T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ADLİ BİLİŞİM ANABİLİM DALI
ADLİ BİLİŞİM BİLİM DALI

YALOVA İLİ BİLİŞİM SUÇ TÜRLERİNİN YAPAY ZEKÂ YÖNTEMİYLE TAHMİNİ

YÜKSEK LİSANS TEZİ

Sezer YURDUSEVEN

TEZ DANIŞMANI: Dr. Öğr. Üyesi Güneş HARMAN

YALOVA
TEMMUZ 2024

T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ADLİ BİLİŞİM ANABİLİM DALI
ADLİ BİLİŞİM BİLİM DALI

YALOVA İLİ BİLİŞİM SUÇ TÜRLERİNİN YAPAY ZEKÂ YÖNTEMİYLE TAHMİNİ

YÜKSEK LİSANS TEZİ

Sezer YURDUSEVEN
228101001

DANIŞMAN: Dr. Öğr. Üyesi Güneş HARMAN

YALOVA
TEMMUZ 2024

ETİK BEYAN

Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Kuralları'na uygun olarak hazırladığım "YALOVA İLİ BİLİŞİM SUÇ TÜRLERİNİN YAPAY ZEKÂ YÖNTEMİYLE TAHMİNİ" başlıklı bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir, aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi taahhüt ve beyan ederim.

Sezer YURDUSEVEN

ÖNSÖZ

Yüksek lisans eğitimim boyunca benden yardımlarını esirgemeyen, akademik anlamda bana her zaman destek olan ve doğru yolu gösteren sayın danışman hocam Dr.Öğr.Üyesi Güneş HARMAN'a teşekkür ederim. Hem ders günlerinde hem de tez hazırlık süreçlerinde çalışmalarıma devam edebilmem için her türlü fedakarlığı ve desteği sağlayan eşim Beyza YURDUSEVEN'e, tecrübeleri ile bana destek olan mesai arkadaşım Sefer MADEN'e teşekkürlerimi sunarım.

Temmuz– 2024 Sezer YURDUSEVEN

İÇİNDEKİLER

ETİK BEYAN i
ÖNSÖZ ii
İÇİNDEKİLER iii
KISALTMALAR LİSTESİ iv
TABLOLAR LİSTESİ v
ŞEKİLLER LİSTESİ vi
ÖZET vii
ABSTRACT viii
1. GİRİŞ 1
1.1. Tezin Amacı/Hipotez 2
2. BİLİŞİM SUÇLARI 4
2.1. Bilişim Yoluyla İşlenen Suçların Yapısı 5
2.2. Bilişim Suçu Türleri 6
2.3. Bilişim Suçlarının Tespiti Maksadıyla Yapılan Araştırma Türleri 7
2.3.1. Açık kaynak araştırması 7
2.3.2. Bilgi çarpıtma (dezenformasyon) araştırması 7
2.3.3. Derin sahte (deepfake) araştırması 8
2.4. TCK'da Düzenlenen Bilişim Suçları 9
3. LİTERATÜR ARAŞTIRMASI 10
4. YALOVA İLİNDE MEYDANA GELEN ADLİ BİLŞİM SUÇLARININ DEĞERLENDİRİLMESİ 15
4.1. Bilişim Suçlarında Makine Öğrenmesi Uygulamaları 16
4.1.1. Makine öğrenmesi algoritmaları 17
4.1.2. Performans metrikleri 23
4.2. Sistem Metotları 25
4.3. Veri Analizi 26
5. BULGULAR 40
6. SONUÇLAR VE ÖNERİLER 51
KAYNAKLAR 54
ÖZGEÇMİŞ 57

KISALTMALAR LİSTESİ

Çok Katmanlı YSA	: Çok Katmanlı Yapay Sinir Ağları
DVM	: Destek Vektör Makineleri
E Devlet	: Elektronik Devlet
E İmza	: Elektronik İmza
ESA	: Evrişimli Sinir Ağları
IBK	: K- En Yakın Komşular Algoritması
TCK	: Türk Ceza Kanunu
YSA	: Yapay Sinir Ağları

