Hindawi
Security and Communication Networks
Volume 2018, Article ID 6238607, 3 pages
https://doi.org/10.1155/2018/6238607

Editorial

Privacy Issues in Big Data Mining Infrastructure, Platforms, and Applications

Xuyun Zhang,[1] Julian Jang-Jaccard,[2] Lianyong Qi,[3] Md Z. A. Bhuiyan,[4] and Chang Liu[5]

[1] *Department of Electrical and Computer Engineering, The University of Auckland, Auckland 1023, New Zealand*
[2] *Institute of Natural and Mathematical Sciences, Massey University, Auckland 0632, New Zealand*
[3] *School of Information Science and Engineering, Chinese Academy of Education Big Data, Qufu Normal University, Qufu 276826, China*
[4] *Department of Computer and Information Sciences, Fordham University, JMH 328A, Bronx, NY, USA*
[5] *School of Computing Science, Newcastle University, Newcastle NE4 5TG, UK*

Correspondence should be addressed to Xuyun Zhang; xuyun.zhang@auckland.ac.nz

Received 4 February 2018; Accepted 6 February 2018; Published 5 March 2018

We are pleased to announce the publication of the special issue focusing on privacy issues in big data mining infrastructure, platforms, and applications. The integration of extensive parallel computation power, scalable platforms, and advanced communications has profoundly unleashed the potentials of big data mining in recent years. A large number of cloud data centers have been established around the globe and provide necessary tools and infrastructure to utilize economical, on-demand, rapid-elasticity computation and storage services. With these, an increasingly huge amount of data of various types and formats has been collected from many different sources such as online social media, Internet of Things (IoT), mobile devices, and genome projects via both wired and wireless communication channels. Unlocking the value of big data through analytics and mining has been regarded as the key enabler of many innovation and marketing strategies which, in turn, has pushed more efforts and support to the big data related R&D. As an evidence, for example, Gartner has recently reported that most of the world's largest 200 companies have plans to invest in the development of intelligent apps as well as utilizing the full toolkit of big data and analytics tools by 2018. New founding from these investments then is to be incorporated to refine the services offered by companies and improve customer experience. This illustrates that an extensive research is expected to be more actively supported for big data mining infrastructure, platforms, and applications that runs both on wired and on wireless communication channels in order to conduct more efficient knowledge discovery and smart decision support.

One of the major concerns in big data mining approach is with security and privacy. With big data applications such as online social media, mobile services, and smart IoT widely adopted in our daily life, an enormous amount of data has been generated based on various aspects of the individuals. Without a proper security and privacy protection in all aspects of computing environment including communication environment, this can be disclosed intentionally or unintentionally, posing severe threats on the individuals. Moreover, as the storage, delivery, management, processing, and mining of such massive data sets are often outsourced to cloud data centers, traditional security solutions confined within a well-defined security perimeter fail to be applied in such open and sharing environments. These security and privacy issues pose tremendous barriers to taking advantages from the full use of our huge data assets. As such, it is high time to investigate the security and privacy issues in big data mining by examining big data infrastructure, platforms, and applications in detail. This special issue gained substantial interests of researchers from all over the world, and our editorial team consisting of five researchers in this field has selected twelve articles for publication. The research topics include privacy-preserving outsourced auditing, privacy-preserving data sharing, privacy-aware data placement, privacy of location-based services, privacy-preserving recommendation, key management, watermarking, misbehavior detection, and trust management in cloud platforms, wireless sensor networks, delay-tolerant networks, and big data analytics platforms.

In the paper entitled "Privacy-Preserving Outsourced Auditing Scheme for Dynamic Data Storage in Cloud," T. Tu et al. studied the data privacy problems when enabling third-party auditors (TPA) to have read access right over users' outsourced data and introduced the notion of User Focus for outsourced auditing which emphasizes the users' dominance over their own data. Accordingly, the authors proposed scheme without depending on data encryption that not only can prevent users' data from leaking to TPA, but also avoid the practically challenging issue of using of additional independent random source. Dynamic updating is also supported by this scheme.

In the paper entitled "Protecting Privacy in Shared Photos via Adversarial Examples Based Stealth," Y. Liu et al. explored the privacy disclosure problems in the online image sharing scenario and proposed a novel Stealth algorithm that can make the automatic detector blind to the existence of object in an image by crafting adversarial examples. The results have shown that the scheme has a higher success rate than the state-of-the-art methods like Mosaic, Blur, and Noise, while guaranteeing privacy and having the smallest impact on the image visual quality.

