UNIVERSITY of NICOSIA

Course Syllabus

Course Code	Course Title	ECTS Credits
COMP-552DL	Data Privacy and Ethics	10
Prerequisites	**Department**	**Semester**
None	Computer Science	FALL
Type of Course	**Field**	**Language of Instruction**
Elective	Data Science	English
Level of Course	**Lecturer(s)**	**Year of Study**
2nd Cycle	Dr Thomas Liebig	1st
Mode of Delivery	**Work Placement**	**Corequisites**
Distance Learning	N/A	None

Course Objectives:

The main objectives of the course are to:

- Learning the Challenges of Data Privacy
- Present Knowledge on Privacy-preserving methods for data storage/transmission/analysis and reports
- Explain the Privacy-by-design in analytics methods
- Introduce Ethical Questions regarding data privacy
- Explain how Privacy can be achieved in the data stream setting.
- Introduce Applied Privacy preserving methods.
- Present Laws and legislative regulations relative to data issues.
- Present the Ethical assessment process.

Learning Outcomes:

After completion of the course students are expected to be able to:

- Explain and Interpret the multiple privacy challenges involved in storing, processing and modelling Big Data, data streams or episodic data.
- Recall principles of data protection
- Explain Differential Privacy
- Outline Secret Sharing methods
- Discuss cryptographic principles
- Implement and make informed judgements on privacy preserving techniques
- Perform a privacy assessment of a software system

Course Content:

1. Introduction to Data Privacy
    a. Re-identification risks
    b. Levels and notion of data privacy
    c. Taxonomy of privacy definitions
2. Privacy via Aggregation
    a. Data aggregation methods
    b. Data Utility with aggregation
    c. Label proportions
3. Privacy via Secret Sharing
    a. Multi-party computation
    b. Privacy preserving vertical k-means
    c. Privacy preserving horizontal k-means
4. Privacy via Sketches
    a. Streaming Algorithm
    b. Lossy Counting
    c. Reservoir Sampling
    d. Count-Min Sketches
    e. Flajolet-Martin Sketches
5. Privacy via Data Perturbation
    a. Filtering
    b. Simplification
    c. Generalization
6. Privacy via Differential Privacy
    a. Concept of Differential Privacy
    b. Laplacian Noise
    c. Privacy preserving data publication
7. Fundamentals of Cryptography
    a. Discrete logarithm
    b. Discrete roots
    c. Extended Euclidian algorithm
    d. Chinese Remainder theorem
8. Privacy via Cryptography
    a. Symmetric vs asymmetric cryptography
    b. Hash functions
    c. RSA
9. Privacy via Homomorphic Encryption
    a. Paillers Homomorphic Encryption Scheme
    b. Shamir's Secret Sharing
    c. E-voting systems
10. Application Domains and Ethics
    a. Domain specific ethical privacy questions

UNIC

b. Domain specific solutions
11. Ethics and Law
    a. GDPR
    b. UNDG
12. Ethics and Big Data
    a. Assessment of data privacy and ethics
    b. Awareness for ethical challenges from big data

Learning Activities and Teaching Methods:

Lectures, Exercises, Lab Sessions, Case-Study Presentations, Discussions.

Assessment Methods:

Final Assessment*, Homework, Lab Reports.

* The Final Assessment can be either a Final Exam or Final Assignment(s) with Viva

Required Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Privacy-aware knowledge discovery: novel applications and new techniques	Bonchi, Francesco, and Elena Ferrari	CRC	2010	978-1-439-80365-3
Report on Data Privacy*	Thomas Liebig, Katharina Morik	Tech Report	2017	

* Made freely available online: http://www.thomas-liebig.eu/wordpress/wp-content/papercite-data/pdf/vaveld41.pdf

Recommended Textbooks / Readings:

Title	Author(s)	Publisher	Year	ISBN
Mobility, Data Mining and Privacy	Giannotti, Fosca, Pedreschi, Dino	Springer	2008	978-3-540-75177-9