Privacy, data Assurance, Security Solutions for Internet of Things (PASS4IoT): Guest Editorial

Shancang Li, Lida Xu, Houbing Song, and Tom Chen

The emerging Internet of Things (IoT) is unleashing the next wave of innovations due to its inherent capability of connecting billions of devices together, which bridges the gap between the physical world and cyber world. In recent years, the successful applications of IoT have demonstrated the massive potential benefits that IoT can make for global social economy. Coming along with the benefits, the IoT is facing an increasingly number of security and privacy challenges, including data encryption, privacy, secure machine-to-machine (M2M) communications, device security, cyber-attack, cloud security in IoT environment, and more. These challenges must be fixed quickly and effectively. To address these challenges, this special issue was proposed to bring recent research progress in theories and applications in privacy, data assurance, security issues in IoT that may help put together a clear picture for the security of IoT.

Recently, a large number of security and privacy preserving solutions and techniques have been proposed to develop a secure and safe IoT environment. For example, lightweight cryptographic, energy-efficient, privacy-preserving communication protocols, symmetric encrypted data transmissions, secret keys generation and distribution, etc. In data assurance, secure one-time password algorithm, holistic security architecture, LASeR (lightweight authentication and secured routing), and resource-limited privacy assurance, such as data assurance, access control, data validation, big data prediction systems, etc.

In this special issue, more than 20 research manuscripts were submitted and finally, after a thorough peer-review, seven papers were selected for publication. The first paper entitled "Routing protocol for battery management system of electric vehicles based on ad-hoc network", authored by Jiajia Song, Jinbo Zhang, and Xinnan Fan, brings a secure routing protocol solution over resource constrained IoT networks, in which a new secure routing protocol is proposed based on the ad-hoc on-demand distance vector junior (AODVjr). The second paper, entitled "Efficient aggregation technique for data privacy in wireless sensor networks", authored by Manjula Raja and Raja Datta, offers an efficient aggregation technique for data privacy over resource constrained environment in IoT, such as wireless sensor networks, etc. The aggregation algorithm bridges data privacy, communication overhead, and reliability metric to gauge the performance of proposed solution. The third paper, "Secured cloud computing for medical data based on watermarking and encryption", authored by Mohamed Boussif, Noureddine Aloui, and Adnene Cherif, is a contribution on hardware implementation of local cloud for storing, sharing, and archiving data in healthcare systems, including health report, medical image, etc. In this work, a cloud-based data encryption solution is developed for the healthcare systems. The fourth paper, entitled "Potential threats mining methods based on correlation analysis of multi-type logs", by Tao Qin, Yuli gao, Lingyan Wei, Zhaoli Liu, and Chenxu Wang, introduces a potential threats mining technique using multi-type log analysis, which involves behaviour analysis, attribute extraction, and measure of features from multi-type logs based on the characteristics of known and potential attacks. Meanwhile, a normalization method is proposed to deal with these heterogeneous features. The fifth paper is "Adaptive timing model for improving routing and data aggregation in Internet of things networks using RPL", by Ainaz Bahramlou and Reza Javidan. In this paper, the authors proposed a data aggregation method for routing protocol for low power and lossy network (RPL) in the IoT environment. The proposed method is able to construct a network graph along the path to the sink node and a novel metric is proposed to determine the degree of the environmental changes. The sixth paper entitled “Six-face cubical key encryption and decryption based on product cipher using hybridisation and Rubik's cubes”, authored by Rajavel Dhandabani, Shantharajah S. Periyasamy, Padma Theagarajan, and Arun Kumar Sangaiah, introduces a novel approach to generate cubical key that symbolises message and key in six-face cubical structure. In the proposed approach, the cubical message is hybridised to generate the cipher in the encryption, and hybridisation of cubes is performed using XOR operation to the six-face cubical original message, in which six-face random sequence is used to guarantee the randomness in each phase of hybridization. The final paper, entitled “Evolution of ransomware”, by Philip O'Kane, Sakir Sezer, Domhnall Carlin, reviews the evolution of ransomware in IoT environment. This paper explores the transition from the early-day scams to extortion implemented by current ransomware by analysing the pathway from the first clumsy ransomware attempts to the present day sophisticated ransomware attack campaigns.

Finally, we would like to express our gratitude to all authors for sharing their recent exciting research efforts. We also thank all anonymous reviewers for their timely reviews of all papers and valuable comments. We extend our sincere thanks to the editor-of-chief and all members in the editorial group for their assistances in this work.

Shancang Li,
Department of Computer Science, University of the West of England, Bristol BS16 1QY, UK.
(Email: Shancang.li@uwe.ac.uk)

Dr Shancang Li received the B.Sc. and M.Sc. degrees in mechanics engineering and the Ph.D. degree in computer science from Xi’an Jiaotong University, Xi’an, China, in 2001, 2004, and 2008, respectively.

He is currently a senior lecturer with department of computer science and creative technologies at University of the West of England, Bristol, UK. His current research interests include digital forensics for emerging technologies, cyber security, IoT security, data privacy-preserving, Internet of Things, Blockchain technology, and the lightweight cryptography in resource constrained devices. He has authored over 60 papers published in high profile journals and conferences. Dr. Li is the Associate Editor of IEEE Access and Journal of Industrial Information Integration. He is a member of the British Computer Society.

Lida Xu,
Department of Information Technology, Old Dominion University, Norfolk, USA.
(Email: lxu@odu.edu)

Li Da Xu (M’86-SM’11-F’16) received the B.S. degree in information science from University of Science and Technology of China, in 1978, M.S. degree in information science from University of Science and Technology of China, in 1981, and Ph.D. degree in systems science and engineering from Portland State University, USA, in 1986. He is an IEEE Fellow, academician of the European Academy of Sciences, and academician of the Russian Academy of Engineering (formerly USSR Academy of Engineering). Dr.

Xu is a 2016 and 2017 Highly Cited Researcher in the field of engineering named by Clarivate Analytics (formerly Thomson Reuters Intellectual Property & Science).

Houbing Song, Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, USA.
(Email: Houbing.Song@erau.edu)

Houbing Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012.In August 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He served on the faculty of West Virginia University from August 2012 to August 2017. In 2007 he was an Engineering Research Associate with the Texas A&M Transportation Institute. He serves as an Associate Technical Editor for IEEE Communications Magazine. He is the editor of four books, including Smart Cities: Foundations, Principles and Applications, Hoboken, NJ: Wiley, 2017, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Chichester, UK: Wiley-IEEE Press, 2017, Cyber-Physical Systems: Foundations, Principles and Applications, Boston, MA: Academic Press, 2016, and Industrial Internet of Things: Cybermanufacturing Systems, Cham, Switzerland: Springer, 2016. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, internet of things, edge computing, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. Dr. Song is a senior member of ACM. Dr. Song was a recipient of the prestigious Air Force Research Laboratory's Information Directorate (AFRL/RI) Summer Faculty Research Fellowship in 2018, and the very first recipient of the Golden Bear Scholar Award, the highest campus-wide recognition for research excellence at West Virginia University Institute of Technology (WVU Tech), in 2016.

Tom Chen, School of Mathematics, computer science & engineering, City University of London, London, UK.
(Email: tom.chen.1@city.ac.uk)

Thomas Chen is a Professor in Cyber Security at City, University of London. Previously, he was a Professor in Networks at Swansea University, associate professor at Southern Methodist University, Texas, and senior member of technical staff at GTE Labs (now Verizon). He was formerly editor-in-chief of IEEE Communications Magazine, IEEE Network, and IEEE Communications Surveys. His research interest is network security.