In the paper entitled "Data Placement for Privacy-Aware Applications over Big Data in Hybrid Clouds", X. Xu et al. investigated the privacy-aware data placement in the hybrid cloud context where both private and public cloud services are employed and proposed a cost- and energy-aware data placement method named CEDP for privacy-aware big data applications deployed in a hybrid cloud mode. Both formalized analysis and empirical evaluation have demonstrated the efficiency and effectiveness of the proposed method.

In the paper entitled "An Improved Privacy-Preserving Framework for Location-Based Services Based on Double Cloaking Regions with Supplementary Information Constraints", C. Li et al. studied the problem of privacy disclosure in location-based services, especially caused through the supplementary information held by attackers. Accordingly, they proposed an improved privacy-preserving framework for location-based services based on double cloaking regions with supplementary information constraints. Empirical studies have shown that the approach can prevent users against strong privacy attacks with supplementary information and reduce the computational overheads of generating dummy positions.

In the paper entitled "A Heuristic Model for Supporting Users' Decision-Making in Privacy Disclosure for Recommendation," H. Wu et al. investigated management of users' information disclosure decisions in the context of high-quality experiences from social media and IoT and formulated the analysis of why the heuristics from crowds can influence the decision and how to optimize the user experience. Specifically, the authors proposed a novel heuristic model that defines the data structures of requested items and participants in social media and uses a modified decision tree classifier to predict participants' next disclosures. Empirical evaluation demonstrates that the heuristics model can "persuade" participants to change their disclosure behaviors and reveals that users' answers to the mildly sensitive items tend to be more variable and less predictable.

In the paper entitled "LEPA: A Lightweight and Efficient Public Auditing Scheme for Cloud-Assisted Wireless Body Sensor Networks," S. Li et al. examined the integrity issues of the health related data collected from wireless body sensor networks (WBSNs) and stored in cloud services and proposed a lightweight and efficient public auditing scheme named LEPA to address the conflict between the high data density and weak processing capacity in WBSNs. Compared with similar schemes, the WBSNs' client only needs to do one symmetrical encryption with low computational cost in LEPA. Security proof shows that LEPA can resist two types of adversaries in random oracle model.

In the paper entitled "Efficient Anonymous Authenticated Key Agreement Scheme for Wireless Body Area Networks," T. Li et al. investigated the authentication protocols for wireless body area networks (WBANs) which is widely used in telemedicine but prone to many security threats on clients' personal information and proposed an efficient authenticated key agreement scheme for WBANs with adding a key update phase to enhance the security. Session keys are generated during the registration phase and kept secretly, thus reducing computation cost in the authentication phase. The performance analysis demonstrates that the scheme is more efficient than the existing schemes.

In the paper entitled "Parameterization of LSB in Self-Recovery Speech Watermarking Framework in Big Data Mining," S. Li et al. proposed a novel self-recovery speech watermarking framework with taking trustable communication in big data mining into account. The watermark is a compressed version of the original speech and embedded into the least significant bit (LSB) layers, which can be used to detect and recover tampered speech at a later stage. The relationship between LSB and other parameters are explicitly formulated in a mathematical manner, in order to facilitate the selection of parameters for the framework. Experimental results show that when the number of LSB layers varies from six to three, the imperceptibility of watermark increases, while the quality of the recovered signal decreases.

In the paper entitled "A Security and Efficient Routing Scheme with Misbehavior Detection in Delay-Tolerant Networks," F. Li et al. studied the security and efficiency issues of delay-tolerant networks (DTNs) and designed a secure and efficient routing scheme named SER by integrating a routing decision mechanism and an attack detection mechanism. The global trust status can be derived from the nodes where the local trust degrees on other nodes and contact summary information are locally maintained. The mechanism of detecting malicious or selfish nodes exploits the global summary information, and the routing decision mechanism makes use of the trust degree of forwarding messages among nodes.

In the paper entitled "Trusted Service Scheduling and Optimization Strategy Design of Service Recommendation," X. Xia et al. explored the problem of personalized service recommendation based on trust relationships and proposed a service recommendation and scheduling approach based on user preference derived from social trust relationships. Specifically, social topology and service demand information are analysed to infer the social trust relationships. A fusion model of the historical service preferences and the potential preferences is constructed for service recommendation.

