Wu, Yulei; Yan, Zheng; Choo, Kim Kwang Raymond; Yang, Laurence T.

IEEE Access Special Section Editorial

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2019.2915489

Published: 01/01/2019

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Wu, Y., Yan, Z., Choo, K. K. R., & Yang, L. T. (2019). IEEE Access Special Section Editorial: Internet-of-Things Big Data Trust Management. *IEEE Access*, *7*, 65223-65227. Article 8728071.
https://doi.org/10.1109/ACCESS.2019.2915489

Digital Object Identifier 10.1109/ACCESS.2019.2915489

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: INTERNET-OF-THINGS BIG DATA TRUST MANAGEMENT

I. INTRODUCTION

Internet of Things (IoT) is increasingly common in our society and daily life, with applications ranging from personal devices (e.g., wearable devices such as Google Smartwatches) to smart home (e.g., smart TVs and Amazon Echo) to smart city/grid (e.g., unmanned aerial and/or ground vehicles), as well as in battlefield settings (e.g., Internet of Battlefield / Military Things). One corresponding trend associated with the increase in IoT devices, in terms of both number and diversity, is a significant increase in the volume, velocity, variety, variability, and value of the generated and resultant data (i.e., 5Vs of big data[1]).

This new computing paradigm involving both IoT and big data reshapes the landscape of engineering system design, business operations, compliance and many other activities, partly due to the magnitude and impact of data-related challenges in our data-driven society. For example, in a typical IoT system, any entity (human, software, and/or machines) is highly reliant on other entities within the network in their various activities, as well as ensuring the security, privacy, trustworthiness of data, and trustworthiness of services. Trust management is, undeniably, an emerging critical factor in system design, operations, compliance, and management in the IoT big data era; hence, the focus of this Special Section in IEEE Access.

IoT big data trust management is a hot and ongoing research agenda, and examples of current research challenges include those relating to heterogeneous IoT configurations, power and performance optimization, autonomic trust management, legal and compliance, and other operational requirements (e.g., the need for a comprehensive and distributed trust management framework, and interoperation or integration of data transmission and communication trust with other trust management mechanisms).

Due to the complexity of the challenges underpinning IoT big data trust management, we often need intellectual input of experts from different disciplines (e.g., science, technology, engineering and mathematics – STEM, and social sciences) and backgrounds, for example in terms of sectors (e.g., industry, governments and academia) and culture. Hence, this Special Section solicits the contributions from a diverse audience. On the basis of significance, originality, novelty and presentation, 26 articles were selected to be included in this Special Section. We will now introduce the 26 accepted articles.

II. MACHINE LEARNING-BASED APPROACHES

In the article entitled ‘‘Predict pairwise trust based on machine learning in online social networks: a survey,’’ Liu, *et al*., presented an overview of existing machine learning-based research efforts in pairwise trust prediction in the context of social networking. Specifically, the article summarizes existing trust-related datasets, classifiers and different metrics that had been used to evaluate trained classifiers. Based on the surveyed literature review, the authors identified a number of open issues and potential future research topics, such as trust prediction robustness, privacy preservation, context-awareness, fine-grained prediction and comprehension.

In ‘‘Machine learning-based malicious application detection of Android,’’ Wei, *et al*., designed a machine learning-based approach to detect malicious mobile malware in Android applications, including attacks that could not be effectively detected previously. A prototype tool, Androidetect, was also presented. Along similar lines (in the context of mobile IoT devices), in ‘‘Framework for mobile Internet of Things security monitoring based on big data processing and machine learning,’’ Kotenko, *et al*., explored the potential of combining big data processing and machine learning to facilitate security monitoring of mobile IoT devices.

III. CRYPTO-BASED APPROACHES

In order to overcome limitations associated with prior searchable public-key ciphertexts with hidden structures (SPCHS) schemes, the article entitled ‘‘Fast and parallel keyword search over public-key ciphertexts for cloud-assisted IoT,’’ by Xu, *et al*., presented a new instance of SPCHS to achieve fast and parallel keyword search over public-key ciphertexts. Specifically, the authors constructed a new type of hidden relationship among searchable ciphertexts to ensure that every searchable ciphertext has a hidden relationship with a common and public parameter. Thus, it is possible to disclose

[1] https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/ (last accessed Jan 23, 2019)

all corresponding relationships in parallel and efficiently find matching ciphertexts.

