Big Data Privacy in the Internet of Things Era

Charith Perera, *The Open University*
Rajiv Ranjan, *Commonwealth Scientific and Industrial Research Organization*
Lizhe Wang, *Chinese Academy of Sciences*
Samee U. Khan, *North Dakota State University*
Albert Y. Zomaya, *University of Sydney*

The Internet of Things (IoT) enables data collection on a large scale, but the extraction of knowledge from this data can lead to user privacy issues. This article discusses privacy challenges in the IoT.

The Internet of Things (IoT)[1] is a network of networks in which a massive number of objects, sensors, or devices are connected through the ICT infrastructure to provide value-added services. The IoT connects people and things anytime, anyplace, with anything and anyone, ideally using any path or network and any service (although other definitions have also been proposed[2]). By 2020, 50 to 100 billion devices will be connected to the Internet,[2] generating *big data*[3] for analysis and knowledge extraction.

Big data has no clear definition,[3] but it isn't wholly about size. Rather, it's defined based on three primary characteristics, also known as the 3Vs: volume, variety, and velocity.[4] Volume relates to the data's size (terabytes, petabytes, or zettabytes). Variety refers to the type of data and its source (sensors, devices, social networks, the Web, mobile phones, and so on). Velocity means how frequently the data is generated (for instance, every millisecond, second, minute, hour, day, week, month, or year). It is widely believed that cloud computing provides a promising platform for storing and processing big data (see Table A in the Web extra at http://doi.ieeecomputersociety.org/10.1109/MITP.2015.34).

Even though data collected by individual devices might provide insufficient information, aggregated data from numerous physical devices and virtual sensors can provide a wealth of knowledge for important application areas, including disaster management, customer sentiment analysis, smart cities, and bio-surveillance.[2] Data collection and analysis in IoT applications has many objectives.

With customer sentiment analysis, for example, such data can be used to improve personalized recommendations, leading to better customer experiences. In the case of smart cities, governments and city councils can use the knowledge extracted to make strategic decisions and future city plans (traffic light placement, construction of new roads or bridges, and so on).[5,6] However, the data collected by smart IoT devices can contain sensitive personal information based on the application type and the data source. Therefore, such data must be managed carefully to avoid any user privacy violations.

Here, we briefly discuss the importance of addressing IoT privacy challenges[7] and present survey results that consolidate public opinion toward IoT solutions and their impact on user privacy. We also examine the research challenges that must be addressed for the IoT to become a pleasant experience for users and businesses, and highlight leading research in this field.

Privacy in Action: Looking Back

Jennifer Golbeck and Matthew Mauriello have shown that average Facebook users significantly underestimate the amount of data to which they allow third-party applications access.[8] The authors also noted that most of us tend to overlook privacy terms[9] and policies on the Web.

In the IoT era, the amount of user data that can be collected will be significantly higher than in the past. For example, recent wearable technologies such as Google Glass, Apple iWatch, Google Fit, Apple Health Kit, and Apple Home Kit can collect sensitive information about users ranging from their health conditions to financial status by observing or recording their daily activities. Note that to succeed in the IoT marketplace, product and service providers must gain consumers' confidence.[10]

Privacy issues in the Internet age have received significant attention over the past few years. For example, allegations of governments spying on their citizens and new laws such as the "right to be forgotten"[11] have opened up a whole range of debate. Compared to the Web era, the IoT is more vulnerable to privacy violations. Therefore, researchers as well as IT professionals will pay more attention to IoT technologies, business models, and potential regulatory efforts to ensure that more secure and privacy-preserving IoT data management techniques are developed.

In a recent survey, TRUSTe highlighted the fact that privacy concerns could be a significant barrier to the IoT's growth.[12] According to the survey, about 60 percent of Internet users have basic privacy awareness about the IoT and know that smart devices, such as smart TVs, fitness devices, and in-car navigation systems, could collect personal activity data. Moreover, 85 percent of Internet users would like to understand more about data collection, and 88 percent of respondents wanted to control the data collected from their smart devices. Finally, the survey revealed that 87 percent of Internet users were concerned about the type of personal information collected.

