Journal of Parallel and Distributed Computing 141 (2020) 59–60

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

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

Editorial

Preface: Security & privacy in social big data

Qin Liu [a,*], Md Zakirul Alam Bhuiyan [b], Jiankun Hu [c], Jie Wu [d]

[a] *College of Computer Science and Electronic Engineering, Hunan University, Changsha, Hunan Province, 410082, PR China*
[b] *Department of Computer and Information Sciences, Fordham University, BRONX NY, 10458, USA*
[c] *School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy, Canberra, ACT 2600, Australia*
[d] *Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA*

ARTICLE INFO

Article history:
Available online 27 March 2020

Keywords:
Preface
Big data
Social network
Security
Privacy

ABSTRACT

This special issue assembles a set of 11 papers, which provide deep research results to report the advance of security and privacy technology in social big data. This preface provides overview of all articles in the viewpoint set.

The rapid expansion of social networks remarkably changes the way people think, work, and interact. With more users proactively generate and share digital contents through social media, social networks have become a pivotal source of big data [11]. However, with such vast interconnectivity, convergence of relationships, and shared user information comes increased security and privacy concerns in social big data. On one hand, users carelessly posting their personal information on social media which can easily have their privacy breached. On the other hand, malicious attackers may manipulate such information to make a profit.

There are two important security and privacy issues in social networks. The first is how to effectively utilize social data while protecting user privacy. The second is how to guarantee the authenticity of social data for an in-depth data analysis. Traditional security mechanisms and models tailored to small-scale or isomorphic data are inadequate to securing social big data which exhibit enormous volume and diverse formats [5]. Therefore, how to develop scalable cryptographic algorithms/protocols and lightweight data mining/organization/optimization models to solve the security and privacy challenges becomes crucial for the successful application of social big data. The purpose of this special issue is to publish high-quality research papers as well as review articles that address the security, privacy, and trust challenges in social big data era. After a thorough review process, this special issue has selected a set of 11 papers, which provide new insights on the above-mentioned research areas.

Wang et al. [8] present a comprehensive survey for the security properties of machine learning (ML) algorithms under adversarial settings in the context of various applications. The authors analyze the ML security model, review adversarial attack methods, and discuss the defense strategies against these attacks. Their work is helpful to design more secure ML models.

Hassan et al. [2] provide a detailed overview for privacy-preserving strategies of smart meters and propose a differential-privacy-based real-time load monitoring approach (DPLM) to preserve user privacy when using smart meters. Their work is validated through rigorous security/performance analysis and experimental evaluation.

Wu et al. [10] research the risk defense method based on microscopic state prediction in social networks. The authors define the boundary nodes of network risk propagation and propose the risk restraining method based on propagation prediction (RRPP) to defend against network risks. Empirical studies have shown the effectiveness of the work.

Wei et al. [9] utilize differential privacy to protect a user's actual trajectory in trajectory community recommendation (TCR). Specifically, the authors propose a DP-based trajectory community recommendation (DPTCR) scheme to provide effective TCR service without relying on any fully trusted third party. Security analysis proves that the DPTCR scheme achieves ε-DP, and experimental results verify the effectiveness of the DPTCR scheme.

Yao et al. [13] consider the verifiable topic-based rank search problem in social data outsourcing scenario and propose two

[*] Corresponding editor.
E-mail address: gracelq628@126.com (Q. Liu).

https://doi.org/10.1016/j.jpdc.2020.03.011
0743-7315/© 2020 Elsevier Inc. All rights reserved.

schemes to guarantee the authenticity of social data. In the basic scheme, data consumers utilize their received query results and verification objects to verify the correctness of query results probabilistically. In the enhanced scheme, OSN can classify all topics into K clusters to reduce the number of considered rank values. Extensive experiments on real-world online social networks confirm the efficiency of their schemes

Yang et al. [12] address the problem of verifiable privacy-preserving k nearest neighbor (KNN) query on road networks. The authors propose an authenticated graph encryption scheme based on network Voronoi diagram, pseudo-random functions, and Paillier cryptosystem to ensure confidentiality and integrity of KNN queries. Security analysis proves that their scheme achieves CQA2-security with reasonable leakages, and experimental results show the effectiveness of the scheme.

Tran et al. [7] present a comprehensive survey of privacy-preserving big data analytics. The authors first introduce well-designed taxonomies to offer systematic views and detailed classification, then give insights into recent works, and finally identify open future research directions in this research field. This survey can serve as a good reference source for the development of modern privacy-preserving techniques in practice.

Liang et al. [3] address the problem of privacy-preserving range query over multi-source electronic health records in cloud computing. The authors identify three threats in real cloud-based eHealth systems, and propose a multi-source order-preserving encryption (MSOPE) scheme based on the security notion of indistinguishability under multi-source ordered chosen plaintext attack (IND-MSOCPA) to resist these threats. Their work is validated through rigorous security/performance analysis and experimental evaluation.