In the paper entitled "A Multidomain Survivable Virtual Network Mapping Algorithm", X. Xiao et al. investigated the mapping problem in the multidomain virtual networks and proposed a survivable virtual network mapping algorithm (IntD-GRC-SVNE) to dress the issue that physical networks fail to ensure the normal provision of network services due to external reasons like network interruption during transmission. Specifically, the proposed algorithm maps virtual communication networks onto different domain networks and provides backup resources to virtual links for improving the survivability of the special networks.

In the paper entitled "Service Composition Optimization Method Based on Parallel Particle Swarm Algorithm on Spark," X. Guo et al. explored the large-scale service composition problem in the cloud computing environment and proposed a parallel optimization approach named Spark Particle Swarm Optimization (SPSO) based on the Apache Spark distributed environment. A parallel covering algorithm is designed to cluster similar web services. Then, the cluster centers as the starting point of particles are fed to the swarm optimization algorithm to improve the diversity of the initial population. Finally, the particle elite selection strategy is used to remove the inert particles in order to optimize the performance of the combination of service selection.

We strongly believe that this special issue will advance the understanding and research of various privacy issues in big data mining infrastructure, platforms, and applications. We hope that you will enjoy reading these novel contributions!

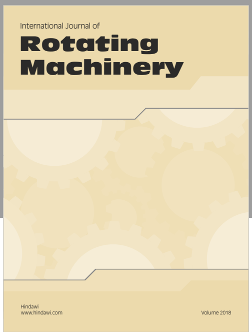
Acknowledgments

We would also like to thank all the reviewers who have participated in the review process of the articles submitted to this special issue and the special issue coordinators and acknowledge the technical support from the publishing team.

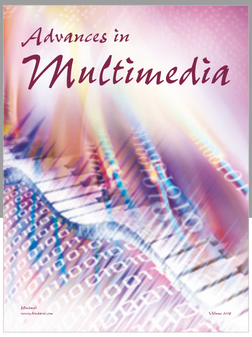
Xuyun Zhang
Julian Jang-Jaccard
Lianyong Qi
Md Z. A. Bhuiyan
Chang Liu

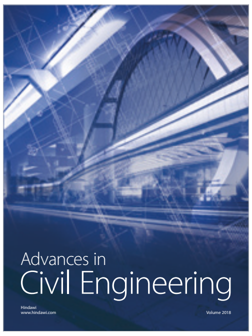
Journal of
Engineering

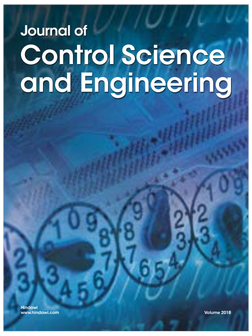
The Scientific
World Journal


International Journal of
Rotating
Machinery

Journal of
Sensors

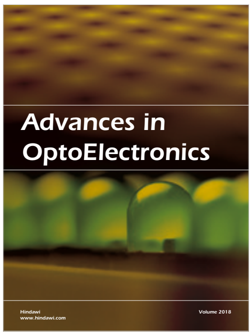

Advances in
Multimedia


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

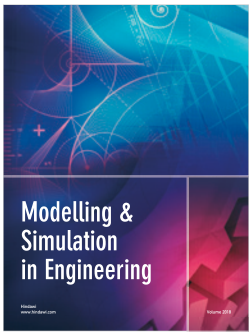
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

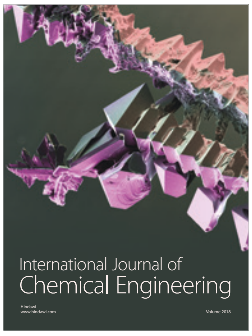

Advances in
OptoElectronics

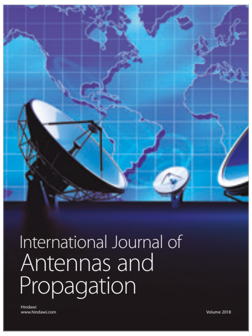
VLSI Design

International Journal of
Navigation and
Observation

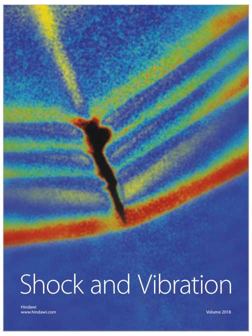

Modelling &
Simulation
in Engineering

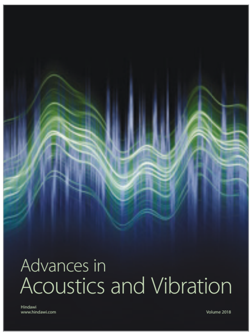
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration