Ek 8. Ders Tanımlama Formu ***(Değişik: Gazi Üniversitesi Senatosunun 20/05/2021 tarihli ve 10 sayılı toplantısı, 2021/127 sayılı karar)***

DERS TANIMLAMA FORMU	
Dersin Kodu ve Adı	BM444 YAPAY ZEKÂ GÜVENLİĞİ (TEK. SEÇ.)
Dersin Yarıyılı	8
Dersin Katalog Tanımı (*İçeriği*)	Yapay zekâya yönelik saldırı türleri, sınıflandırmaya yönelik saldırılar, model gizliliğine yönelik tehditler, aldatıcı örnek üretme teknikleri, tehdit modelleme ve saldırı benzetimi, saldırı etkisini ölçme ve değerlendirme, güvenli öğrenme, mahremiyet koruyan öğrenme, çekişmeli eğitim ve model toplulukları
Temel Ders Kitabı	Adversarial Learning and Secure AI by David J. Miller, Zhen Xiang, George Kesidis, Cambridge University Press, 2023.
Yardımcı Ders Kitapları	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.
Dersin Kredisi (*AKTS*)	6
Dersin Önkoşulları (*Ders devam zorunlulukları, bu maddede belirtilmelidir.*)	Ön koşulu yoktur. %70 devam zorunluluğu vardır.
Dersin Türü	Teknik seçmeli
Dersin Öğretim Dili	Türkçe
Dersin Amacı ve Hedefi	Bu derste yapay zekâ modellerinin güvenliğine yönelik tehditleri ve saldırı türlerini tanıtmak, bu saldırılara karşı dirençli modeller geliştirmekte kullanılabilecek yöntemleri karşılaştırmalı olarak anlatmak ve öğrencilerin daha güvenli yapay zekâ modelleri geliştirmesini sağlamak hedeflenmektedir.
Dersin Öğrenim Çıktıları	Bu dersi alan öğrenciler 1. Yapay zekâ modellerine ilişkin güvenlik problemlerini anlar, 2. Yapay zekâ modellerine yönelik saldırıları uygular, 3. Yapay zekâ modellerinin saldırılara karşı direncini analiz eder, 4. Saldırılara dirençli yapay zekâ modeli geliştirme yaklaşımlarını karşılaştırır, 5. Yapay zekâ güvenliğini artıran yöntemleri kullanır.
Dersin Veriliş Biçimi *(Yüz yüze, Uzaktan vb.)*	Yüz yüze

Dersin Haftalık Dağılımı

1. Hafta: Yapay zekânın temelleri
2. Hafta: Siber güvenliğin temelleri
3. Hafta: Veri ve veritabanı güvenliği
4. Hafta: Yapay sinir ağları
5. Hafta: Derin öğrenme algoritmaları
6. Hafta: Yapay zekâya yönelik saldırı türleri
7. Hafta: Sınıflandırmaya yönelik saldırılar – Kaçınma
8. Hafta: Sınıflandırmaya yönelik saldırılar – Zehirleme
9. Hafta: Model gizliliğine yönelik tehditler
10. Hafta: Aldatıcı örnek üretme teknikleri (FGSM, PGD, C&W)
11. Hafta: Tehdit modelleme ve saldırı benzetimi
12. Hafta: Saldırı etkisini ölçme ve değerlendirme
13. Hafta: Savunma – güvenli öğrenme ve mahremiyet koruyan öğrenme
14. Hafta: Savunma – çekişmeli eğitim ve model toplulukları

Öğretim Faaliyetleri
(Burada belirtilen faaliyetler için harcanan zaman krediyi belirleyecektir. Dikkatli doldurulması gerekmektedir.)

Haftalık teorik ders saati: 3
Okuma faaliyetleri
İnternetten tarama, kütüphane çalışması
Materyal tasarlama, uygulama
Rapor hazırlama
Sunu hazırlama ve sunum
Ara sınav ve ara sınava hazırlık
Yarıyıl sonu sınavı ve yarıyıl sonu sınavına hazırlık

Değerlendirme Ölçütleri
(Toplam katkı yüzdesi 100 olacak şekilde ayarlanmalıdır.)