In the article entitled "Privacy-preserving and dynamic multi-attribute conjunctive keyword search over encrypted cloud data," by Zhang, *et al.*, the authors proposed a privacy-preserving conjunctive keyword search scheme over encrypted cloud data. This scheme can support dynamic update operations and multi-attribute conjunctive keyword search, such as equality conjunction, subset conjunction and range conjunction. Although its pre-processing cost is higher than existing work, it achieves lower computational overhead in terms of initialization, trapdoor generation and queries.

In "Virtualization of the encryption card for trust access in cloud computing," Xu, *et al.*, presented a virtualization architecture, where they established a risk model to investigate security requirements for encryption card virtualization. Specifically, they proposed a multi-classification access control model to ensure the security of the dynamic schedule of encryption cards and a hardware trust verification procedure, and designed protocols to establish a trusted chain between users and encryption cards.

The authors of "An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services," by Ji, *et al.*, proposed a certificateless conditional privacy-preserving authentication scheme, based on elliptic curve cryptography. The scheme allows one to perform batch authentication of multiple clients without incurring significant computational cost at the application provider. The scheme was also shown to resist attacks due to the loss of the device.

IV. PRIVACY- AND TRUST-RELATED WORK

Mobile crowdsourcing is also commonly found in IoT systems. Focusing on such a setting, Yang, *et al.*, in "Density-based location preservation for mobile crowdsensing with differential privacy," presented a data release mechanism that satisfies differential privacy, according to worker density and non-uniform worker distribution. Such a mechanism is designed to ensure the privacy of worker locations. A geocast region selection method was also presented to facilitate task assignment, in order to balance task assignment success rate by considering worker travel distances and system overheads. Thus, both worker location privacy and system performance can be achieved. Similarly, in "A study of enhancing privacy for intelligent transportation systems: k-correlation privacy model against moving preference attacks for location trajectory data," Sui, *et al.*, proposed an anonymity solution for publishing trajectory data, where the location frequency-inverse user frequency and k-correlation region are used to address the re-identification problem.

To address accountability and privacy challenges in IoT networks, the article entitled "An architecture for accountable anonymous access in the Internet-of-Things network," by Ma, *et al.*, proposed an architecture to provide accountable anonymous access to IoT networks based on services. Specifically, they introduced a self-certifying identifier for a service.

In order to ensure a trusted connection between IoT devices and edge servers, in "Remote software update in trusted connection of long range IoT networking integrated with mobile edge cloud," Kim, *et al.*, proposed a software update method. They applied a low-power wide area network (LPWAN) as a long-range IoT networking technology and used a mobile edge cloud to improve computing efficiency in an access network with resource-insufficient IoT devices. Through statistical connection information analysis, LPWAN trusted connection is determined for software update.

V. BIG DATA-RELATED WORK

IoT systems based on wireless sensor networks are vulnerable to a broad range of attacks, including malicious insider attacks. Trust management is one of several solutions deployed for intrusion detection, although the presence of big data could potentially degrade the effectiveness of trust computation. Thus, in "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," Meng, *et al.*, explained how one can combine Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure.

In "Malware visualization for fine-grained classification," Fu, *et al.*, proposed a new visualization method for characterizing malware globally and locally to achieve fast and effective fine-grained classification. This work attempts to overcome the challenges caused by large-scale and complex malware data sets on classification accuracy and computational overhead.

In the survey article by Atat, *et al.*, entitled "Big data meet cyber-physical systems: a panoramic survey," a cyber-physical system (CPS) taxonomy (comprising data collection, storage, access, processing, and analysis phases) was presented. The article also focuses on the different security solutions proposed for CPS big data storage, access, and analytics. In addition, the authors described challenges caused by big data in green CPS systems, such as how to ensure privacy preservation and correctness of such systems.

VI. FORENSIC-RELATED WORK

To deal with big data, in "IoT device forensics and data reduction," by Quick and Choo, the authors outlined a process of bulk digital forensic data analysis designed to efficiently process significant volumes of data by reducing their sizes through selective imaging and quick analysis, coupled with automated data extraction.

