Course Title	Data Privacy in the era of Data Mining and AI				
Course Code	CYS633				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	1st or 2nd Year / 2nd or 3rd Semester				
Teacher's Name	TBA				
ECTS	8	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide a comprehensive overview of growing data privacy threats to future communication technologies and Internet of Things (IoT) applications such as the Smart Grid and Smart Cities, e-Health and Wireless Sensor Technologies. Recent advances in the technical ICT fields of pervasive communications, combined with the science of big data mining and machine learning, are continuously transforming the way we interact with each other, with physical devices and infrastructures. Such technologies are becoming more tightly intertwined with our daily activities and we are becoming more integrated into the cyber-physical systems that surround us. The positive (economic) impact on society of such advances is enormous; however, big data information flows exposes important privacy details of our daily lives and our behavioural patterns. Such information may potentially be abused for purposes ranging from digital identity theft to targeted marketing, or discrimination based on medical history or other digital footprints, leading to fundamental privacy concerns. On this basis, the objectives of this course further include: a) Understanding interdisciplinary aspects of data handling and cyber security solutions: ultimately, this involves modelling and defining the trade-off between privacy and utility in information sharing IoT scenarios, in a mathematically rigorous way. b) Familiarise with fundamental data mining and machine learning algorithms with a focus on their application as privacy-invasive technologies. c) Learn how to develop application-specific privacy enhancing techniques, including security layers such as intrusion detection, privacy-by-design methods, and privacy-aware sensing.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Understand privacy-by-design principles.				

	• Get an overview of EU legislative and business regulatory aspects of data handling. • Use cyber security protocols to engineer holistic data privacy system solutions. • Apply fundamental data mining and activity recognition algorithms to run privacy-invansive security tests. • Understand the principles of differential privacy and implement privacy-preserving algorithms. • Design privacy solutions for IoT scenarios, including Smart Grid, Smart Cities and wearable sensor technologies.		
Prerequisites	None	Co-requisites	None
Course Content	IoT scenarios and privacy concerns: Smart meter data collection, wearable and smartphone mobile sensing technologies, data handling and data linking potential risks and system-level analysis. Mathematical privacy metrics and privacy invasion tools: relative entropy, mutual information, cluster classification, regression analysis, residual features, activity recognition, non-intrusive appliance load monitoring, exploratory data mining, differential privacy and atypicality. Cyber-security privacy protection solutions: anonymisation with trusted third party, data aggregation, data splitting, secure multi-party communication protocols, homomorphic encryption, zero-proof cryptosystem, data obfuscation, physical behaviour optimisation. Information-theoretic privacy preserving techniques: privacy-utility trade-off optimisation, privacy-aware data sensing, lossy data compression, rate-distortion function, differentially private billing. Standardisation, regulatory and business aspects: consent-based approaches, ethical aspects of data collection, access control restrictions, business requirements and risks. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical privacy scenarios and IoT considerations.		
Teaching Methodology	Face – to – face		
Bibliography	*Larry L Peterson and Bruce S Davie, Computer Networks: A Systems Approach. Morgan Kaufman, 5th edition, 2011.*		

	Keith M Martin, Everyday Cryptography. Oxford University Press, 2012. *Agrawal, Rakesh and Srikant, Ramakrishnan, Privacy-preserving Data Mining, SIGMOD Rec., vol. 29, no. 2, pp. 439-450, June 2000.* *Hall, Mark and Frank, Eibe and Holmes, Geoffrey and Pfahringer, Bernhard and Reutemann, Peter and Witten, Ian H., The WEKA Data Mining Software: An Update, SIGKDD Explor. Newsl., vol. 11, no. 1, pp. 10-18, June 2009.* *Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity. CRC press, May 2011.*
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English