Trends, Predictions, and Opinions

One of us (Charith Perera) and Arkady Zaslavsky conducted a survey[13] to find out public opinion about the *sensing-as-a-service* model,[5] an IoT business model for data markets. Sensing as a service envisions a marketplace in which contextually enriched sensor data can be exchanged between different parities for financial or social benefits. The survey was conducted among 137 participants in the US. Respondents were asked to assume 100 percent guaranteed privacy and security. Given this, a majority of the responses (64 percent) would be in favor of the trading-based sensing-as-a-service model. In a market environment in which owners of IoT solutions could sell data, 67 percent of respondents said they would expect less than US$500 worth of value returned per year. The survey also revealed that 66 percent of respondents would be happy to make a large initial investment and any additional investments required to support the sensing-as-a-service model, as long as the additional cost could be recovered within three months. Furthermore, the survey also revealed that the sensing-as-a-service model would motivate 65 percent of respondents to purchase smart devices for IoT adaptation, even at higher prices than current market value. In a secondary survey, Perera and Zaslavsky asked 1,000 US participants whether they would like to exchange data for a financial return without explicitly mentioning and assuring user privacy.[13] As expected, 79 percent responded negatively to such an idea.

Fortinet conducted a survey on consumer interest toward the IoT marketplace,[14] focusing on the adaptation of IoT devices by 1,801 homeowners. The survey was administered in Australia, China,

Table 1. Summary of research questions.

Category	Questions
User consent acquisition	How do we present privacy policies and terms to IoT users in a user-friendly and understandable manner?
Control, customization, and freedom of choice	How do we allow users to control and manage their data? How do we ensure interoperability between vendors to assure freedom of choice?
Promise and reality	How do we ensure that service providers will not use data for any other purpose than what users have given permission for?
Anonymity technology	How do we maintain the anonymity of users throughout the different phases of a data life cycle?
Security	How do we protect the data (throughout its life cycle) as well as the infrastructure from external forces with malicious intents?

France, Germany, India, Italy, Malaysia, South Africa, Thailand, the UK, and the US. According to the survey, 61 percent of homeowners agreed that the connected home is "extremely likely" to become a reality in the next five years. At the same time, 68 percent were "extremely" or "somewhat" concerned about the exposure of personal data. Around 57 percent of respondents considered privacy an important issue in the IoT, and they currently don't understand or trust how the data collected through their IoT device would be used. According to Fortinet, 67 percent of respondents consider data privacy to be an extremely sensitive issue. Moreover, 70 percent said that they want to have personal control over the collected data, and 66 percent believe that only they or those to whom they give permission should have access to the data. Almost half of respondents (54 percent) also expected government or nongovernment organizations to regulate data collection and processing in the IoT domain to mitigate privacy issues. As regards a question about the responsibility for vulnerabilities in IoT solutions, respondents seemed to have a divided opinion, with 48 percent believing the device manufacturer was responsible for updating/patching its devices, and 31 percent believing that it was the homeowner's responsibility. Fortinet's survey also found that homeowners were willing to pay for a connected home, with 40 percent responding with "definitely" and another 48 percent with "maybe." It's evident that an innovative business model is required to motivate the 48 percent of the "maybe" group toward investing in IoT solutions. This is where business models such as sensing as a service would come into play.

Privacy Challenges in the IoT

Today, online service consumers are aware that when they use free online services (email, social networking, and news feeds, for example), they automatically become data sources for businesses, which can analyze this data to improve customer satisfaction. Even worse, the data can be sold to third parties for further analysis. However, in the future IoT era, it's likely that service providers will adopt one of the two following models: some consumers might willingly pay to consume services with the aim of protecting their privacy; others might offer to give away data, under some limitations and conditions, in return for consuming services free of charge.