TABLOLAR LİSTESİ

Tablo 4.1. Yalova ili nüfusu 16
Tablo 4.2. Karışıklık (confusion) matrisi 23
Tablo 5.1. DVM algoritması performans değerleri 40
Tablo 5.2. Çok katmanlı YSA algoritması performans değerleri 41
Tablo 5.3. RO algoritması performans değerleri 41
Tablo 5.4. IBK algoritması performans değerleri 41
Tablo 5.5. Sınıflandırma algoritmalarının performans değerleri karşılaştırması 42
Tablo 5.6. Bilişim suçu türlerine ait DVM algoritması performans değerleri 43
Tablo 5.7. Bilişim suçu türlerine ait çok katmanlı YSA algoritması performans değerleri 45
Tablo 5.8. Bilişim suçu türlerine ait RO algoritması performans değerleri 47
Tablo 5.9. Bilişim suçu türlerine ait IBK algoritması performans değerleri 49

ŞEKİLLER LİSTESİ

Şekil 2.1. Açık kaynak istihbaratı 7
Şekil 4.1. Yalova ilçeleri 15
Şekil 4.2. Uygulanan metot 25
Şekil 4.3. Veri setine ait özellikler 27
Şekil 4.4. Meydana gelen bilişim suçu olaylarının yıllara göre dağılım oranları 28
Şekil 4.5. Bilişim suçu olaylarının yıllara göre dağılımı 28
Şekil 4.6. Bilişim suçu türlerinin dağılımı 29
Şekil 4.7. Bilişim suçlarına karışan kişilerin cinsiyet dağılım ve oranları 30
Şekil 4.8. Medeni durum dağılımı 31
Şekil 4.9. Bilişim suçlarına karışan kişilerin yaş grupları 32
Şekil 4.10. Bilişim suçları içerisindeki cinsiyet dağılımı ve sayıları 33
Şekil 4.11. Veri seti içerisindeki kişilerin eğitim durumları 35
Şekil 4.12. Yalova ili ilçelerinde meydana gelen bilişim suçlarının dağılımı 37
Şekil 4.13.Yalova ilçelerinde meydana gelen bilişim suçlarının meslek dağılımı….38
Şekil 4.14. Bilişim suçlarına karışan kişilerin olay taraf dağılım ve oranları……...39
Şekil 5.1. DVM algoritması çok sınıflı ROC eğrileri 44
Şekil 5.2. Çok katmanlı YSA algoritması çok sınıflı ROC eğrileri 46
Şekil 5.3. RO algoritması çok sınıflı ROC eğrileri 48
Şekil 5.4. IBK algoritması çok sınıflı ROC eğrileri 50

YALOVA İLİ BİLİŞİM SUÇ TÜRLERİNİN YAPAY ZEKÂ YÖNTEMİYLE TAHMİNİ

ÖZET

Çağımız dünyasında gelişen teknolojilerle birlikte meydana gelen bilişim suçu türlerinin de hızla arttığı gözlenmektedir. Yeterli eğitim düzeyine sahip olmayan kişilerin birbirleri ile etkileşim içerisinde bulunmaları bilişim suç oranlarını arttırmaktadır. Artan suç oranlarıyla birlikte Yalova ilinde bulunan kişiler ve kullanılmakta olan dijital cihazlar her an tehdit altında bulunmaktadır. İşlenmekte olan suç çeşitliliğinin artması gerek hukuki altyapıyı gerekse kolluk birimlerinin işlerini zorlaştırmakta, elde edilen adli dijital verilerin artması analiz ve raporlama gibi süreçlerin uzamasına sebep olmaktadır. Bu çalışmada, 2020-2023 yılları arasında Yalova Cumhuriyet Başsavcılığı'na intikal etmiş bilişim suçları makine öğrenmesi algoritmaları kullanılarak yorumlanmaya çalışılmıştır. Aynı zamanda sonuçlar doğrultusunda, meydana gelmesi olası bilişim suçu türleri ile olaylara müdahil olan kişi profillerinin tespiti yapılmaya çalışılmıştır.

