INTERNATIONAL

INVITED SESSION SUMMARY

Title of Session:

Security and Privacy of Data Analytics in Information-Thriving Intelligent Infrastructure

Name, Title, and Affiliation of Chair:

Yuh-Jong Hu, Professor, National Chengchi University, Taipei, Taiwan

Name, Title, and Affiliation of Co-Chair:

Celimuge Wu, Associate Professor, the University of Electro-Communications, Tokyo, Japan

Details, Aim, and Scope of Session:

In today's cyber–physical world, an enormous amount of data is continuously created from the ubiquity of smart devices such as smart phones, smart watches, the Internet of Things (IoT), driverless cars, and energy meters. Once big data are collected and aggregated in an information-thriving intelligent infrastructure, data analysts can apply high-dimensional machines or statistical learning to infer correlations of data features and, in turn, cluster, classify, predict, and even derive cause–effect relationships.

From the perspective of data analysts (or users), the incentive of applying data analytics is being able to leverage statistical inferences with big data in order to obtain optimal learning models for intelligent decision making in dynamic and uncertain situations. For example, the aggregation of driverless car running information from IoT devices is very useful for car makers to improve the functionality of new cars, as well as for city transportation administrators to mitigate the impact of traffic jams by analyzing real-time response information during accidents. By extension, updated, real-time traffic maps are useful for data owners (e.g., car owners) to plan alternative travel routes in response to car accidents on original routes. Similarly, the aggregation of daily activity data from smart watches can help doctors to monitor the health status of patients in order to enable timely medical care. But this health information might allow health insurance companies to adjust insurance premiums. Numerous other similar scenarios are available in today's cyber–physical world.

The primary challenge of exercising big data analytics services is to develop information-thriving intelligent infrastructure in which big data are pervasively generated, aggregated, and analyzed from smart devices without worrying about the risk of violating security and privacy. Analytics execution software should be also protected by way of program obfuscation. Otherwise, data owners become reluctant to share data and modelers hesitate to provide analytics services in a public cloud. Well-known public cloud providers such as Amazon and Google have established secure cloud computing environments via virtualization security techniques to defend virtual machine (VM) monitors (or hypervisors) and VMs themselves against malicious attacks. However, from the perspective of data and program protection, since a cloud provider as a platform-as-a-service (PaaS) remains a *curious-but-honest* stakeholder, another layer of data and program protection is necessary with types of software-as-a-service (SaaS) to ensure that data and programs in transit, in use, and at rest meet security and privacy principles in cyber–physical systems.

The aim of this session is to gather academic and industrial papers on secure and private data analytics for particular decision-making scenarios in information-thriving intelligent infrastructure. Secure data analytics ensures accountable and fair decision making from aggregated data and programs that are not manipulated in adversarial learning environments. By using emerging data protection techniques such as homomorphic encryption or differential privacy, the goal of privacy-preserving data analytics can be accomplished to balance data use and privacy in outsourcing multi-tenant public cloud environments.

Solicited topics include but not limited to:

- Secure and private data analytics at or from the IoT and mobile devices;
- Secure and private data analytics for a cyber–physical system;
- Secure and private social network analytics;
- Secure data analytics with program obfuscation in a cloud;
- Privacy-preserving data analytics in a cloud;
- Secure data analytics with accountable and fair decision making;
- Private data analytics via homomorphic encryption;
- Private data analytics with differential privacy;
- Secure and private analytics as SaaS in a cloud; and
- Experiences with implementing secure and private analytics services.

Important Dates and Deadlines:

Submission of Papers: 12 January 2018
Notification of Acceptance: 12 February 2018
Uploading of Final Publication Files: TBA

Website URL of Call for Papers:

http://ent.cs.nccu.edu.tw/sp-da-itii

Email and Contact Details:

Prof. Yuh-Jong Hu
Dept. of Computer Science
National Chengchi University, Taipei, Taiwan
hu@cs.nccu.edu.tw

Associate Prof. Celimuge Wu
Dept. of Computer and Network Engineering
The University of Electro-Communications, Tokyo, Japan
celimuge@uec.ac.jp