Editorial for Special Issue on Security, Privacy and Trust Management on Decentralized Systems and Networks

With the rapid growth of size and scale in current organization, decentralize systems are becoming dominant, which is an interconnected information system where no single entity or central server is employed as a sole authority, such as Internet of Things (IoT), smart home system, smart city system and more. For such systems, sensors are important to gather and process data as the lower-level components. However, with the distributed deployment, decentralized systems are facing various security, privacy and trust issues. For instance, any compromised sensor may leak sensitive data or be used to infect other entities within the system. It is also a long-term challenge to establish trust among different nodes, and defeat malicious insiders. Here there is a requirement to develop suitable management schemes for decentralized systems and networks regarding security, privacy and trust. This special issue focuses on the identification of security, privacy and trust issues in decentralized systems, and the development of effective solutions in handling security, privacy and trust issues for decentralized systems, e.g., IoT, cyber-physical systems (CPS), smart city, smart home.

In the first contribution entitled “A security-enhanced equipment predictive maintenance solution for the ETO manufacturing”, Cao et al. proposed a security-enhanced predictive maintenance scheme specifically designed for ETO-type production equipment. This scheme can use the industrial Internet of Things (IIoT) technology to monitor machines and equipment, constructing prediction models using machine learning methods, and reinforcing the security of the prediction system through adoption of a decentralized architecture with blockchain distributed storage. In this experiment, six supervised learning models were compared, and it was found that the model based on the random forest algorithm achieved an outstanding accuracy rate of 98.88%.

In the second contribution entitled “IGXSS: XSS payload detection model based on inductive GCN”, Wang et al. figured out that XSS is one of the most common web application attacks, in which an attacker can obtain private user information from IoT devices or cloud platforms. To address this issue, the authors proposed an XSS payload detection model based on inductive graph neural networks, shortly IGXSS (XSS payload detection model based on inductive GCN). The method aims to detect XSS payloads under an IoT environment by segmenting the samples as nodes and obtaining the feature matrix of nodes and edges.

In the third contribution entitled “Privacy-protected object detection through trustworthy image fusion”, Zhang et al. identified that user privacy may be leaked as infrared images may contain sensitive information. The authors then proposed a procedure for enhancing the database privacy--object detection based on multi-band infrared image datasets, and they utilized the transfer learning technique to migrate knowledge learned from external infrared data to internal infrared data. The proposed approach consists of several steps including data preprocessing of multi-band infrared images, multi-band infrared image fusion, and object detection. They found that transfer learning is very beneficial for keeping the privacy of multi-band infrared images during the fusion and detection processes.

In the fourth contribution entitled “ASMTP: Anonymous secure messaging token-based protocol assisted data security in swarm of unmanned aerial vehicles”, Manikandan and Sriramulu argued that there is a need for perfect forward secrecy and non-repudiation during UAV-to-UAV (Unmanned Aerial Vehicles) communication. The authors proposed a protocol for UAV Swarm communication with anonymous secure messaging token-based protocol (ASMTP). Such protocol can help secure UAV-to-base station communication and safeguard the metadata of the sender and receiver nodes.

In the fifth contribution entitled “Privacy-preserving data aggregation achieving completeness of data queries in smart grid”, Li et al. identified that privacy and security should be the priority in smart grid systems. The authors proposed a privacy-preserving data aggregation scheme that aims to support data query. They also developed a multi-level data aggregation mechanism based on Paillier semi-homomorphic encryption, in order to reach efficient aggregation of user data in the control center. They used a data query mechanism based on electricity consumption intervals to enable the control center to query aggregated ciphertexts for different users.

In the sixth contribution entitled “A secure and light-weight patient survival prediction in Internet of Medical Things framework”, Mittal et al. aimed to explore the interplay of objective and subjective data in predicting postoperative outcomes and use this to help reduce data transmission costs in the Internet of Medical Things. Based on open dataset, they found that ensemble learning classifiers is superior when adopting all features, resulting in an accuracy rate of 0.92. In addition, when integrating select subjective features, a comparable accuracy rate of 0.91 can be reached.