Data collected through smart wearable and smart home devices can be used to generate contextually enriched information.[2] Device owners should remain in charge of such data at all times, even if they give access to their data to external parties temporarily to accomplish a specific task. Consequently, the IoT era poses significant privacy challenges, especially due to the IoT's sheer scale. The EU Commission report on the IoT, *The Cluster of European Research Projects on the Internet of Things*,[10] has identified security and privacy as a major IoT research challenge that encompasses privacy-preserving technology for heterogeneous device sets; models for decentralized authentication and trust; energy-efficient encryption; data-protection technologies; security and trust for cloud computing; data ownership; legal and liability issues; repository data management; access and use rights; rules to share added value; responsibilities; liabilities; artificial immune system solutions for the IoT; secure, low-cost devices; integration with or connection to privacy-preserving frameworks; and privacy policies management.

In the subsequent text, we introduce and discuss some of the major IoT privacy challenges.[15] Table 1 presents a summary of research questions.

User Consent Acquisition

In the IoT, user consent is about acquiring the required level of permission from users and non-users who are affected by devices or services. In the traditional Web, the method of receiving user consent is through privacy terms and policies presented to users via long paragraphs of text. With the emergence of social media and mobile apps, consent-acquiring mechanisms have changed. Researchers have found that the current methods of asking user consent in social media platforms such as Facebook are ineffective, and most users underestimate the authorization given to third-party applications.[8] In some cases, developers might not provide accurate information to users for the consenting decision. In other cases, developers might provide accurate information, but users can't understand exactly what the consent entails due to a lack of technical knowledge. One major privacy challenge in the IoT is to develop technologies that request consent from users in an efficient and effective manner. This is a challenging task because every user has limited time and technical knowledge to engage in the process. Such research will need to combine principles and techniques from human-computer interaction and cognitive sciences.

Control, Customization, and Freedom of Choice

In the IoT, data owners must have full control of data and be able to delete or move data from one service provider to another at any time. Unfortunately, existing IoT solutions in the marketplace provide only limited access to users. Moreover, users should be able to choose hardware devices and software components from different vendors to build their smart environments (for example, a smart home). This gives users full control and freedom of choice. Consequently, users must decide on what kind of data they will share, with what access rights for service providers. Users should also have the ability to withdraw or change previous user consents. It's also important for users to understand that, without having access to some data types, a service provider won't be able to facilitate certain types of services. However, service providers must not unfairly treat consumers, such as by disabling certain features or changing subscription fees to motivate users to provide consent.

Promise and Reality

Each IoT solution promises to offer a select number of functionalities. Service providers achieve this by requiring certain types of raw data to be processed and analyzed. However, with the development of new technologies, businesses might be able to derive more knowledge from user-acquired data. However, if service providers want to use raw data to derive more knowledge, then they must explicitly request permission by explaining the new possibilities and potential consequences to users. The bottom line is that service providers must not use already collected data for any other purpose without explicit user consent. Both regulations and technology must be developed and put in place to avoid such a misuse.

Anonymity Technology

Network communication interfaces typically have media access control (MAC) addresses that can be used to trace data communication paths. Combining multiple devices' MAC addresses will help create unique fingerprints and a unique profile in which analytics can be used to extract knowledge. Consequently, user location can easily be tracked. It's important to discover new technologies that can anonymize data communication paths to protect user privacy. Due to the usage of large numbers of sensors and services, anonymizing multidimensional data is challenging. In particular, it's easy to build fairly unique profiles that might enable knowledge extraction for a specific user. Currently, network communication technologies don't preserve user anonymity. Newer IoT platforms will be required to adopt technologies such as Tor (www.torproject.org), which conceals user location. In essence, a comprehensive anonymization framework is required to facilitate end-to-end anonymity in the IoT. Such a framework must ensure anonymity at different levels, such as data modeling, storage, routing, communication, analytics, and aggregation.

