected even though the query content is still invisible. In addition, any entity without having the authorization from the data owner should not be able to query the owner’s data. State-of-the-art security and privacy protections are essential for intelligent healthcare. Without effective protections, users may not be willing to share their social and health data to others such that the infection analysis would be disabled.

To this end, conditional oblivious transfer protocol is developed for the privacy-preserving data query [9]. On one hand, it allows the authorized entity, such as doctors, to access the patient’s social network data from the social cloud server; on the other hand, it prevents the social cloud server from accessing the data and inferring any information about the query, such as the patient’s identity. Users or data owners are able to grant authorization to the trusted entity before the query. Any entity without user’s authorization cannot query any data. In addition, secure multi-party computation based
on homomorphic encryption [9] is utilized to prevent the untrusted health cloud from learning any private social and health data.

B. Secure Navigation for Intelligent Transportation

Smart city offers intelligent transportation services to citizens and visitors in various aspects, e.g., road traffic adjustment, navigation, point of interest recommendation, parking, etc. As an integral part of intelligent transportation, navigation, attracts extensive attentions [5]. Existing GPS devices can provide static navigation by showing the route on the pre-downloaded maps. However, it lacks real-time road traffic adjustment such that the calculated fastest route may be delayed by the dynamic congestions. Dynamic navigation exploits the human intelligence and dynamic road traffic sensing from travelers on the road and road side units (RSUs) in a crowdsourcing way [3].

As shown in Fig. 4, a querier, i.e., the querying vehicle in the navigation service, sends a navigation query to the closest RSU. The query contains the current location, destination and expired time. Then, the RSU forwards this query to the RSU that covers the destination through the network among RSUs. Upon receiving the navigation query, RSUs send the crowdsourcing task to the vehicles in its coverage area to find a fastest driving route for the querier. The querier retrieves the response from the RSUs when entering the coverage area of each RSU, and finally reaches the destination.

During this type of distributed navigation, the private location information of both querying vehicle and responding vehicles may be disclosed. To this end, Elgamal and AES schemes are utilized to encrypt the querier’s location and vehicle’s query privacy. To prevent RSUs from linking the navigation query and retrieving query to a specific vehicle, each vehicle randomizes the credential issued by the trusted authority to generate a group signature. In addition, to prevent the sensitive information in the navigation response from disclosing, the driving route is encrypted by Elgamal and AES schemes associated with a zero-knowledge range proof, which proves that the time cost is less than the given threshold, without exposing the exact value [8]. Finally, the traceability of group signature allows the trusted authority to trace any malicious vehicle which does not honestly follow the rules.

In summary, this privacy-preserving navigation scheme relies on the distributed RSUs to complete the road planning task in a crowdsourcing way. During the querying, crowdsourcing and navigation phases, both querier and responding vehicles can preserve location privacy.

C. Adaptive Key Management for Smart Grid

Smart grid relies on millions of smart meters to measure the real-time power consumption in residential areas or buildings as shown in Fig. 5. These metering data are aggregated to the control center to optimize the power distribution in return. However, a series of attacks attempt to tamper smart meter records and upload modified data to the control center [15]. Moreover, the ever-increasing volume of metering data poses a new challenging issue of managing secret keys for each device [6]. Predominantly, the data integrity and authentication should be achieved during the aggregation of smart metering. In addition, the metering data of home area may reflect the residence’s lifestyle, home condition (e.g., very low power consumption in a long duration indicates that residents are out) and preference [6]. If the untrusted aggregators learn and reveal this private information, the resident’s privacy would be jeopardized and even economic loss may be caused.

In [7], Zhang et al. propose a privacy-preserving aggregation scheme (PARK) to improve the computational efficiency and protect smart metering data from disclosing to untrusted aggregators. An adaptive key management scheme is developed based on bi-directional Hash chains, generating the encryption key for every smart meter during each period. The trusted authority calculates the decryption key for the aggregator as the summation of encryption keys from a group of smart meters. Only when having all $N$ ciphertexts, the aggregator can decrypt the summation of $N$ smart meters. If no smart meter joins or leaves the smart grid, every smart meter’s encryption key is automatically updated. The aggregator’s decryption key is updated in a synchronous way. The trusted authority determines the length of Hash chains, which reflects the reputation of smart meters. The meter with a high reputa-
tion receives the key with long expiry time. When some meters join or leave the smart grid, the trusted authority only needs to update the aggregator’s decryption key. The revocation overhead is mainly from the re-distribution of the decryption key. As shown in Fig. 6, the proposed PARK scheme costs one-time key distribution in every key update, while other schemes (an distributed key management and naive scheme [7]) update user’s encryption keys costing higher key update overhead. In addition, forward and backward secrecy is achieved based on the security of one-way Hash function.

V. FUTURE RESEARCH DIRECTIONS

Since some off-the-shelf security and privacy solutions [4] may not well conquer all the challenges in smart city, we discuss several open research directions including but not limited to the followings.

