Overview

The collection, analysis and sharing of person-specific data for publication or data mining, raise serious concerns about the privacy of individuals who are represented in the data, as well as the sensitive knowledge patterns that can be exposed when mining the data. To address these concerns, the domain of privacy preserving data mining was brought into existence almost a decade ago. Since then, a wide variety of methodologies for privacy-aware data sharing and integration, privacy preserving data publication and privacy preserving data mining, have been developed. Although significant research on this domain has been conducted over the last years, there are still many challenges that require further investigation both from a theoretical and from a practical point of view. First of all, emerging research areas, such as stream mining, mobility data mining and social network analysis, require new theoretical and applied techniques for the offering of privacy. Second, there is an urging need for privacy methodologies that can offer guarantees about the level of achieved data quality and utility, and thus be suitable for data demanding applications, such as biomedical and healthcare studies, location-based services and e-commerce. Third, the integration or linkage of data in a privacy preserving manner along with the privacy-aware collaborative mining of data require further stimulus to provide scalable methodologies on very large datasets and large number of parties, while offering a high level of privacy.

Topics of interest

The workshop’s topics of interest include, but are not limited to, the following areas:

- Biomedical and healthcare data mining privacy
- Cryptographic approaches for privacy preserving data mining
- Data mining for intrusion detection, fraud and identity theft prevention
- Privacy preserving data publishing and anonymity
- Knowledge hiding methodologies
- Inference and disclosure control for data mining
- Privacy in e-commerce and user profiling
- Privacy-aware access control
- Privacy and security when mining outsourced data
- Privacy aspects of ubiquitous computing systems
- Privacy policy infrastructure, enforcement, and analysis
- Privacy preserving link and social network analysis
- Privacy preserving data integration and record linkage
- Privacy threats due to data mining
- Security and privacy issues in mobility and spatiotemporal data mining
• Link and friend-of-a-friend (FOAF) mining for trust
• Efficiency improvements to known privacy preserving analytics algorithms
• Case studies of practical privacy preserving data analytics

Important dates

• Workshop paper submission deadline: July 23, 2010
• Workshop paper acceptance notification: September 20, 2010
• Workshop paper camera-ready deadline: October 11, 2010

Organizing committee (in alphabetical order)

Workshop chairs

1. Aris Gkoulalas-Divanis, IBM Research Zurich, Switzerland
2. Kun Liu, Yahoo! Research Labs, California, USA
3. Vassilios S. Verykios, University of Thessaly, Greece
4. Ran Wolff, Haifa University, Israel

Tentative Program committee members

1. Elisa Bertino, Purdue University, USA
2. Francesco Bonchi, Yahoo! Research, Spain
3. Peter Christen, Australian National University, Australia
4. Chris Clifton, Purdue University, USA
5. Benjamin C. M. Fung, Concordia University, Canada
6. Wei Jiang, Missouri University of Science and Technology, USA
7. Murat Kantarcıoğlu, University of Texas at Dallas, USA
8. Grigoris Loukides, Vanderbilt University, USA
9. Emmanuel Magkos, Ionian University, Greece
10. Bradley Malin, Vanderbilt University, USA
11. Mohamed Mokbel, University of Minnesota, USA
12. Ercan Nergiz, Sabanci University, Turkey
13. Jian Pei, Simon Fraser University, USA
14. Yucel Saygin, Sabanci University, Turkey
15. Jianhua Shao, Cardiff University, UK
16. Philip S. Yu, University of Illinois at Chicago, USA
17. Evimaria Terzi, Boston University, USA
++ (additional members to be included)

Submission guidelines

Paper submissions should be limited to a maximum of 10 pages in the IEEE 2-column format (http://www.computer.org/portal/web/cscps/formatting). All papers will be double-blind reviewed by the Program Committee on the basis of technical quality, relevance to data mining, originality, significance, and clarity. Papers that have
already been accepted or are currently under review for other conferences or journals will not be considered for PADM 2010.

The authors of a small number of selected (best) papers from the workshop will be invited to prepare a substantially revised and extended version of their work for publication to the journal of Transactions on Data Privacy.