Requirements for Security, Privacy, and Trust in the Internet of Things

Sabah Mohammed | Lakehead University
Tai-hoon Kim | Beijing Jiaotong University
Wai Chi Fang | National Chiao Tung University

The Internet of Things (IoT) has huge potential to push monitoring, computing, and communication deeply into the home, the workplace, medicine, manufacturing, and critical infrastructure. This increased capability offers the hope that urban settings can be transformed in various ways through the innovative deployment of IoT devices. Driven by a decline in the cost of sensors, many cities have adapted a plan to transition services toward being a fully smart city by implementing real-time data-driven management services across urban systems, including efficiently managing water, energy, waste, policing, and transportation among other citywide services. Cities continue to attract new people and the United Nations (UN) estimates that by 2030, more than 60% of the global population will live in large cities.[1] With nearly 38 million people, Tokyo tops the UN's ranking of most populous cities, followed by Delhi, Shanghai, Mexico City, São Paulo, and Mumbai.

The consequences and challenges for such a vast increase in population on the city resources and services are more than obvious. Because urbanization and digital developments must reinforce each other in any smart city plan, a huge amount of data will need to be shared, stored, and analyzed. Municipalities can use data to develop policies that make a city more efficient and sustainable as well as to make living in such cities as comfortable as possible. On the other hand, smart cities will run into several security and privacy problems if no proper safeguards are put into place. Figure 1 illustrates some of the possible security and privacy attacks on smart cities. The complexity of the smart city landscape has led many city governments and researchers to develop and adopt countermeasures to confront several of these attacks.[2]

In This Issue

The response to this theme issue's call for papers was substantial—22 papers were submitted—and a rigorous review process led to the selection of the four articles chosen for inclusion in this issue of *IEEE Security & Privacy* (four or five other submissions remain in the revise-and-review process and may appear in later issues as regular feature articles).

The four articles together give a sense of the breadth of technology issues with smart cities. "Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions" focuses on the intersection of this emerging technology, with societal expectations that data and behavior will be confidential and private. The article highlights a number of research projects within the European Union that address the challenges of meeting those expectations. "Security for Shared Electric and Automated Mobility Services in Smart Cities" recognizes the huge impact the IoT will have on transportation and the attendant cybersecurity challenges. Who among us will blithely use a self-driving vehicle if we perceive that our safety is at risk due to cyberinterference? This article considers a number of likely services enabled by the IoT and the security risks that attend them.

Digital Object Identifier 10.1109/MSEC.2020.3037624
Date of current version: 25 January 2021