In the seventh contribution entitled “Risk-Aware SDN Defense Framework Against Anti-Honeypot Attacks Using Safe Reinforcement Learning”, Gao et al. figured out that the network interaction between SDN servers and users is under risk. The authors proposed a risk-aware SDN defense framework based on safe reinforcement learning that can help mitigate the external attacks. The authors also introduced a risk level function to model the simultaneous dynamic attack and defense processes. Their simulation results showed that the proposed framework could enhance the defense utility by 17.5% and 142.4% compared with the QLearning scheme and the Random scheme.

On the whole, the special issue papers cover a broad range of research on security, privacy and trust on decentralized systems and network, and discuss many potential threats and promising solutions. The team of guest editors would like to thank Editor-in-Chief James Won-Ki Hong for their great support, as well as the paper authors and the reviewers for their contributions.

Weizhi Meng[1]

Sokratis K. Katsikas [2]

Jiageng Chen[3]

Chao Chen[4]

[1]Lancaster University, United Kingdom

[2] Norwegian University of Science and Technology, Norway

[3] Huazhong University of Science and Technology, China

[4]RMIT University, Australia

Correspondence

Weizhi Meng, Lancaster University, United Kingdom

Email: w.meng3@lancaster.ac.uk

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Bio information.

Dr. Weizhi Meng is a Full Professor in the School of Computing and Communications, Lancaster University, United Kingdom, and an adjunct faculty in the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong. He was a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. He also received the IEEE ComSoc Best Young Researcher Award for Europe, Middle East, & Africa Region (EMEA) in 2020 and the IEEE ComSoc Communications & Information Security (CISTC) Early Career Award in 2023. His primary research interests are blockchain technology, cyber security and artificial intelligence in security including intrusion detection, blockchain applications, smartphone security, biometric authentication, and IoT security. He serves as associate editors / editorial board members for many reputed journals such as IEEE TDSC and IEEE TIFS. He is an ACM Distinguished Speaker.

Sokratis K. Katsikas is the Director of the Norwegian Center for Cybersecurity in Critical Sectors and Professor with the Dept. of Information Security and Communication Technology of the Norwegian University of Science and Technology (NTNU). His research activity has resulted in more than 300 published books; book chapters; journal papers; and papers in conference proceedings. He has led or participated in more than 60 funded national and international R&D projects.

Jiageng Chen received his B.S. degree from the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST) in 2004 and received his M.S. and Ph.D.

of computer science from the School of Information Science, Japan Advanced Institute of Science and Technology (JAIST) in 2007 and 2012, respectively. He was working as an Assistant Professor in School of Information Science, Japan Advanced Institute of Science and Technology from 2012 to 2015. And currently, he is an Associate Professor at the School of Computer, Central China Normal University. He is the Associate Editor of Journal of Information Security and Application, and he has served as a guest editor for several International Journals such as the “Future Generation Computer Systems” and “Wireless Communications and Mobile Computing”, “IEICE”, “Security and Communication Networks”and so on. His research areas include cryptography, especially in the areas of Cryptographic protocols, algorithms, cryptanalysis, data analysis, fast implementations and so on.

Chao Chen is currently a Senior Lecturer in RMIT University, Australia. He received his PhD degree in Information Technology from Deakin University in 2017. From 2016 to 2018, he worked as a Data Scientist at Telstra to create customer value from huge and heterogeneous data sources using advanced analytics and big data techniques. He then worked at Swinburne University of Technology as a Research Scientist from 2018 to 2020. He is conducting interdisciplinary research between cybersecurity and artificial intelligence (AI), such as AI for cybersecurity and security issues in AI models. He has published more than 30 research papers in refereed international journals and conferences, such as IEEE Transactions on Information Forensics and Security (TIFS), Privacy Enhancing Technologies Symposium (PETS) and ACM Asia Conference on Computer & Communications Security (ASIACCS). One of his papers was the featured article of that issue (IT Professional Mar.-Apr. 2016).