First, crowdsensing, which exploits smart sensing devices of citizens, can provide the improved sensing capability for smart city rather than purely relying on the pre-deployed fixed sensors. However, the crowdsensing accuracy may vary with contributor’s knowledge, preference, selfishness, etc. An initial idea of stimulating citizens to contribute for crowdsensing is to develop incentives for them. Moreover, trustworthiness should also be considered when designing incentive schemes. In addition, crowdsensing contributor’s privacy hidden in the sensing results may be jeopardized by “smarter” attackers. In particular, when multiple contributors pool their sensing results together, an individual contributor’s private information is likely to be collaboratively inferred by others. Therefore, how to achieve incentive and privacy remains as a challenge for crowdsensing in smart city.

Second, smart city is vulnerable to false data injection in both sensing and control phases. Digital signature techniques [9] cannot prevent the data from being tampered from the origination. An insight into detecting false data injection is to leverage machine learning and data mining to come up with a boundary of reasonable sensing data. Abnormal detection techniques may be an alternative to identify the false data. However, it is still an open issue requiring multidisciplinary knowledge and efforts to address.

Last but not least, the ever-growing volume of data and devices in smart city poses open problems for the sake of intelligent services and privacy. Inside attackers exploit human intelligence and have access to the big data such that the privacy of data owners may be inferred and violated even the traditional cryptographic schemes have been applied to big data. An alternative to detect these inside attackers is to enhance the traceability and allow the trusted third party to monitor and audit. Meanwhile, the collaborative efforts among municipalities, regulation departments, industry, academia and business companies are highly required to set up privacy policies and regulations. In addition, the data privacy, availability and management should be achieved simultaneously.

VI. CONCLUSIONS

In this article, we have investigated smart city and discussed the security and privacy challenges in emerging smart city applications. We have first introduced smart city applications in different aspects and discuss its architecture. Then, we have presented the general security and privacy requirements and identified several security challenges for smart city. In addition, we have dwelled in greater depth on state-of-the-art security and privacy solutions for smart city applications. Several open research directions are also discussed.

We hope this article could shed more lights on the security and privacy for smart city, where more ground-breaking research efforts along this emerging line would be put in the future.

ACKNOWLEDGEMENT

This research has been supported by a research grant from the Natural Science and Engineering Research Council (NSERC) and Care In Motion (CIM) Inc., Canada.

REFERENCES

Kuan Zhang (IEEE S’13) received the B.Sc. degree in Communications Engineering and the M.Sc. degree in Computer Science from Northeastern University, China, in 2009 and 2011, respectively. He received the Ph.D. degree in electrical and computer engineering from University of Waterloo, Canada, in 2016. Currently, he is a postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include security and privacy for mobile social networks, e-healthcare system, and cloud computing.

Jianbing Ni received his bachelor degree and master degree from University of Electronic Science and Technology of China in 2011 and 2014, respectively. Currently, he is pursuing the Ph.D. degree at the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo. His research interests include the security and privacy for crowdsourcing, vehicular ad hoc network, cloud computing and fog computing.

Kan Yang received his B. Eng. degree from University of Science and Technology of China in 2008 and his PhD degree from City University of Hong Kong in August 2013. He is currently a postdoctoral fellow of electrical and computer engineering department at University of Waterloo, Canada. He was a visiting scholar in State University of New York at Buffalo in 2012. His research interests include Cloud Security, Big Data Security, Cloud Data Mining, Cryptography, Social Networks, Wireless Communication and Networks, Distributed Systems etc.

Xiaohui Liang (IEEE M’15) received his Ph.D. degree at the department of Electrical and Computer Engineering of the University of Waterloo, and the master and the bachelor degrees at Computer Science department of the Shanghai Jiao Tong University. He was also a postdoctoral researcher at the Department of Computer Science, Dartmouth College, NH, USA. Since 2015, he has been an assistant professor of the Computer Science Department at the University of Massachusetts Boston. His research interests include security, privacy, and trustworthiness in medical cyber physical systems, cyber security for mobile social networks, and applied cryptography.

Ju Ren (IEEE S’13) received his B.Sc., M.Sc. and Ph.D. degrees in computer science from Central South University, China, in 2009, 2012 and 2016, respectively. From Aug. 2013 to Sept. 2015, he was a visiting Ph.D. student at the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Currently, he is a distinguished professor with the Department of Computer Science at Central South University, China. He has published over 20 peer-reviewed papers on some prestigious international journals and conferences, including IEEE TWC, TH, TVT, TETC and ComMag, etc. His research interests include wireless sensor network, mobile sensing/computing, transparent computing and cloud computing.

Xuemlin (Sherman) Shen (IEEE M’97-SM’02-F’09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982, and the M.Sc. and Ph.D. degrees from Rutgers University, Newark, NJ, USA, in 1987 and 1990, respectively, all in electrical engineering. Dr. Shen is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. Dr. Shen was a recipient of the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, 2010, and 2014 from the University of Waterloo; the Premier’s Research Excellence Award in 2003 from the province of ON; and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He served as the Technical Program Committee Chair/Co-Chair for ACM MobiHoc’15, IEEE Infocom’14, IEEE VTC’10 Fall, the Symposium Chair for IEEE ICC’10, the Tutorial Chair for IEEE VTC’11 Spring and IEEE ICC’08, the Technical Program Committee Chair for IEEE Globecom’07. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.