Security

Even though a detailed discussion on IoT security[16] is out of this article's scope, it's important to mention that standardization and certification would be the foundation of security. Moreover, all stakeholders have a responsibility to secure the infrastructure, the data collection and transfer process, and the people using the devices. Device manufactures will need to upgrade or patch firmware and software. Moreover, such updates
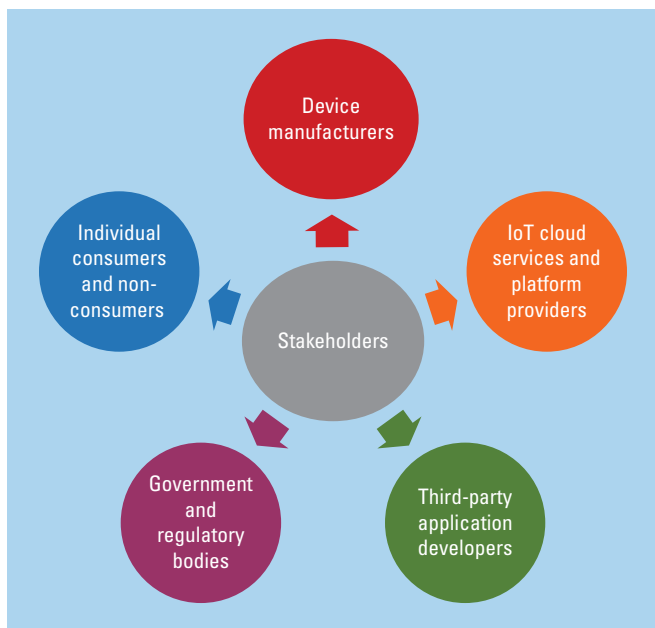
Figure 1. Major stakeholders responsible for protecting user privacy. Protecting user privacy is a responsibility not only of device manufactures, services, and app developers but also of users themselves. Government also has a key role to play in governing standardization processes.

must be pushed onto the devices and automatically installed with minimum user intervention. It might also be owners' responsibility to make sure that their IoT devices and software systems remain up-to-date. Security must be ensured throughout the dataflow within the IoT.

Releasing or selling users' private data could result in them receiving annoying, customized targeted advertising. In more extreme circumstances, criminals could use such data to perform different types of criminal activities that could harm individual consumers (for example, identifying user behavioral patterns to invade houses) or entire communities (identifying critical timeframes to destroy water supplies or energy distribution channels).

Stakeholder Responsibility

As Figure 1 shows, we identify five major stakeholders: device manufacturers, IoT cloud services and platform providers, third-party application developers, government and regulatory bodies, and individual consumers and nonconsumers.[15]

Device manufacturers. Device manufactures must embed privacy-preserving techniques into their devices. Specifically, manufacturers must implement secure storage, data deletion, and

access control mechanisms at the firmware level. Manufacturers must also inform consumers about the types of data their devices collect. Moreover, they must explain what kind of data processing will be employed and how and when data will be extracted from devices. Next, manufacturers must provide the necessary control for consumers to disable any hardware components. For example, in an IoT security solution, consumers might prefer to disable the outside CCTV cameras when inside the home. However, consumers might prefer to keep both inside and outside cameras active when they leave the premises. Finally, device manufacturers might also need to provide programming interfaces for third-party developers to acquire data from the devices.

IoT cloud services and platform providers. It's likely that most IoT solutions will have a cloud-based service that's responsible for providing advanced data analysis support for local software platforms. It's critical that such cloud providers use common standards so that consumers have a choice about which provider to use. Users must be able to seamlessly delete and move data from one provider to another over time. This can be achieved only by following a common set of interfaces and data formats. Most cloud services will also use local software and hardware gateways such as mobile phones that act as intermediate controllers. Such devices can be used to encrypt data locally to improve security and to process and filter data locally to reduce the amount of data sent to the cloud. Such methods will reduce the possibility of user privacy violations that can occur during data transmission.

