İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Bilgi Güvenliği alanında Makine Öğrenmesi Yöntemleri	Machine Learning Methods in Security

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 601E	Güz/Bahar (Fall/Spring)	3	7,5	Dr. (Ph.D.)

Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	İngilizce/Türkçe (English/Turkish)

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Makine öğrenmesi temel konuları, Karar ağaçları, Yapay Sinir ağları, Bulanık mantık, Genetik algoritmalar, Naive Bayes yöntemi, Destek vektör makineleri, Rastgele koşullu alanlar gibi makine öğrenmesi yöntemlerinin bilgi güvenliği alanında kullanım olanakları ve yöntemleri
	Fundamental topics in machine learning. Decision tree. Neural networks. Fuzzy logic. Genetic algorithms. Naïve-Bayes method. Support vector machines. Application of machine learning topics to information security.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	• Makine öğrenmesi yöntemlerinin bilgisayar güvenliğine uygulanabileceği alanların araştırılması • Makine öğrenmesinin temellerinin anlatılması
	• Searching possible areas of computer security that machine learning can be utilized • Teaching the fundamentals of machine learning.
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Öğrenciler makine öğrenmesi ilkelerini öğreneceklerdir. 2. Öğrenciler makine öğrenmesi ilkeleri uyarınca güvenliği iyileştirebilecek yorumlar yapabileceklerdir. 3. Öğrenciler bilgi güvenliğinin çeşitli alanlarında makine öğrenmesi kullanarak yeni ve daha verimli yöntemler geliştirebileceklerdir. 4. Öğrenciler güncel yayınları izleyebileceklerdir.
	1. Students will learn principles of machine learning 2. Students will be able to propose enhancing solutions to security based on machine learning 3. Students will be able to develop new and more efficient methods based on machine learning in several areas of information security 4. Students will be able to follow recent academic literature

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1. Machine Learning: The Art and Science of Algorithms that Make Sense of Data, Peter Flach, 2012, Cambridge University Press. 2. Introduction to Machine Learning, 2nd Ed., Ethem Alpaydın, 2009, The MIT Press. 3. Machine Learning and Data Mining for Computer Security: Methods and Applications, 2006 Ed., Marcus A. Maloof, 2012, Springer. 4. Machine Learning in Cyber Trust: Security, Privacy, and Reliability, 2009 Ed., Jeffrey J. P. Tsai, Philip S. Yu, 2009, Springer. 5. Machine Learning Forensics for Law Enforcement, Security, and Intelligence, Jesus Mena, 2011, Auerbach Publications.
Ödevler ve Projeler **(Homework & Projects)**	1 Dönem Ödevi 1 Term Paper
Laboratuar Uygulamaları **(Laboratory Work)**	-- --
Bilgisayar Kullanımı **(Computer Use)**	-- --
Diğer Uygulamalar **(Other Activities)**	-- --

Başarı Değerlendirme Sistemi

(Assessment Criteria)

Faaliyetler (Activities)	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
Yıl İçi Sınavları (Midterm Exams)	1	% 30 (30 %)
Kısa Sınavlar (Quizzes)	-	-
Ödevler (Homework)	-	-
Projeler (Projects)	-	-
Dönem Ödevi/Projesi (Term Paper/Project)	1	% 30 (30%)
Laboratuar Uygulaması (Laboratory Work)	-	-
Diğer Uygulamalar (Other Activities)	-	-
Final Sınavı (Final Exam)	1	% 40 (40%)

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Giriş ve dersin tanıtımı	
2	Makina öğrenmesi temelleri	
3	Karar ağaçları	
4	Yapay sinir ağları	
5	Bulanık mantık	
6	Genetik ve doğa esinli algoritmalar	
7	Naive Bayes yöntemi	
8	Diğer güncel makina öğrenmesi yöntemleri	
9	Anomali saptamada makina öğrenmesinin kullanımı	
10	Bilgi sınıflandırmada makina öğrenmesinin kullanımı	
11	Saldırı önleme dizgelerinde makina öğrenmesinin kullanımı	
12	Güvenlik politikalarının ödünleştirilmesinde makina öğrenmesi	
13	Güncel yayınlar	
14	Güncel konular üzerine tartışma	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Course outline and introduction	
2	Foundations of machine learning	
3	Decision trees	
4	Neural networks	
5	Fuzzy logic	
6	Genetic and nature inspired algorithms	
7	Naïve-Bayes method	
8	Other up-to-date machine learning methods	
9	Usage of machine learning in anomaly detection	
10	Usage of machine learning in information classification	
11	Usage of machine learning in intrusion prevention systems	
12	Usage of machine learning in trade-off of the security policies	
13	Paper discussion	
14	Discussion on the recent work	

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Doktora Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).	X		
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).			X
iii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).		X	
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).			X
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).	X		
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	X		
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).	X		
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).	X		
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).			X
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).		X	

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Information Security and Crypyography Graduate (PhD) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).	X		
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).			X
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).		X	
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).			X
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).	X		
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).	X		
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).	X		
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).	X		
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).			X
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).		X	

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Prof. Dr. Eşref ADALI	31.03.2014	