Future Generation Computer Systems 78 (2018) 931–932

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Editorial

Internet of Things: Security and privacy in a connected world

Internet of Things (IoT) adopts novel processing, communication architecture, smart technologies and management strategies to seamlessly integrate a large number of smart objects with the Internet. IoT provides a platform to collect and process data via wireless sensor network. As a result, IoT could jointly use peer to peer systems, cloud computing, big data and related technologies to provide computational capability, as an emerging paradigm for the 21st century. There are benefits offered by IoT for the environment, society and economy due to interconnection and cooperation of smart objects, including the wide adoption of mobile services on cloud and fog computing.

However, this new paradigm brings many security and privacy challenges involved with authentication and authorization, data and personal information confidentiality, and secure communication and computation. Hence, investigating and understanding how to address these security and privacy challenges will provide fundamental development in science and technology for achieving widely adopted yet secure and affordable IoT and mobile cloud computing. In the recent literature and news reported globally, there are malicious attacks and security breach such as privacy intrusion, data manipulation, unauthorized access, mobile phone hacking and sophisticated infection of viruses. This motivates us to develop a special issue seeking high quality of papers demonstrating real solutions, proofs-of-concept and recommendation to enforce the importance of security and privacy for IoT.

Following a rigorous and organized review process, we are pleased to present eleven papers dealing with advanced research and technology on the security and privacy in IoT. Authors of our selected papers addressed the security and privacy issues in IoT and presented solutions for these problems.

In the paper entitled "Modeling and Inferring Mobile Phone Users' Negative Emotion Spreading in Social Networks" [1], Du et al. aim to investigate the negative emotion spreading mechanism at the individual level of large user groups in the long term, and finally infer individuals' ability of the negative emotion spreading by observing people's behaviors on mobile social networking. To protect the privacy of the users of VANETs, in the paper entitled "Computationally Efficient Privacy Preserving Anonymous Mutual and Batch Authentication Schemes for Vehicular Ad Hoc Networks" [2], proposal from Vijayakumar et al. can demonstrate a computationally efficient privacy preserving anonymous authentication scheme. Technologies are based on the use of anonymous certificates and signatures for VANETs as a crucial component of Internet of Things (IoT) and the development of smart cities.

Lightweight authentication protocol is an important issue in IoT. In the paper "A Light Weight Authentication Protocol for IoT-enabled Devices in Distributed Cloud Computing Environment" [3], Amin et al. propose an architecture which is applicable for distributed cloud environment, and an authentication protocol using smartcard based on it, where the registered user can access all private information securely from all the private cloud servers. It is well known that there is a rapid development of both Cloud Computing and IoT. In the paper "Secure integration of IoT and Cloud Computing" [4], Stergiou et al. present a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. The paper entitled "Selective Disclosure and Yoking-proof Based Privacy-Preserving Authentication Scheme for Cloud Assisted Wearable Devices" [5] by Liu et al. designs local authentication and remote authentication protocols for cloud assisted wearable devices.

Nowadays, Android platform has become the primary target of attackers. In the paper "Detecting Android Malicious Apps and Categorizing Benign Apps with Ensemble of Classifiers" [6], Wang et al. propose a framework to effectively and efficiently manage a big app market in terms of detecting malicious apps and categorizing benign apps. Verifiable Computation allows resource-restricted clients to delegate expensive computations to more powerful servers, and then to verify the correctness of the results. The paper entitled "Attribute-Based Multi-Function Verifiable Computation" [7] by Wu et al. introduces and formalizes the notion of attribute-based multi-function verifiable computation, which provides fine-grained access control to the computation results.

In previous research, there are no comprehensive authentication protocols designed for wireless body area networks (WBANs) according to its characteristics of network structure. In the paper entitled "A Lightweight Multi-layer Authentication Protocol for Wireless Body Area Networks" [8], Shen et al. propose an efficient multilayer authentication protocol and a secure session key generation method for WBANs. The paper "Secure and Fine-Grained Access Control on E-Healthcare Records in Mobile Cloud Computing" [9] by Liu et al. proposes a fine-grained e-healthcare record (HER) access control scheme which is proven secure in the standard model under the decisional parallel bilinear Diffie-Hellman exponent assumption.

In order to accurately locate and track mobile jammers in Multi-Hop Wireless Network (MHWN), the paper "Collaborative Mobile Jammer Tracking in Multi-Hop Wireless Network" [10] by Wei et al. proposes a distributed mobile jammer tracking scheme, which contains four steps, i.e., monitoring node selection, jamming signal measurement and result collection, jammer localization and monitoring node handover. Promoted by several promising opportunities provided by the advances in IoT and Cloud Computing

http://dx.doi.org/10.1016/j.future.2017.09.017

technologies for facing these challenges, the paper "Multi-layer Cloud Architectural Model and Ontology-based Security Service Framework for IoT-based Smart Homes" [11] by Tao et al. develops a novel multi-layer cloud architectural model to enable effective and seamless interactions/interoperations on heterogeneous devices/services provided by different vendors in IoT-based smart home.

We are grateful to Prof. Peter Sloot and FGCS for allowing us to host this special issue (SI) and serve the community. We plan to blend our scholarly activities with forthcoming conferences. Once again we thank all the contributing authors to make our scholarly work a great success.

References

[1] Z. Du, Yongjian Yang, Q. Cai, C. Zhang, Y. Bai, Modeling and inferring mobile phone users' negative emotion spreading in social networks, Future Gener. Comput. Syst. 78 (2018) 933–942.

[2] P. Vijayakumar, V. Chang, L.J. Deborah, B. Balusamy, P.G. Shynu, Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks, Future Gener. Comput. Syst. 78 (2018) 943–955.

[3] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment, Future Gener. Comput. Syst. 78 (2018) 956–963.

[4] C. Stergiou, K.E. Psannis, B.G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. 78 (2018) 964–975.

[5] H. Liu, H. Ning, Y. Yue, Y. Wan, L.T. Yang, Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Gener. Comput. Syst. 78 (2018) 976–986.

[6] W. Wang, Y. Li, X. Wang, J. Liu, X. Zhang, Detecting android malicious apps and categorizing benign apps with ensemble of classifiers, Future Gener. Comput. Syst. 78 (2018) 987–994.

[7] Y. Wu, M. Liu, R. Xue, R. Zhang, Attribute-based multi-function verifiable computation, Future Gener. Comput. Syst. 78 (2018) 995–1004.

[8] J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A lightweight multi-layer authentication protocol for wireless body area networks, Future Gener. Comput. Syst. 78 (2018) 1005–1019.

[9] Y. Liu, Y. Zhang, J. Ling, Z. Liu, Secure and fine-grained access control on e-healthcare records in mobile cloud computing, Future Gener. Comput. Syst. 78 (2018) 1020–1026.

[10] X. Wei, C. Tang, T. Wang, J. Fan, Collaborative mobile jammer tracking in multi-hop wireless network, Future Gener. Comput. Syst. 78 (2018) 1027–1039.

[11] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes, Future Gener. Comput. Syst. 78 (2018) 1040–1051.

Lead Guest Editor
Prof. Jin Li
School of Computer Science, Guangzhou University, China
E-mail address: jinli71@gmail.com.

Guest Editor
Assistant Prof. Qiben Yan
Department of Computer Science, University of Nebraska Lincoln, USA
E-mail address: yanqiben@gmail.com.

Guest Editor
Dr. Victor Chang
International Business School Suzhou, Xi'an Jiaotong-Liverpool University, China
E-mail address: ic.victor.chang@gmail.com.