Liu et al. [4] propose a security disjoint routing-based verified message (SDRVM) scheme for gathering big data in energy harvesting networks. The SDRVM scheme establishes two disjoint connected dominating sets (CDS), a data CDS and a v-message CDS, for improving the data successful arrival ratio, and records the ID information in data packets to adjust the duty cycle adaptively. Their work is validated using simulations.

Salem et al. [6] investigate four major space-filling curve representations that allow for a cache-oblivious adaptation of parallel TU decomposition for rectangular matrices over finite fields (TURBO). The research results are helpful to improve the performance on parallel machines with private or shared caches and on GPU's. Their work is validated through rigorous security/performance analysis and experimental evaluation.

Amato et al. [1] present a semantic-based methodology that enhances the analysis process of a forensic investigation, with respect of evidence discovery, integrity and correlation. The methodology is able to add semantic assertion to data generated by forensics tools so as to provide efficient access and enhanced retrieval and reasoning capabilities in extraction processes. Their work is validated using simulations.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

In preparing this special issue we would like to thank Prof. Viktor Prasanna, the Editor-in-Chief of Journal of Parallel and Distributed Computing (JPDC) for his support. Furthermore, we would also like to thank Swetha Gudiseva and Hong Li of Elsevier for helping with all cases that needed specific consideration. We thank all reviewers of the manuscripts for this special issue their efforts have improved the quality of the volume considerably. We also thank the authors for participating in and contributing to this special issue.

References

[1] Flora Amato, Aniello Castiglione, Giovanni Cozzolino, Fabio Narducci, A semantic-based methodology for digital forensics analysis, J. Parallel Distrib. Comput. 138 (2020) 172–177.

[2] Muneeb Ul Hassan, Mubashir Husain Rehmani, Ramamohanarao Kotagiri, Jiekui Zhang, Differential privacy for renewable energy resources based smart metering, J. Parallel Distrib. Comput. 131 (2019) 69–80.

[3] Jinwen Liang, Zheng Qin, Sheng Xiao, Jixin Zhang, Hui Yin, Keqin Li, Privacy-preserving range query over multi-source electronic health records in public clouds, J. Parallel Distrib. Comput. 135 (2020) 127–139.

[4] Xiao Liu, Anfeng Liu, Tian Wang, Kaoru Ota, Mianxiong Dong, Yuxin Liu, Zhiping Cai, Adaptive data and verified message disjoint security routing for gathering big data in energy harvesting networks, J. Parallel Distrib. Comput. 135 (2020) 140–155.

[5] Qin Liu, Guojun Wang, Feng Li, Shuhui Yang, Jie Wu, Preserving privacy with probabilistic indistinguishability in weighted social networks, IEEE Trans. Parallel Distrib. Syst. 28 (5) (2017) 1417–1429.

[6] Fatima K. Abu Salem, Mira Al Arab, Laurence T. Yang, Extending the limits for big data RSA cracking: Towards cache-oblivious TU decomposition, J. Parallel Distrib. Comput. (2020).

[7] Hong-Yen Tran, Jiankun Hu, Privacy-preserving big data analytics a comprehensive survey, J. Parallel Distrib. Comput. 134 (2019) 207–218.

[8] Xianmin Wang, Jing Li, Xiaohui Kuang, Yu-an Tan, Jin Li, The security of machine learning in an adversarial setting: a survey, J. Parallel Distrib. Comput. 130 (2019) 12–23.

[9] Jianhao Wei, XinYao Yaping Lin, Voundi Koe Arthur Sandora, Differential privacy-based trajectory community recommendation in social network, J. Parallel Distrib. Comput. 133 (2019) 136–148.

[10] YouKe Wu, Haiyang Huang, Qun Wu, Anfeng Liu, Tian Wang, A risk defense method based on microscopic state prediction with partial information observations in social networks, J. Parallel Distrib. Comput. 131 (2019) 189–199.

[11] Youke Wu, Haiyang Huang, Ningyun Wu, Yue Wang, Md Zakirul Alam Bhuiyan, Tian Wang, An incentive-based protection and recovery strategy for secure big data in social networks, Inform. Sci. 508 (2020) 79–91.

[12] Shumei Yang, Shaohua Tang, Xiao Zhang, Privacy-preserving k nearest neighbor query with authentication on road networks, J. Parallel Distrib. Comput. 134 (2019) 25–36.

[13] Xin Yao, Yizhu Zou, Zhigang Chen, Ming Zhao, Qin Liu, Topic-based rank search with verifiable social data outsourcing, J. Parallel Distrib. Comput. 134 (2019) 1–12.