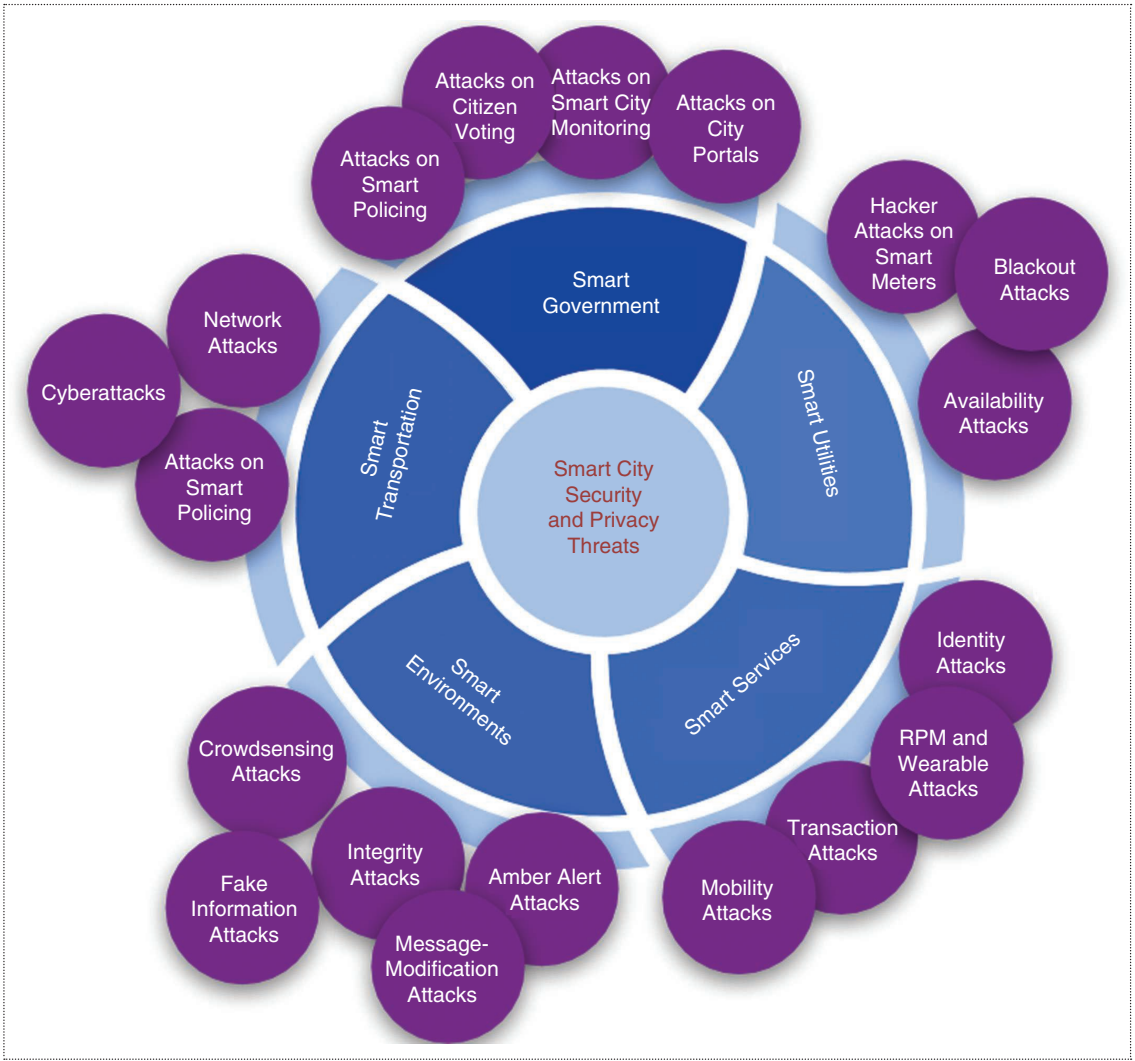

Figure 1. Smart city security and privacy attacks. RPM: remote patient monitoring.

Another article, "Privacy Regulations, Smart Roads, Blockchain, and Liability Insurance: Putting Technologies to Work," zeros in on the privacy issues that IoT-augmented road travel brings up, particularly in the context of European General Data Protection Regulation requirements. It discusses the role of insurance and insurance companies in managing information use and privacy protection. Finally, "A Self-Healing Mechanism for Internet of Things Devices" considers the probability that smart city infrastructure will have to automatically defend itself against cyberattack and discusses "self-healing" means designed to allow the infrastructure to detect, react, and recover from such attacks.

We thank the authors who submitted articles to this issue, the reviewers who helped guide us with our final selections, and the *IEEE Security & Privacy* editors—especially Associate Editor in Chief Terry Benzel—for their guidance and support during the process. ■

References

1. "World's population increasingly urban with more than half living in urban areas," United Nations, New York, July 10, 2014. [Online]. Available: http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html
2. T-h Kim, C. Ramos, and S. Mohammed, "Smart city and IoT," *Future Gener. Comput. Syst.*, vol. 76, pp. 159–162, Nov. 2017. doi: 10.1016/j.future.2017.03.034.

