Track: Data Science, Privacy and Security

Recent trends have shown a drastic increase in large data repositories by corporations, governments, and healthcare organizations. These data are collected from various sources, such as crowdsourcing, with or without consent from data donors. These data create opportunities for developing knowledge and information-based decision making systems by utilizing data mining. However, there is a significant risk of compromising sensitive information. This risk of information leakage by using data mining tools has become an obstacle to the advancement of the data science. This special track solicits papers that discuss various aspects of data privacy from either theoretical or practical perspectives. Research papers providing real-life privacy solutions, various applications of machine learning, data mining and deep learning are particularly encouraged.

The IEA/AIE has been a unique platform for computer science research, presenting the latest developments and bringing together researchers and practitioners. The 31st annual conference is seeking previously unpublished papers offering novel research contributions in any aspect of the track/conference scopes. Papers may present advances in the theory, implementation, analysis, or empirical evaluations of software and/or hardware systems. Topics of interest in data science and machine learning include, but are not limited to, the following:

- Privacy Preserving Data Publishing (PPDP)
- Privacy, Security and Data Usability
- Anonymity of Data
- Differential Privacy
- Privacy and Genome Data
- Risk of re-identification and Privacy attacks
- Privacy-preserving Models
- Privacy and Cloud Computing
- Privacy and Social Networks Data
- Privacy and Health Data
- Privacy and Location-based Services
- Security and privacy metrics
- Privacy and Data Mining

- Statistical Disclosure Control (SDC)
- Privacy, Security and Big Data
- Network Security and Privacy
- Applications of Data Mining
    - Cybersecurity and Text Mining
    - Security and Fraud detection
    - Security and Intrusion Detection
    - Big Data
- Applications of Machine Learning
    - Biometrics and cybersecurity
- Deep Learning

Track Chairs

1. Dr. A. N. K. Zaman, Computer Science, University of Guelph, Canada
2. Dr. Rozita Dara, Computer Science, University of Guelph, Canada

Important Dates:

Paper Submission deadline: January 7, 2018

Notification of Acceptance/Rejection: February 5, 2018

Camera Ready Paper Submission: February 26, 2018