Third-party application developers. Application developers have a responsibility to certify their apps to ensure that they don't contain any malware. Moreover, it's the developers' responsibility to ensure that they present clear and accurate information to users to acquire explicit user consent. Some critical information includes the tasks that the app performs, the required data to accomplish tasks, what hardware and software sensors are employed, the kind of aggregation and data analysis techniques that the app will employ, and the knowledge that the app will derive via data processing.

Users must be presented with a list of features that the application provides, and what authoriza-

tion they need to give to activate each feature. The control must be given to users to decide which features they want to activate. Moreover, in the IoT, acquiring user consent should be a continuous and ongoing process. Consequently, application developers must continuously let users withdraw, grant, or change their consent. Moreover, users must receive full access to the data the IoT devices collect.

Government and regulatory bodies. Either government or independent regulatory bodies must lead and enforce standardization and legal efforts.[17] Standardization efforts should comprise both a certification process and a technology development process. However, such efforts must not hinder innovation but rather ensure interoperability among different IoT solutions, a fair marketplace, and competition. Standardization of data transfer and storage will reduce entry barriers to the IoT marketplace. For example, some standardization efforts within the IoT domain, such as AllSeen Alliance (https://allseenalliance.org), have attracted several leading industries. It's important to establish a governing body similar to the World Wide Web Consortium for the IoT to oversee standardization and certification processes. Some critical areas for standardization include communication; device descriptions and discovery; data exchange; encryption; user consent mechanisms; and data modeling, storage, and routing. As stated previously, standardization efforts must be complemented with a certification process. Currently, individual companies are attempting to certify devices and apps by themselves. Unfortunately, such efforts will hinder interoperability. The certification mechanism for the IoT would be similar to the certificate authority model that's used for the Internet. However, the IoT certification model would be much broader because it might need to certify both hardware products and software services.

Individual consumers and nonconsumers. Individual stakeholders can be both IoT product consumers and nonconsumers. Most existing IoT solutions are focused mainly on consumers. However, nonconsumers can also be affected by some kinds of IoT solutions. For example, IoT products such as Google Glass pose a threat not only to wearers but also to people within the viewpoint. IoT device owners should be sensitive to similar matters. Moreover, when IoT devices are installed in private homes, office environments, or apartment complexes, it's important to notify nonconsumers regarding the nature of the solutions deployed and related information. This notification would be similar to CCTV surveillance notifications we see in public places today. However, due to the complexity of the monitoring and actuation tasks, it might be necessary to employ interactive and digital means to inform nonconsumers.

State of the Art

The EU-funded OpenIoT project (openiot.eu) is an IoT cloud platform that supports the sensing-as-a-service model. OpenIoT provides instantiations of cloud- and utility-based sensing services, enabling the sensing-as-a-service concept via an adaptive middleware framework for deploying and providing cloud services. However, OpenIoT doesn't adequately address privacy issues. Instead, it promotes the use of public data sources, such as the Linking Open Data project.

Microsoft Research's Lab of Things (LoT) is a flexible platform that uses connected devices in homes.[18] It enables researchers to easily interconnect devices and implement application scenarios, and facilitates the sharing of data, code, and participants, which further lowers the barrier for evaluating ideas in a diverse set of homes. However, the LoT assumes that privacy concerns must be manually handled, with the deployer signing an agreement with data owners.

The Hub of All Things (HAT; hubofallthings. com), funded by the Engineering and Physical Sciences Research Council, is an ongoing project that aims to develop data markets to support trading data generated by IoT solutions in smart home environments. The HAT doesn't address privacy issues. Its primary goal is to provide an API so that smart-home owners can push data to the cloud.

Several industrial efforts to build IoT platforms also exist. Xively (https://xively.com) offers a platform as a service that lets IoT devices connect to the cloud. It doesn't address any privacy issues other than providing secure data storage. In Xively, privacy protection is the responsibility of the person who builds applications and services using the Xively platform.