Çalışma kapsamında toplam 2500 adet veri üzerinden 11 adet öznitelik belirlenmiştir. Kullanılan veri seti üzerinde Rastgele Orman (RO), Destek Vektör Makineleri (DVM), Çok Katmanlı Yapay Sinir Ağları (Çok Katmanlı YSA), K-En Yakın Komşular (IBK) gibi makine öğrenmesi algoritmaları kullanılarak performansları karşılaştırılmıştır.

Kullanılan makine öğrenmesi algoritmalarının performans değerlendirmeleri karşılaştırıldığında bilişim suçu olaylarına karışan kişilerin müşteki (mağdur) mi yoksa şüpheli mi olduğuna karar verebilmek adına en iyi sonuç 0.83 doğruluk oranı ile DVM-Sigmoid algoritmasından alınmıştır.

Bilişim suçu türlerine ait makine öğrenmesi algoritmalarının performans değerlendirmeleri karşılaştırıldığında en iyi sonuç değeri 0.85 doğruluk oranıyla RO algoritmasından alınmıştır. RO algoritması içerisinde performans değerlendirmesi yapılan bilişim suçu türleriyle ilgili diğer performans değerlerine bakıldığında, en yüksek skor 0.90 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçundan alınmıştır.

Kullanılan veri seti üzerinde yapılan analizler; olaylara müdahil olan kişilerin genel olarak evli, erkek, ortaöğretim mezunu ve genç yaşta olduklarını göstermektedir. Sonuç olarak, Yalova ilinde meydana gelen bilişim suçu sayılarının artarak devam edeceği anlaşılmıştır.

Anahtar Kelimeler: Yalova ili, Bilişim suçları, Yapay zekâ

PREDICTION OF IT CRIME TYPES IN YALOVA PROVINCE USING ARTIFICIAL INTELLIGENCE METHOD

ABSTRACT

It is observed that the types of cybercrimes that occur with the developing technologies in our modern world are also increasing rapidly. Interaction between people who do not have sufficient education increases the cyber crime rates. With the increasing crime rates, people in Yalova province and the digital devices used are under threat at all times. The increase in the variety of crimes being committed complicates the work of both the legal infrastructure and law enforcement units, and the increase in forensic digital data obtained causes processes such as analysis and reporting to take longer. In this study, cyber crimes reported to the Yalova Chief Public Prosecutor's Office between 2020 and 2023 were tried to be interpreted using machine learning algorithms. At the same time, in line with the results, an attempt was made to determine the possible types of cyber crimes that may occur and the person profiles involved in the incidents.

Within the scope of the study, 11 attributes were determined from a total of 2500 data. Their performances were compared using machine learning algorithms such as Random Forest (RO), Support Vector Machines (SVM), Multilayer Artificial Neural Networks (Multilayer ANN), K-Nearest Neighbors (IBK) on the used data set.

When the performance evaluations of the machine learning algorithms used were compared, the best result was obtained from the SVM-Sigmoid algorithm with an accuracy rate of 0.83 in order to decide whether the people involved in cyber crime incidents are complainants (victims) or suspects.

When the performance evaluations of machine learning algorithms for cyber crime types were compared, the best result value was taken from the RO algorithm with an accuracy rate of 0.85. When we look at the other performance values related to the types of cyber crimes whose performance is evaluated within the RO algorithm, the highest score is 0.90, obtained from the crime of blocking, corrupting the information system, destroying or changing data.

Analyzes made on the data set used; It shows that the people involved in the incidents are generally married, male, secondary school graduates and young in age. As a result, it is understood that the number of cyber crimes occurring in Yalova province will continue to increase.

Keywords: Yalova province, Cyber crimes, Artificial intelligence

1. GİRİŞ

Günümüzde bilişim ve iletişim alanlarındaki teknolojilerin hızla gelişmesiyle birlikte, bilişim kavramının önemi artmaya başlamıştır. Bu teknolojik ilerlemeler, bilişim teriminin günlük hayatta ve akademik çalışmalarda daha sık kullanılmasına yol açmıştır. Bilişimin gelişmeye başlamasıyla birlikte kendi iktisadi ve kültürel yeniliklerini oluşturmuş, tüm dünyanın haberleşmesinde kullandığı teknolojik sistemler sayesinde düzenli bir biçimde bilginin işlenmesini ve yönetilmesini öngören bir bilim dalı haline gelmiştir. Bilişim, teknoloji ile bilgi arasında bir köprü işlevi görmeye başlamış; veri toplama, saklama, işleme, iletişim kurma ve analiz etme süreçlerini kolaylaştırmıştır. Bu sayede, bireyler ve işletmeler verimliliklerini artırabilmiştir.