Sabah Mohammed is a full professor in the Department of Computer Science at Lakehead University,

Thunder Bay, Ontario, P7A 8A1, Canada, where he is also a core professor in the BioTechnology program. His research interests include intelligent systems that must operate in large, nondeterministic, cooperative, highly connected, survivable, adaptive, or partially known domains. Mohammed received a Ph.D. in computer science from Brunel University. He is the editor in chief of *International Journal of Extreme Automation and Connectivity in Healthcare* as well as the supervisor of the Smart Health FabLab at Lakehead University. He is currently the chair of the Smart and Connected Health special-interest group with the IEEE Communications Society e-Health Technical Committee. He is also a member of Professional Engineers Ontario and an information processing professional with the Canadian Information Processing Society. He is a Senior Member of IEEE. Contact him at mohammed@lakeheadu.ca.

Tai-hoon Kim is a professor at Beijing Jiaotong University, Beijing, 100044, China, and a visiting scholar of the University of Tasmania, Hobart, 7005, Australia. His research interests include biometric authentication, pattern recognition, security, and medical imaging. Kim has received two Ph.D.s: one in electrics, electronics, and computer engineering from Sungkyunkwan University, Korea; and another in computer engineering from Bristol University, United Kingdom. He serves as a vice-chair of the Science & Engineering Research Support soCiety (SERSC). He has served as either a general chair or a program committee chair for more than 20 international conferences. He is a Member of IEEE, the Association for Computing Machinery, Korea Institute of Industrial Technology, and SERSC. Contact him at taihoonn@daum.net.

Wai-Chi Fang is the Taiwan Semiconductor Manufacturing Company Distinguished Chair Professor with the Institute of Electronics, National Chiao Tung University, Hsinchu, 300 ROC, Taiwan. His current research interests include Internet of Things security, artificial intelligent systems, biomedical circuits and systems, very large-scale integration neural networks, high-performance computing and networking systems, smart sensor networks, and advanced space avionics. Fang received a Ph.D. from the Electrical Engineering Department of the University of Southern California, Los Angeles. From 1985 to 2009, he was with NASA's Jet Propulsion Laboratory, Pasadena, California. He has authored more than 200 referred technical papers. He holds 20 patents and 13 NASA new technologies. He was a recipient of the 1995 IEEE VLSI Transactions Best Paper Award. He received two NASA Space Act Awards in 2002 and 2003. He was a member of the Board of Governors of the IEEE Circuits and Systems Society from 2004 to 2009. He also served as the vice president for the IEEE Systems Council from 2008 to 2010. He was the general chair of the 2012 International Conference on Biomedical Circuits and Systems, Taiwan. He is a Fellow of IEEE and an international leader in professional activities. Contact him at wfang@mail.nctu.edu.tw.

Message from *IEEE S&P*'s Outgoing Editor in Chief

The masthead in this issue of *IEEE Security & Privacy* lists Sean Peisert as editor in chief (EIC), as he assumed that role at the beginning of January, and the date on the cover is January/February 2021. He lays out his aspirations for the magazine in his debut "From the Editors" column and chronicles his long and impressive history with the magazine. That said, this issue was conceived, organized, and laid out as my last one as EIC.

During my tenure, *IEEE Security & Privacy* has won two awards, the APEX 2020 Award for Publication Excellence and an honorable mention at the 2020 Folio Eddie and Ozzie Awards, in recognition of the high quality of a particular theme issue. Although the board of *IEEE Security & Privacy* associate EICs surveys the landscape and recruits articles for particular themes, the awards were for the November/December 2019 issue, "GDPR at Year One: Enter the Designers and Engineers," which, like this one, was proposed and managed by members of the readership and supported by the magazine's staff and the IEEE Computer Society. The volunteer editorial staff comes and goes, but this approach persists and works. It's been an honor to serve in the EIC role for the past three years, and I'm grateful for all the help I received at every step along the way. I am confident that I leave the helm of this magazine in good hands.—*David M. Nicol*

Digital Object Identifier 10.1109/MSEC.2020.3037626
Date of current version: 25 January 2021