	Sayısı	**Katkısı (%)**
Ara sınav	1	20
Ödev	2	20
Uygulama		
Projeler	1	20
Pratik		
Kısa sınav		
Yarıyıl sonu sınavı		40
Toplam		100

Dersin İş Yükü

Etkinlik	**Toplam Hafta Sayısı**	**Süre (Haftalık Saat)**	**Dönem Sonu Toplam İş Yükü**
Haftalık teorik ders saati	14	3	42
Haftalık uygulamalı ders saati			
Okuma faaliyetleri	14	2	28
İnternetten tarama, kütüphane çalışması	14	2	28
Materyal tasarlama, uygulama	6	4	24
Rapor hazırlama	2	4	8
Sunu hazırlama ve sunum	1	4	4
Ara sınav ve ara sınava hazırlık	1	10	10
Final sınavı ve final sınavına hazırlık	1	12	12
Toplam iş yükü			156
Toplam iş yükü/ 25			6,24
Dersin AKTS Kredisi			6

Ders Çıktıları ile Program Çıktıları Arasındaki Katkı Düzeyi

No	Program Çıktıları	1	2	3	4	5
1	Matematik, fen bilimleri, temel mühendislik, bilgisayarla hesaplama ve bilgisayar mühendisliği disiplinine özgü konularda bilgi; bu bilgileri, karmaşık mühendislik problemlerinin çözümünde kullanabilme becerisi.					X

	2	Karmaşık mühendislik problemlerini, temel bilim, matematik ve mühendislik bilgilerini kullanarak ve ele alınan problemle ilgili BM Sürdürülebilir Kalkınma Amaçlarını gözeterek tanımlama, formüle etme ve analiz becerisi.					X
	3	Karmaşık mühendislik problemlerine yaratıcı çözümler tasarlama becerisi; karmaşık sistemleri, süreçleri, cihazları, yazılımları, algoritmaları veya ürünleri gerçekçi kısıtları ve koşulları gözeterek, mevcut ve gelecekteki gereksinimleri karşılayacak biçimde tasarlama becerisi.					X
	4	Karmaşık mühendislik problemlerinin analizi ve çözümüne yönelik, tahmin ve modelleme de dâhil olmak üzere, uygun teknikleri, kaynakları ve modern mühendislik ve bilişim araçlarını, sınırlamalarının da farkında olarak seçme, kullanma ve geliştirme becerisi.					X
	5	Karmaşık mühendislik problemlerinin veya bilgisayar mühendisliği alanındaki araştırma konularının incelenmesi için literatür araştırması, deney tasarlama, deney yapma, veri toplama, sonuçları analiz etme ve yorumlama dahil, araştırma yöntemlerini kullanma becerisi.					X
	6	Mühendislik uygulamaları ve bu uygulamalarda kullanılan standartların BM Sürdürülebilir Kalkınma Amaçları kapsamında, topluma, sağlık ve güvenliğe, ekonomiye, sürdürülebilirlik ve çevreye etkileri hakkında bilgi; mühendislik çözümlerinin bilgi güvenliği ve hukuk alanlarında doğurduğu sonuçlar konusunda farkındalık.				X	
	7	Mühendislik meslek ilkelerine uygun davranma, etik sorumluluk hakkında bilgi; hiçbir konuda ayrımcılık yapmadan, tarafsız davranma ve çeşitliliği kapsayıcı olma konularında farkındalık.				X	
	8	Bireysel olarak ve disiplin içi ve çok disiplinli takımlarda (yüz yüze, uzaktan veya karma) takım üyesi veya lideri olarak etkin biçimde çalışabilme becerisi.				X	
	9	Hedef kitlenin çeşitli farklılıklarını (eğitim, dil, meslek gibi) dikkate alarak, teknik konularda Türkçe veya İngilizce sözlü, yazılı etkin iletişim kurma, rapor hazırlama, etkili sunum yapma ve yazılım dokümantasyon hazırlama becerisi.				X	
	10	Proje, risk ve değişiklik yönetimi ve ekonomik yapılabilirlik analizi gibi iş hayatındaki uygulamalar hakkında bilgi; girişimcilik ve yenilikçilik hakkında farkındalık.			X		
	11	Bağımsız ve sürekli öğrenebilme, yeni ve gelişmekte olan bilimsel uygulamalara ve teknolojilere uyum sağlayabilme ve teknolojik değişimlerle ilgili sorgulayıcı			X		

		düşünebilmeyi kapsayan yaşam boyu öğrenme becerisi.					
Dersi Verecek Öğretim Eleman(lar)ı ve İletişim Bilgileri	Doç. Dr. Mehmet DEMİRCİ mdemirci@gazi.edu.tr						