Gelişen teknoloji altyapısıyla birlikte bilgi teknolojileri hemen hemen her alanda yerini almıştır. Bu sayede erişimi zor olan yenilikler tüm insanlığın hizmetine sunularak hayatın kolaylaşmasına fayda sağlamıştır.

Bu süreçte teknolojiye ulaşmanın en kolay yolu olan internet kullanımı da ciddi oranda artmış bununla birlikte dijital ortamlarda işlenen suçlarda da artışlar meydana gelmiştir. Teknolojik yapıların artışının en büyük avantajı insan hayatını kolaylaştırmasıdır. Ancak en büyük dezavantajı da kötü niyetli tehdit unsurlarının birçok kaynağa erişim sağlamasına ve sistem hatalarından meydana gelen sistem açıklarına erişim sağlayıp, istismar etmesine olanak tanımıştır (Yılmaz ve diğ., 2016).

Teknolojik cihazların ve ağ teknolojilerinin yaygınlaşmasıyla birlikte, bu sistemleri kötü amaçları için kullanan kişiler ortaya çıkmıştır. Bu durum, bilişim suçları olarak adlandırılan suç türünün doğmasına yol açmıştır (Ermeydan, 2018). Bilişim suçlarının tüm yönleriyle incelenmesi ve şüphelilerin tespit edilmesinde adli bilişim en büyük destekleyici unsur olmuştur.

Adli bilişim, bilgisayar sistemleri üzerinde muhafaza edilen veya bu gibi alanlardan iletilen bilgilerin toplanıp incelenmesi ve raporlanmasını sağlayan bilim dalı olmasının yanı sıra belli bir bilgi, ilke ve disipline sahiptir (Bilgi Teknolojileri ve İletişim Kurumu, 2019). Diğer bir deyişle adli bilişim, meydana gelen bir bilişim suçu kapsamında bilişim ağlarında bulunan dijital delillere ulaşıldığı andan adli mercilere ulaştırılmasına kadar geçen sürecin bütünüdür.

Adli bilişim kavramının, kanuni uygulamalarından ziyade teknolojik boyutu ön plandadır. Bilişim sistemlerinden elde edilen delillerin ayrıştırılarak hukuki bir delil olma özelliğine dönüştürme süreci oldukça zordur. Aynı zamanda teknolojik altyapıya sahip teknik bilgi gerektiren bir iştir. Bu nedenle adli bilişim sürecinde çeşitli sorunlarla karşılaşılmaktadır. Bilişim suçlarında işlenen veri boyutlarının büyük olması, teknolojik altyapıların yetersizliği, bilgi teknolojilerindeki değişim ve yeniliklere karşı hukuki düzenlenmelerin yapılmasında geç kalınması bunların başlıcaları olarak sıralanabilir.

Adli bilişim incelemesi sürecinde kullanılan ve delil özelliği taşıyan verilerin, normal bir bilgisayar kullanıcısı tarafından tespit edilmesi mümkün değildir. Bu nedenle belli teknolojik altyapı ve bilgi birikimine sahip adli bilişim uzmanlarına gereksinim duyulmaktadır.

Adli bilişim uzmanın görevlerinden bazıları şunlardır;

- Teknolojik cihazlar içerisinde bulunan verileri kurtarmak ve yorumlamak,
- Elde edilen verilerin hukuki delil olarak kullanılmasını sağlamak,
- Meydana gelen bilişim suçları şüphelilerinin kimliğinin tespit edilmesine çalışmak,
- Adli delil niteliği taşıyan verilerin korunmasını sağlamak,
- Dijital materyallerde bulunan silinmiş verilerin kurtarılmasına yardımcı olmak,
- Adli süreç esnasında tanzim edilen raporların eksiksiz bir şekilde düzenlenmesini sağlamaktır.

