World Wide Web (2020) 23:389–391
https://doi.org/10.1007/s11280-019-00772-z

Guest editorial: special issue on trust, privacy, and security in crowdsourcing computing

An Liu[1] · Guanfeng Liu[2] · Mehmet A. Orgun[2] · Qing Li[3]

Published online: 8 January 2020

Crowdsourcing is the process of engaging a crowd to provide services that can take place on many different levels and across various domains. The human-centric and cooperation-oriented feature of crowdsourcing prompts us to reexamine the trust, privacy, and security issues in this new paradigm since the individuals in the crowd typically are unfamiliar with each other and usually have different motivation behind participation. The goal of this special issue is to solicit high quality, original research contributions on all aspects of trust, privacy and security on crowdsourcing computing, thereby capturing the state of the art and stimulating further developments in the related areas. This will serve as not only a reference to all researchers working in the area, but also an important resource for the industry, showing the maturity of trust, privacy and security technology and creating an atmosphere for funding new trust, privacy and security projects.

Following an open call for papers, we received 26 submissions. Manuscripts passing the initial screening went through a rigorous two-round review process, during which each submission was evaluated by at least two reviewers based on topic relevance, originality of ideas, technical quality, significance of results, and quality of presentation. Finally, we accepted 12 papers. In the following, we will highlight the contributions of each paper.

Paper "A Survey of Blockchain Technology on Security, Privacy, and Trust in Crowdsourcing Services" by Ying Ma, Yu Sun, Yunjie Lei, Nan Qin, and Junwen Lu surveys existing blockchain technology to security, privacy, and trust issues in crowdsourcing services from the direction of industry and research, by discussing background knowledge, related concepts and basic models of blockchain, and analysing the current research status and the application of blockchain. The authors summarise the advantages and challenges of

This article belongs to the Topical Collection: *Special Issue on Trust, Privacy, and Security in Crowdsourcing Computing*
Guest Editors: An Liu, Guanfeng Liu, Mehmet A. Orgun, and Qing Li

✉ An Liu
anliu@suda.edu.cn

[1] School of Computer Science and Technology, Soochow University, Suzhou 215006, China

[2] Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

[3] Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China

blockchains, and shed light on the future research on blockchain technology used in crowdsourcing services.

Paper "Privacy Protection in Mobile Crowd Sensing: A Survey" by Yongfeng Wang, Zheng Yan, Wei Feng, and Shushu Liu surveys existing solutions to privacy issue from the view of the privacy target and evaluates their performances by employing the proposed requirements. The authors summarise with several open issues and significant future research directions, which help the design of practical privacy preservation mechanisms in mobile crowd sensing.

Paper "A Crowd-Efficient Learning Approach for NER based on Online Encyclopedia" by Maolong Li, Zhixu Li, Qiang Yang, Zhigang Chen, Pengpeng Zhao, and Lei Zhao, uses a crowd-efficient method for NER with the help of the knowledge in the online encyclopedia. The authors select some important samples to be labelled based on three criteria: representativeness, informativeness and diversity, which greatly reduces the cost of crowdsourcing.

Paper "Adaptive Knowledge Subgraph Ensemble for Robust and Trustworthy Knowledge Graph Completion" by Guojia Wan, Bo Du, Shirui Pan, and Jia Wu investigates the problem of facts noise in bottom-up constructed knowledge graph. In order to deal with this problem, the authors propose an ensemble strategy to enhance the robustness and trust of existing knowledge graph embedding approaches. Experimental results show that the robustness of the strategy outperforms exiting KG embedding methods on manually injected noise as well as inherent noisy extracted KGs.

Paper "Secure Range Query over Encrypted Data in Outsourced Environments" by Ningning Cui, Xiaochun Yang, Bin Wang, Jing Geng, and Jianxin Li presents a fully secure algorithm that preserves the confidentiality of data, query, result, access pattern and path pattern during range query over outsourced database. Two schemes are also proposed to accelerate query speed, making the algorithm useful in practical applications.