In "TMEC: a trust management based on evidence combination on attack-resistant and collaborative Internet of Vehicles," Chen, *et al.*, proposed a security scheme that uses evidence combination method to combine local data with external evidence to evaluate the reliability of multi-dimensional data received from other peer nodes. In addition, this article used European Telecommunications

Standards Institute (ETSI) standard and Decentralized Environmental Notification Message (DENM), and proposed a trust calculation method based on collaborative filtering by introducing a small time interval to detect the changes of node behaviors.

VII. NETWORKING- AND CLOUD-RELATED APPROACHES

In the article entitled "Solving anomalies in NFV-SDN based service function chaining composition for IoT network," Zou, *et al*., presented a composition method to fix the anomalies while composing distinct policies in an IoT network with multiple IoT service managers. This allows one to overcome the challenges due to conflicting global Service Function Chaining (SFC) policies. Two algorithms were designed to eliminate anomalies between policies, with minimal overhead introduced during the process of generating data plane rules. A review of network security-related data collection technologies was presented in the article entitled "A survey on network security-related data collection technologies," by Lin, *et al*., where the authors discussed the methods, mechanisms and technologies for collecting network data in terms of the functional and security objectives.

In "On-demand capacity provisioning in storage clusters through workload pattern modeling," Hu, *et al*., proposed a QoS-oriented capacity provisioning mechanism. Based on workload features, the mechanism models the pattern of current workloads as a suitable queuing model. In accordance with the model, the proposed mechanism can forecast the actual resource capacity demand without violating the service level agreement, and offers the required resource capacity.

Vehicular ad hoc networks (VANETs) and wireless sensor networks (WSNs) continue to be of interest in the academic community, due to their potential in smart cities (e.g., intelligent transportation). This is also evidenced in the two articles entitled "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," by Zhong, *et al*., and "RNOB: receiver negotiation opportunity broadcast protocol for trustworthy data dissemination in wireless sensor networks," by Lai and Wang. In the former, the authors proposed a practical, conditional privacy-preserving authentication scheme. This scheme uses the registration list instead of the revocation list to reduce communication overhead. In the second article, the authors presented a receiver negotiation opportunity broadcast protocol, which uses opportunistic routing for point-to-multipoint data dissemination to reduce redundant rebroadcasts and enhance the trustworthiness of transmission.

The long-term evolution (LTE)/LTE-advanced (LTE-A) network provides advanced services for billions of users due to its capability to support higher bandwidths, and achieve better spectrum efficiency and lower latency, in comparison to legacy cellular networks. A comparative summary is presented in the article entitled "LTE/LTE-A network security data collection and analysis for security measurement: a survey," where He, *et al*., reviewed existing security data collection and data analysis approaches for LTE/LTE-A networks.

In the article by Kazim, et al., "A framework for orchestrating secure and dynamic access of IoT services in multi-cloud environments," a framework for dynamic and secure IoT services access across multi-clouds using the cloud on-demand model was presented. This framework facilitates multi-cloud collaboration, and findings from the authors' experiments suggested that the proposed framework is scalable, and the proposed authentication protocols incur minimal overhead compared to standard authentication protocols. In addition, any Service Level Agreement violation by a cloud provider could potentially be recorded and reported back to the user.

In the article entitled "CloudVMI: a cloud-oriented writable virtual machine introspection," Qiang, *et al*., presented a writable and cross-node monitoring virtual machine introspection (VMI) framework for automated and centralized cloud management. This framework is designed to solve the semantic gap problem by redirecting the critical execution of system calls issued by the VMI program into the monitored virtual machines (VMs), and allows the introspection program to inspect heterogeneous guest operating systems and monitor VMs distributed on remote host nodes. It achieves effective and practical management for cloud with acceptable performance overhead.

In the article by Yeow, *et al*., "Decentralized consensus for edge-centric Internet of Things: a review, taxonomy, and research issues," a comprehensive review on decentralized consensus systems for edge-centric IoT was performed. In the review article, the authors presented a thematic taxonomy, outlining pivotal features and characteristics, and a number of open research issues for decentralized consensus systems.

Information-centric networking (ICN) is a promising networking paradigm, which can potentially provide fast content availability and service continuity in an IoT system. In the article entitled "FETMS: fast and efficient trust management scheme for information-centric networking in Internet of Things," Fang, *et al*. reviewed and analyzed security attacks and defenses for ICN. Moreover, they proposed a fast and efficient trust management scheme for detecting and defending against the on-off attack, which was shown to achieve low latency and high speed in detecting and mitigating such attack nodes.