Datacoup (datacoup.com) is a new startup that will let users sell personal data. Primarily, its focus is on social media data, such as Facebook, Twitter, and

YouTube. Currently, Datacoup doesn't focus on IoT data. Rather, it's among the few initiatives that focus on trading any kind of personal data. Datacoup pays $8 for each user that shares data (www.technologyreview.com/news/524621/sell-your-personal-data-for-8-a-month/). However, users must trust Datacoup completely because it sells user data through its own servers. Mydex (https://mydex.org) is a British social enterprise that helps make it easier and safer for individuals to hold, control, and reuse their personal information in effective and secure ways. Mydex is also a personal data sharing platform. More discussion about the state of the art is presented in the Web extra.

Collecting data through IoT solutions and analyzing them at a large scale offer significant value for both individual users and businesses. Furthermore, this can significantly affect society in general through increased productivity and reduced waste. However, existing technologies and regulations aren't sufficient to support a privacy-guaranteed data management lifecycle. From the time the data is captured by the sensors embedded in IoT solutions to the point at which knowledge is extracted and raw data is permanently and securely deleted, user privacy must be protected and enforced. Only by doing this can IoT solutions gain consumers' confidence. The technology's limitations will need to be mitigated by strict laws and regulations, including serious penalties for offenders and misusers.

Future research efforts will focus on developing novel efficient and scalable privacy-preserving algorithms that scale across IoT data processing technologies (SQL/NoSQL datastores, batch processing systems, and stream processing systems) while adapting to uncertain data sizes and variety. This will be achieved by exploiting the inherent workload and resource performance features of big data processing technology for scaling privacy-preserving algorithms. **IT**

References

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networking*, vol. 54, no. 15, 2010, pp. 2787–2805.
2. C. Perera et al., "Context Aware Computing for the Internet of Things: A Survey," *IEEE Comm. Surveys & Tutorials*, vol. 16, no. 1, 2013, pp. 414–454.
3. A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a Service and Big Data," *Proc. Int'l Conf. Advances in Cloud Computing* (ACC), 2012, pp. 21–29.
4. C. Eaton et al., *Understanding Big Data*, McGraw-Hill, 2012.
5. C. Perera et al., "Sensing as a Service Model for Smart Cities Supported by Internet of Things," *Trans. Emerging Telecommunications Technologies*, vol. 25, no. 1, 2014, pp. 81–93.
6. A. Asin and D. Gascon, "50 Sensor Applications for a Smarter World," white paper, 2012; www.libelium.com/top_50_iot_sensor_applications_ranking/download.
7. C.P. Mayer, "Security and Privacy Challenges in the Internet of Things," *Workshops on Scientific Conf. Communication in Distributed Systems*, 2009; http://journal.ub.tu-berlin.de/eceasst/article/view/208/205/.
8. J. Golbeck and M.L. Mauriello, *User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns*, tech. report HCIL-2014-19, Univ. of Maryland, 2014; http://hcil2.cs.umd.edu/trs/2014-19/2014-19.pdf.
9. D. Miorandi et al., "Internet of Things: Vision, Applications, and Research Challenges," *Ad Hoc Networks*, vol. 10, no. 7, 2012, pp. 1497–1516.
10. H. Sundmaeker et al., "Vision and Challenges for Realizing the Internet of Things," *Cluster of European Research Projects on the Internet of Things*, 2010, www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf.
11. "Proposal for a Regulation of the European Parliament and of the Council," European Commission, 2012; http://ec.europa.eu/digital-agenda/en/news/proposal-regulation-european-parliament-and-council-establishing-connecting-europe-facility.
12. "Internet of Things Industry Brings Data Explosion, but Growth Could Be Impacted by Consumer Privacy Concerns," TRUSTe Research, 29 May 2014; www.truste.com/blog/2014/05/29/internet-of-things-industry-brings-data-explosion-but-growth-could-be-impacted-by-consumer-privacy-concerns.
13. C. Perera and A. Zaslavsky, "Improve the Sustainability of Internet of Things through Trading-Based Value Creation," *Proc. IEEE World Forum on Internet of Things* (WF-IoT), 2014, pp. 135–140.
14. "Fortinet Reveals 'Internet of Things: Connected Home' Survey Results," Fortinet press release, 23 June 2014; www.fortinet.com/press_releases/2014/internet-of-things.html.
15. "Opinion 8/2014 on the Recent Developments on the Internet of Things," European Commission, Article 29 Data Protection Working Party, 2014.
16. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, 2011, pp. 51–58.

