COURSE DESCRIPTION FORM	
Course Code and Name	CENG444 ARTIFICIAL INTELLIGENCE SECURITY (TECH. ELECT.)
Course Semester	8
Catalogue Data of the Course (*Course Content*)	Types of attacks on artificial intelligence, attacks on classification, threats to model privacy, adversarial example generation techniques, threat modeling and attack simulation, measuring and evaluating attack impact, secure learning, privacy-preserving learning, adversarial training and model ensembles.
Course Textbooks	Adversarial Learning and Secure AI by David J. Miller, Zhen Xiang, George Kesidis, Cambridge University Press, 2023.
Supplementary Textbooks	Adversarial Machine Learning (1st Edition) by Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, J. D. Tygar, Cambridge University Press, 2019. Adversarial Machine Learning by Yevgeniy Vorobeychik, Murat Kantarcioglu, Springer, 2018.
Credit (*ECTS*)	6
Prerequisites for the Course (*Attendance Requirements*)	No prerequisite. %70 attendance is required.
Course Type	Technical elective
Language of Instruction	English
Course Objectives	This course is aimed to introduce the threats to and attacks on the security of artificial intelligence models, to comparatively explain the methods that can be used to develop models resistant to these attacks, and to enable students to develop more secure artificial intelligence models.
Course Learning Outcomes	Students taking this course 1. Understand security problems related to artificial intelligence models, 2. Apply attacks against artificial intelligence models, 3. Analyze the resistance of artificial intelligence models against attacks, 4. Compare approaches to developing artificial intelligence models that are resistant to attacks, 5. Use methods that increase artificial intelligence security.
Instruction Method *(Face-to-face, Distance education etc.)*	Face to face
Weekly Schedule of the Course	Week 1: Fundamentals of artificial intelligence Week 2: Fundamentals of cyber security Week 3: Data and database security Week 4: Artificial neural networks Week 5: Deep learning algorithms Week 6: Types of attacks against artificial intelligence Week 7: Attacks on classification – Evasion Week 8: Attacks on classification – Poisoning Week 9: Threats to model privacy Week 10: Adversarial example generation techniques (FGSM, PGD, C&W) Week 11: Threat modeling and attack simulation Week 12: Measuring and evaluating attack impact Week 13: Defense – secure learning and privacy-preserving learning Week 14: Defense – adversarial training and model ensembles
Teaching Activities *(The time spent for the activities listed here will determine the amount of credit required)*	Weekly theoretical course hours: 3 Reading activities Internet search and library work Designing and implementing materials Making a report Preparing and making presentations Midterm and revision for midterm Final exam and revision for final exam

Assessment Criteria

	Number(s)	Weight (%)
Midterm exam	1	20
Assignment	2	20
Application		
Project	1	20
Practice		
Quiz		
Final exam		40
Total		100

Workload of the Course

Activity	Number of Weeks	Duration (Weekly Hour)	End of Semester Total Workload
Weekly theoretical course hours	14	3	42
Weekly practical course hours			
Reading activities	14	2	28
Internet search and library work	14	2	28
Designing and implementing materials	6	4	24
Making a report	2	4	8
Preparing and making presentations	1	4	4
Midterm and revision for midterm	1	10	10
Final exam and revision for final exam	1	12	12
Total workload			156
Total workload/ 25			6,24
Course Credit (ECTS)			6

Contribution Level between Course Outcomes and Program Outcomes

No	Program Outcomes	1	2	3	4	5
1	Knowledge of mathematics, science, basic engineering, computing, and computer engineering; ability to use this knowledge in solving complex engineering problems.					X
2	Ability to define, formulate and analyze complex engineering problems using basic science, mathematics and engineering knowledge and considering the UN Sustainable Development Goals relevant to the problems addressed.					X
3	Ability to design creative solutions to complex engineering problems; ability to design complex systems, processes, devices, software, algorithms or products to meet current and future requirements, considering realistic constraints and conditions.					X
4	Ability to select, use and develop appropriate techniques, resources and modern engineering and informatics tools, including estimation and modeling, for the analysis and solution of complex engineering problems while being aware of their limitations.					X
5	Ability to use research methods to examine complex engineering problems or research topics in computer engineering, including reviewing the literature, designing experiments, conducting experiments, collecting data, analyzing and interpreting results.					X
6	Knowledge of the effects of engineering practices and the standards used in these			X		

		practices on society, health and safety, economy, sustainability and environment within the scope of the UN Sustainable Development Goals; awareness of the consequences of engineering solutions in the fields of information security and law.					
	7	Acting in accordance with engineering professional principles and knowledge on ethical responsibility; awareness of acting impartially, without discrimination on any issue, and being inclusive of diversity.			X		
	8	Ability to work effectively individually and as a team member or leader in intradisciplinary and multidisciplinary teams (face-to-face, remote, or hybrid).			X		
	9	Ability to conduct effective verbal and written communication on technical issues in Turkish or English, prepare reports, make effective presentations and prepare software documentation, considering the various differences of the target audience (such as education, language, profession).			X		
	10	Knowledge of business practices such as project, risk and change management and economic feasibility analysis; awareness of entrepreneurship and innovation.		X			
	11	Lifelong learning skill that includes the ability to learn independently and continuously, to adapt to new and developing scientific practices and technologies, and to think inquisitively about technological changes.		X			

Lecturer(s) and Contact Information	Assoc. Prof. Dr. Mehmet DEMİRCİ mdemirci@gazi.edu.tr