Paper "SGPM: A Privacy Protected Approach of Time-Constrained Graph Pattern Matching in Cloud" by Jinjing Huang, Wei Chen, Zhixu Li, Pengpeng Zhao, Weiqing Wang, Hongzhi Yin, and Lei Zhao explores the problem of enabling general queries on encrypted data directly. The authors present an effective dual-cloud protocol (DCP) which enables the cloud to recognize the results of comparisons though homomorphic encrypted values and a privacy protected approach of time-constrained graph pattern matching.

Paper "A Low Cost and Un-Cancelled Laplace Noise Based Differential Privacy Algorithm for Spatial Decompositions" by Xiaocui Li, Yangtao Wang, Jingkuan Song, Yu Liu, Xinyu Zhang, Ke Zhou, and Chunhua Li studies the security problem of applying differential privacy into spatial docomposition. The authors propose a secure spatial decomposition algorithm by indefeasible Laplace noise and show it can achieve an optimal trade-off between data privacy and data utility.

Paper "Co-Detection of Crowdturfing Microblogs and Spammers in Online Social Networks" by Bo Liu, Xiangguo Sun, Zeyang Ni, Jiuxin Cao, Junzhou Luo, Benyuan Liu, and Xinwen Fu investigates the problem of spammer detection in the new environment of crowdturfing microblogs. The authors combine user individual features, message content feature, and network property to propose a semi-supervised method which can effectively detect both spammers and crowdtrufing microblogs.

Paper "Distributed Time-respecting Flow Graph Pattern Matching on Temporal Graphs" by Tianming Zhang, Yunjun Gao, Linshan Qiu, Lu Chen, Qingyuan Linghu, and Shiling Pu explores the problem of distributed graph pattern matching in temporal graphs. The authors propose a distributed algorithm based on GraphX as well as an enhanced version by utilizing the properties of time-respecting flow graph, which can scales well over massive temporal graphs.

Paper “Spatial crowdsourcing based on Web mapping services” by Detian Zhang, Shiting Wen, Fei Chen, Zhixu Li, and Lei Zhao introduces a spatial crowdsourcing system based on Web mapping services, i.e., the spatial crowdsourcing platform can subscribe distance, live travel time and detailed route information from Web mapping services through their APIs, and utilize these retrieved map data for crowdsourcing processing. The authors also propose pruning and route sharing approaches to reduce the number of requesting these APIs.

Paper “Multi-Fuzzy-Objective Graph Pattern Matching in Big Graph Environments with Reliability, Trust and Social Relationship” by Lei Li, Fang Zhang, Zan Zhang, Peipei Li, and Chenyang Bu performs efficient query and matching on big graph data, specifically finds matched subgraphs to locate the required patterns to accomplish specific tasks. The authors introduce fuzziness and reliability into multi-objective graph pattern matching, and then use a multi-objective genetic algorithm NSGA-II to find the subgraphs with higher reliability and better attributes including social trust and social relationship.

Paper “Reverse-auction-based crowdsourced labelling for active learning” by Hai Tang, Mingjun Xiao, Guoju Gao, and Hui Zhao uses crowdsourcing to tackle the scarcity of training data in active learning. Based on the single-minded reverse auction for data labelling in active learning, the authors propose an approximately truthful, individually rational, privacy-preserving incentive mechanism with a guaranteed approximate performance.

The above 12 contributions encompass a wide range of research and topics in trust, security and privacy in crowdsourcing, thereby appealing to both the experts in the field and those who want a snapshot of the current breadth of the research field. As guest editors, we would like to thank the authors for their high-quality work and their contribution to this special issue. We appreciate all reviewers for their valuable comments and suggestions. We are also grateful to the Springer staff for their great support and guidance during the publication of this special issue. Last but not least, we would like to sincerely thank Prof. Yanchun Zhang, the Editor-in-Chief, for giving the opportunity to make this special issue possible.