17. R.H. Weber, "Internet of Things—Need for a New Legal Environment?" *Computer Law & Security Rev.*, vol. 25, no. 6, 2009, pp. 522–527.
18. A.B. Brush et al., "Lab of Things: A Platform for Conducting Studies with Connected Devices in Multiple Homes," *Proc. 2013 ACM Conf. Pervasive and Ubiquitous Computing*, 2013, pp. 35–38.

Charith Perera *is a research associate at The Open University. His research interests include the Internet of Things, smart cities, mobile and pervasive computing, context-awareness, and ubiquitous computing. Perera worked at the Information Engineering Laboratory, ICT Center, Commonwealth Scientific and Industrial Research Organization (CSIRO), and was involved in the OpenIoT project (FP7-ICT-2011.1.3). He received a PhD in computer science from the Australian National University. Contact him at charith.perera@ieee.org.*

Rajiv Ranjan *is a senior researcher and Julius fellow at CSIRO, Australia. He's conducted leading research in two key areas: cloud and big data computing, where he is developing techniques for quality-of-service-based management and processing of multimedia and big data analytics applications across multiple cloud datacenters; and automated decision support for migrating applications to datacenters. Ranjan has published more than 120 scientific papers, and serves on the editorial boards of* IEEE Transactions on Computers, IEEE Transactions on Cloud Computing, IEEE Cloud Computing, *and* Future Generation Computer Systems. *Contact him at raj.ranjan@csiro.au.*

Lizhe Wang *is a professor at the Institute of Remote Sensing & Digital Earth, Chinese Academy of Sciences (CAS), and a ChuTian Chair Professor at the School of Computer Science, China University of Geosciences (CUG). His research interests include digital Earth, high-performance geocomputing, and spatial information processing. Wang leads a group on spatial data processing at CAS and also leads the high-performance computing lab at CUG, and has published roughly 170 papers. He's a fellow of IET and the British Computer Society, and a senior member of IEEE. Contact him at wanglz@radi.ac.cn.*

Samee U. Khan *is an associate professor of electrical and computer engineering at North Dakota State University. His research interests include optimization, robustness, and the security of cloud, grid, cluster, and big data computing, social networks, wired and wireless networks, power systems, smart grids, and optical networks. His work has appeared in more than 250 publications. He's on the editorial boards of* IEEE Transactions on Computers, IEEE Access, *IEEE Cloud Computing, IEEE Communications Surveys & Tutorials, Scalable Computing, Cluster Computing, Security and Communication Networks, and the* International Journal of Communication Systems. *Contact him at samee.khan@ndsu.edu.*

Albert Y. Zomaya *is the Chair Professor of High Performance Computing & Networking in the School of Information Technologies, University of Sydney, and the director of the Centre for Distributed and High Performance Computing. His research interests include cloud computing, complex systems, datacenters, green computing, and parallel and distributed computing. Zomaya is the author/coauthor of seven books and more than 450 papers, and the editor of 14 books and 20 conference proceedings. He's the recipient of the IEEE TCPP Outstanding Service Award and the IEEE TCSC Medal for Excellence in Scalable Computing. Contact him at albert.zomaya@sydney.edu.au.*

cn **Selected CS articles and columns are available for free at http://ComputingNow.computer.org.**