VIII. CONCLUSION

In conclusion, we introduced the 26 accepted articles, categorized into machine learning-based approaches, crypto-based approaches, privacy- and trust-related work, big data-related work, forensic-related work, and networking- and cloud-related approaches. IoT will likely play a more important and pervasive role in our society in the foreseeable future. Therefore, there remains a need to keep a watchful eye on emerging challenges, as well as those that currently exist.

YULEI WU, *Guest Editor,*
University of Exeter
Exeter, U.K.

ZHENG YAN, *Guest Editor,*
Xidian University
Xi'an, China
Aalto University
Aalto, Finland

KIM-KWANG RAYMOND CHOO, *Guest Editor,*
University of Texas at San Antonio
San Antonio, TX, USA

LAURENCE T. YANG, *Guest Editor,*
St. Francis Xavier University
Antigonish, NS, Canada

YULEI WU received the B.Sc. degree (Hons.) in computer science and the Ph.D. degree in computing and mathematics from the University of Bradford, U.K., in 2006 and 2010, respectively. He is currently a Senior Lecturer with the Department of Computer Science, University of Exeter, U.K. His main research interests include network slicing and softwarization, future Internet architecture and technologies, smart network management, green networking, big data for networking, wireless networks, network security and privacy, and analytical modeling and performance optimization. His recent research was supported by the Engineering and Physical Sciences Research Council, U.K., the National Natural Science Foundation of China, the University's Innovation Platform, and industries. He is a Senior Member of the IEEE and Fellow of the HEA.

ZHENG YAN (M'06–SM'14) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science and Doctor of Science in Technology degrees in electrical engineering from the Helsinki University of Technology, Helsinki, Finland. She is currently a Professor with Xidian University, Xi'an, and a Visiting Professor and a Finnish Academy Research Fellow with Aalto University, Espoo, Finland. Her research interests include trust, security, privacy, and security-related data analytics. She achieved the Best Journal Paper Award of the IEEE ComSoc TCBD (2017) and the Outstanding Associate Editor of 2017 for the IEEE ACCESS. She serves as the General or Program Chair for over 30 international conferences and workshops. She is a Steering Committee Co-Chair of the IEEE Blockchain International Conference. She is also an Associate Editor of many reputable journals, e.g., the IEEE INTERNET OF THINGS JOURNAL, *Information Sciences*, *Information Fusion*, JNCA, the IEEE ACCESS, and SCN.

KIM-KWANG RAYMOND CHOO (SM'15) received the Ph.D. degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA) and has a courtesy appointment at the University of South Australia. He is a Fellow of the Australian Computer Society. In 2016, he was named the Cybersecurity Educator of the Year—APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015, he and his team won the Digital Forensics Research Challenge organized by the Germany's University of Erlangen-Nuremberg. He was a recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the IEEE TrustCom 2018 Best Paper Award, the ESORICS 2015 Best Research Paper Award, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship, in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award, in 2008. He is the Co-Chair of the IEEE Multimedia Communications Technical Committee (MMTC)'s Digital Rights Management for Multimedia Interest Group.

LAURENCE T. YANG received the B.Eng. degree in computer science and technology and the B.Sc. degree in applied physics from Tsinghua University, and the Ph.D. degree in computer science from the University of Victoria, Canada. He is currently a Professor and the W. F. James Research Chair with St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, embedded systems/Internet of Things, ubiquitous/pervasive computing and intelligence, and big data. He has published over 400 international journal papers in the above areas, of which half are on top IEEE/ACM transactions and journals, and others are mainly on Elsevier, Springer, and Wiley Journals. He is an elected Fellow of the Canadian Academy of Engineering (CAE) and the Engineering Institute of Canada (EIC). He has been involved and actively acts as the Steering Chair for over ten IEEE international conferences. He has been the Chair of the IEEE CS Technical Committee of Scalable Computing, since 2018, and the Chair of the IEEE SMC Technical Committee on Cybermatics, since 2016. He is also serving as an Editor for many international journals, such as the IEEE Systems Journal, the IEEE Access, *Future Generation of Computer Systems* (Elsevier), *Information Sciences* (Elsevier), *Information Fusion* (Elsevier), and *Big Data Research* (Elsevier).

• • •