CS6290: PRIVACY-ENHANCING TECHNOLOGIES

Effective Term
Semester B 2024/25

Part I Course Overview

Course Title
Privacy-enhancing Technologies

Subject Code
CS - Computer Science
Course Number
6290

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
P5, P6 - Postgraduate Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
CS5285 Information Security for eCommerce

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract
Large amount of data containing sensitive personal information are being constantly collected in today's digitised world. Examples include e-health records in medical systems and location data in ubiquitous mobile applications. How can we

guarantee that the collected user data are not misused and privacy policies not violated? How can we protect user privacy while simultaneously allowing effective data sharing and utilization? When the servers are not fully trusted, how can we still provide desirable services to users and respect their privacy?

This course aims at providing students with advanced concepts and latest progress on emerging techniques in information security and privacy. Topics will be adjusted to reflect the latest trend and the interests of students. Exemplary topics include, but not limited to, cloud security, cryptocurrency and decentralised ledger technologies, machine learning and security, data anonymization, and encrypted databases. Learning activities include lectures, group projects, case studies, and tutorial sessions.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Identify and analyse common privacy issues of modern applications, and suggest countermeasures.	20	x	x	
2	Explain the concept and design principles of privacy-enhancing mechanisms with merits assessment.	20	x	x	
3	Describe and analyse guidelines to apply privacy-enhancing techniques in real-world settings.	20	x	x	x
4	Discuss constraints of different privacy-enhancing designs and identify directions to address shortcomings.	20	x	x	
5	Analyse and evaluate the effectiveness of privacy-enhancing designs through written reports and oral presentations.	20	x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Students will engage with case studies for identifying the security and privacy issues in digitised world, and exploring countermeasures that support privacy-assured applications.	1, 2, 3, 4, 5	2 hours

2	Seminars	Students will discuss and clarify the concept of knowledge points, and also to develop in-depth understanding on the related design principles, followed by critique and discussions.	2, 5	2 hours
3	Tutorials	Students will work on given concrete cases or assigned reading materials with problems during tutorial sessions to gain enhanced understanding of the lecture materials.	3, 4	1 hour
4	Course Project	Students will participate in the course project to catch up with the state-of-the-art topics to improve and broaden their knowledge.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Assignments	1, 2, 3, 4, 5	40	Individual assignments will be given. It may consist of technical questions and/or research and mini-report on the security and privacy topics covered in this course.
2	Project with written report and presentation	1, 2, 3, 4, 5	20	Students will perform a critical study of the techniques related to the course and report of their findings under the guidance of the Course Leader. Possible deliverables could include a software prototype, a substantial case study, or a technical report with theoretical merits.

Continuous Assessment (%)

60

Examination (%)

40

Examination Duration (Hours)

2

Additional Information for ATs
For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task
Assignments (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Ability to identify various privacy risks in today's technologies and point out counter measures.

Excellent
(A+, A, A-) Strong evidence of capacity to analyse and synthesize.

Good
(B+, B, B-) Evidence of capacity to analyse and synthesize.

Fair
(C+, C, C-) Ability to analyse and solve simple problems in the material.

Marginal
(D) Familiarity with the subject matter.

Failure
(F) Little evidence of familiarity with the subject matter.

Assessment Task
Project (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion
Capacity to conduct critical and substantial study on privacy-enhancing topics.

Excellent
(A+, A, A-) Strong evidence of original thinking; good organization; extensive knowledge base.

Good
(B+, B, B-) Evidence of familiarity with literature, critical capacity and analytic capacity.

Fair
(C+, C, C-) Limited evidence of familiarity with literature, critical capacity and analytic capacity.

Marginal
(D) Familiarity with the project subject.

Failure
(F) Weakness in critical and analytic skills; limited, or irrelevant use of literature.

Assessment Task
Examination (for students admitted before Semester A 2022/23 and in Semester A 2024/25 & thereafter)

Criterion

Ability to describe and analyse the methodologies of privacy enhancing technologies, and evaluate tradeoffs among privacy, performance, and utility.

Excellent
(A+, A, A-) Strong evidence of grasp of subject matter and understanding of issues.

Good
(B+, B, B-) Evidence of grasp of subject matter and understanding of issues.

Fair
(C+, C, C-) Limited evidence of grasp of subject matter and understanding of issues.

Marginal
(D) Familiarity with the subject matter.

Failure
(F) Little evidence of grasp of the subject matter.

Assessment Task
Assignments (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Ability to identify various privacy risks in today's technologies and point out counter measures.

Excellent
(A+, A, A-) Strong evidence of capacity to analyse and synthesize.

Good
(B+, B) Evidence of capacity to analyse and synthesize.

Marginal
(B-, C+, C) Limited ability to analyse and solve simple problems in the material.

Failure
(F) Not even reaching marginal levels.

Assessment Task
Project (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion
Capacity to conduct critical and substantial study on privacy-enhancing topics.

Excellent
(A+, A, A-) Strong evidence of original thinking; good organization; extensive knowledge base.

Good
(B+, B) Evidence of familiarity with literature, critical capacity and analytic capacity.

Marginal
(B-, C+, C) Limited evidence of familiarity with literature, critical capacity and analytic capacity.

Failure

(F) Not even reaching marginal levels.

Assessment Task

Examination (for students admitted from Semester A 2022/23 to Summer Term 2024)

Criterion

Ability to describe and analyse the methodologies of privacy enhancing technologies, and evaluate tradeoffs among privacy, performance, and utility.

Excellent

(A+, A, A-) Strong evidence of grasp of subject matter and understanding of issues

Good

(B+, B) Evidence of grasp of subject matter and understanding of issues

Marginal

(B-, C+, C) Limited evidence of grasp of subject matter and understanding of issues

Failure

(F) Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

Topics will be chosen to reflect the latest trend and the interests of students. Possible topics include: Cloud security, search over encrypted data, cryptocurrency and blockchain machine learning and security, data anonymization and de-anonymization techniques, oblivious remote storage, encrypted databases. Other topics could include privacy issues in mobile computing, web tracking, targeted advertising, and social networks.

Reading List

Compulsory Readings

	Title
1	Ari Juels and Alina Oprea, New Approaches to Security and Availability for Cloud Data, Communications of the ACM, Vol. 56 No. 2, Pages 64-73, 2013
2	Raluca Ada Popa and Nickolai Zeldovich. How to Compute With Data You Can’ t See. IEEE Spectrum, July 23, 2015
3	Dawn Song, Elaine Shi, Ian Fischer, Umesh Shankar. Cloud Data Protection for the Masses. IEEE Computer, vol. 45, no. 1, page(s): 39-45. January 2012
4	Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten, SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, in Proc. of IEEE Symposium on Security and Privacy, 2015
5	Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen, Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell, Robert K. Cunningham, SoK: Cryptographically Protected Database Search, in Proc. of IEEE Symposium on Security and Privacy, 2017
6	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Hardcover, Princeton University Press, July 19, 2016
7	Articles from selected IEEE/ACM magazines, journals, conference proceedings, will further be provided when necessary.

Additional Readings

	Title
1	Kui Ren, Cong Wang, and Qian Wang. Security challenges for the public cloud. IEEE Internet Computing, vol. 16, no. 1, 2012.
2	Cong Wang, Kui Ren, Wenjing Lou, and Jin Li. Toward publicly auditable secure cloud data storage services. IEEE Network, vol. 24, no. 4, 2010.
3	Articles from selected IEEE/ACM magazines, journals, conference proceedings, will further be provided when necessary.