Introduction to the Special Section on Human-centered Security, Privacy, and Trust in the Internet of Things

The Internet of Things (IoT) is enabling applications that touch almost all aspects of our lives. Example application domains include smart healthcare environments, home automation, efficient transportation networks, and smart cities. However, while such applications and IoT systems promise to ease our lives, they also raise major security and privacy concerns for their users. The risks of privacy violation, data misuse, real-time surveillance, and intrusions by malicious attackers, as well as a lack of transparency, hinder the wider adoption of those new technologies and systems.

To increase the trust of users in IoT applications and systems, and thereby pave the way for increased adoption, security and privacy protection solutions should provide more support for, and involvement of, users in the protection of their data and privacy, i.e., users should be supported in understanding how their data is collected, processed, analyzed, stored, accessed, and kept safe. They should also be able to exert their fundamental rights (as specified in applicable data protection laws, e.g., GDPR and CCPA) to control what is collected about them, when and where and for what purposes collected data can be exploited, and the right to be forgotten. Users should also be provided with a transparent view into the system to verify, at any point in time, how their data is processed and exploited.

IN THIS SPECIAL ISSUE

This special issue sought to collect recent advances, innovations, and practices in software and data engineering for building security and privacy protection systems and for developing techniques and solutions that provide effective involvement of users and increase their trust in IoT technologies. A total of 10 submissions were accepted from 51 submitted articles.

The article by Sharma, Dyer, and Bashir, titled "Enabling User-centered Privacy Controls for Mobile Applications: COVID-19 Perspective," explored the privacy and security concerns raised by the use of mobile tracing applications, such as the ones used to contain the spread of COVID-19. The article presented an interesting empirical study involving 1,550 users of COVID-19 tracking apps. The study analyzed the privacy and security concerns of those users and identified a set of measures and guidelines that can be exploited by the developers of mobile tracking applications to address the identified concerns.

The article by Mehta, Gooch, Bandara, Price, and Nuseibeh, "Privacy Care: A Tangible Interaction Framework for Privacy Management," explores the interactional challenges that users face when trying to manage their privacy dynamically in everyday UbiComp contexts. Focusing on the user experience, the authors propose using more tangible and embodied style interactions

ACM Reference format:
Mahmoud Barhamgi, Michael N. Huhns, Charith Perera, and Pinar Yolum. 2021. Introduction to the Special Section on Human-centered Security, Privacy, and Trust in the Internet of Things. *ACM Trans. Internet Technol.* 21, 1, Article 16 (January 2021), 3 pages.
https://doi.org/10.1145/3445790

1533-5399/2021/01-ART16
https://doi.org/10.1145/3445790

and present the Privacy Care interaction framework. The framework is rooted in the literature of privacy and tangible computing and promises the provision of an embodied experience that is *Direct, Ready-to-Hand*, and *Contextual* for effectively raising *Awareness* and empowering users with seamless *Control*. The framework provides conceptual guidance on a set of dimensions that interaction designers should follow when designing for effective and seamlessly natural privacy management. The resulting design concepts could then guide software engineers on the functionalities to develop and assist hardware engineers to think about the form-factors and modalities that are desirable.

The article by Can and Ersoy, "Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring," addressed the problem of analyzing biomedical data collected by wearable IoT objects while protecting the privacy of users. This problem is especially important in the healthcare application domain, where collected data could reveal privacy-sensitive information about the users, such as their diseases, sexual lives, and locations. The authors proposed a solution that exploits federated deep learning techniques. The solution transfers local models instead of IoT collected data to a centralized server to preserve the privacy of users, while achieving the same learning outcomes.

The article by Yan, Peng, Feng, and Yang, titled "Social-Chain: Decentralized Trust Evaluation Based on Blockchain in Pervasive Social Networking," addresses the problem of trust evaluation among interacting participants in pervasive social networks (PSNs). This problem is quite challenging due to the dynamic topology of pervasive social networks. The authors proposed Social-Chain, a decentralized trust evaluation system in PSN by leveraging blockchain. They designed a lightweight consensus mechanism, Proof-of-Trust, by embedding trust evaluation and verification according to human social behaviors into block generation and selection. The security properties of the solution were thoroughly analyzed, and the efficacy, effectiveness, and efficiency of the solution were demonstrated through a set of experiments.

The article by Chicha, Al Bouna, Nassar, Chbeir, Haraty, Oussalah, Benslimane, and Alraja, titled "A User-centric Mechanism for Sequentially Releasing Graph Datasets under Blowfish Privacy," addressed the problem of anonymizing user interaction graphs that could be generated by IoT systems. The proposed solution is built using a Blowfish Privacy (BP) mechanism and significantly allows data owners to fine-tune the anonymization degree to strike the right balance between data privacy and utility. Conducted experiments showcased the efficacy of the proposed solution.

The article by Peng, Chen, Vijayakumar, Kumar, and He, titled "Efficient Distributed Decryption Scheme for IoT Gateway-based Applications," addressed the problem of securing data transmission between IoT objects and applications in gateway-based IoT architectures. Specifically, the authors proposed a secure and end-to-end data encryption scheme that has the particularity of supporting multiple IoT applications. That is, the scheme allows an untrusted IoT platform to distribute the data transmitted by IoT objects to several applications based on their data access rights without decrypting the data. The security of the proposed scheme was thoroughly evaluated and its performance and efficiency were demonstrated based on a good set of experiments.

The article by Hu, Li, Liu, and Sun, titled "DuroNet: A Dual-robust Enhanced Spatial-temporal Learning Network for Urban Crime Prediction," addressed the problem of crime predication in monitored urban spaces. Specifically, the authors proposed a machine learning–based model that can remove the noise effects in collected time series of urban crime data. Conducted experiments demonstrated the efficacy of the proposed model relative to existing solutions.

The article by Loukil, Ghedira, Boukadi, Benharakat, and Benkhelifa, "Data Privacy Based on IoT Device Behavior Control Using Blockchain," describes a solution for allowing the users of IoT systems to control their own IoT devices and detect the compromised ones. The solution is built

using blockchain technologies and involves the use of smart contracts to control communications among IoT devices and ensure their compliance with the privacy preferences of users.

The article by Singh, Thakur, Jolfaei, Srivastava, Elhoseny, and Mohan, titled "Joint Encryption and Compression–based Watermarking Technique for Security of Digital Documents," investigates the problem of securing the exchange of digital contents over the Internet and IoT networks. The authors proposed an encryption solution that exploits the techniques of watermarking and compression and can be applied to various content types, including text, image, audio, and videos. The performance and the efficacy of the solution were demonstrated with a good set of experiments and compared with existing solutions to showcase its superiority.

The article by Hourany, Habib, Fountaine, Makhoul, Piranda, and Bourgeois, titled "PROLISEAN: A New Security Protocol for Programmable Matter," proposed a new lightweight security protocol suitable for low resources programmable matter. It is composed of two parts: authentication and encryption. The aim of the protocol is to create a hashing function based on an encryption algorithm and a block code already embedded in the devices. An empirical analysis and simulations are presented to showcase the efficiency and the security properties of the method.

Mahmoud Barhamgi
Michael N. Huhns
Charith Perera
Pinar Yolum

Guest Editors