Wright State University

CORE Scholar

Computer Science & Engineering Syllabi

College of Engineering & Computer Science

Winter 2012

CS 790-01: Privacy-Aware Computing

Keke Chen
Wright State University - Main Campus, keke.chen@wright.edu

Follow this and additional works at: https://corescholar.libraries.wright.edu/cecs_syllabi

Part of the Computer Engineering Commons, and the Computer Sciences Commons

Repository Citation

CS790 – Privacy-Aware Computing

Wright State University, Winter 2012

Credit hours 4
Time: 4:10 pm - 5:25 pm, MW
Location: Russ 302
Course Website: http://www.cs.wright.edu/keke.chen/cs790/, and pilot

Instructor

Keke Chen, Ph.D.
Office: 385 Joshi
Office hours: MW, 2-3:30pm
Email: keke.chen@wright.edu
Phone: (937) 775-4642
Web: http://www.cs.wright.edu/~keke.chen/

Course Description

In this course, we will discuss a set of research papers on various topics of privacy-aware computing: data perturbation, data anonymization, randomized responses, privacy preserving data mining, privacy preserving multivariate statistical analysis, private information retrieval, and secure data outsourcing, etc. Students are expected to read some papers and submit paper summaries. Participation in the class discussion is encouraged. Students will need to finish a course project and give a project presentation. Each project team can have 1~2 people. (4 Hours Lecture).

Prerequisite:

Basic knowledge of statistics, machine learning, data mining, and distributed systems

Text Books and Materials

There is no textbook for this course. All materials will come from recently published papers and online documents. A reference list is at
http://www.cs.wright.edu/~keke.chen/cs790/reading_list.htm

Assignments

There will be several reading assignments. Students should submit reading summaries for the assigned papers. Each paper summary consists of a few paragraphs with less than one

page, including the problem, the technical contributions, the strengths and weaknesses of the approach. There is one term project, which has three parts: presentation, report and project demo. Some project topics will be given. Students can also use their own project ideas. There is no exam for this course.

Grading Policy

Reading summaries   30%
Project presentation   10%
Project report   30%
Project code & demo   20%
Class participation   10%

Covered Topics

1. Introduction to privacy aware computing   1 class

2. Data perturbation   3 classes

3. Privacy metrics   1 class

4. Data anonymization   3 classes

5. Randomized responses   1 class

6. Privacy preserving mining: classification, clustering, rule mining, and multivariate analysis   3-4 classes

7. Privacy preserving information retrieval   2 classes

8. Secure data outsourcing   2-3 classes

9. Privacy in online social networks   2-3 classes

10. Location privacy   1-2 classes