Bu tez çalışması 6 bölümden oluşmaktadır. Çalışmanın ikinci bölümünde bilişim suçlarına yer verilmiştir. Tez çalışmasının üçüncü bölümünde literatür araştırması yapılmıştır. Bir sonraki bölüm olan dördüncü bölümde ise; tezin analizinde kullanılan makine öğrenmesi uygulamalarına, tekniklerine, sınıflandırma algoritmalarına, performans metriklerine ve sisteme ilişkin metot ile gerçekleştirilen uygulamalara yer verilmiştir. Çalışmanın beşinci bölümünde elde edilen bulgulara yer verilirken, çalışmanın son bölümünde sonuçlar ve önerilere çalışmanın bir parçası olarak yer verilmiştir.

1.1. Tezin Amacı/Hipotez

Adli bilişim suçlarıyla ilgili karşılaşılan sorunlar hakkında; adli bilişim uzmanlarıyla yapılan görüşmeler sonucunda, meydana gelen bilişim suçlarında genellikle delil niteliği taşıyan verilerde bulunan şifreleme algoritmalarının sürekli kendisini güncellediği görülmüştür. Ayrıca teknoloji sistemlerinin birbirleriyle belirli bir ekosistem içerisinde olması nedeniyle

delil niteliği taşıyan verilerin farklı cihazlar aracılığıyla kısmen veya tamamen silinmesi sorunlarıyla karşılaşılmıştır. Adli bilişim uzmanları meydana gelen bilişim suçu olaylarında şifreleme algoritmalarını genellikle genç nüfus ve eğitim seviyesi olarak ilköğretim seviyesinden yüksek kişiler tarafından kullanıldığını tespit ettiklerinden dolayı siber suçlar farkındalık ve bilinçlendirme seminer planlamalarında önceliği genellikle evli ve genç nüfusa verdiklerini dile getirmişlerdir.

Bu çalışmada, 2020-2023 yılları arasında Yalova ili Cumhuriyet Başsavcılığı'na intikal etmiş bilişim suçlarının analizi yapılmıştır. Çalışmada kullanılan veri setinin oluşturulması sırasında bilişim suçlarıyla ilgili, Yalova ilinde meydana gelen bilişim suçu türleri, bilişim suçlarına müdahil olan kişilerin genel özellikleri, bilişim suçları tespitinin nasıl yapıldığı, meydana gelen suçların aydınlatılma aşamaları, bilişim suçlarının ortaya çıkartılmasında ne tür bilgilere ihtiyaç duyulduğu, bilişim suçları analizinde kullanılan yöntemler hakkında bilgi alınmıştır. Alınan bilgiler doğrultusunda olay tarihi, olay ilçesi, suç türü, müşteki(mağdur), şüpheli, cinsiyet, yaş, medeni hal, meslek, uyruk, öğrenim durumu özelliklerini de kapsayacak şekilde düzenlenen toplam 2500 adet veri, özel hayatın gizliliğini ihlal etmeyecek şekilde hazırlanarak Yalova Cumhuriyet Başsavcılığı'ndan çalışmada kullanılmak üzere temin edilmiştir.

Gelişen teknolojiyle birlikte yapay zekâ tabanlı makine öğrenme algoritmaları karar verme mekanizması veya karar verme mekanizmasına yardımcı etken olarak kullanılmaktadır. Bu çalışmada çeşitli makine öğrenmesi algoritmaları kullanılarak yorumlanmaya çalışılmıştır. Sonuçlar doğrultusunda, meydana gelmesi olası bilişim suçu türleri ile olaylara müdahil olan kişi profillerinin tespiti yapılmaya çalışılmıştır.

Bu çalışmanın en önemli kazanımlarından biri gerçek veriler kullanarak bilişim suç türlerine göre alınması gereken tedbirler konusunda rehberlik etmesidir. Bu bağlamda tespiti yapılan sorunlarla, çalışmada elde edilen sonuçlara bakıldığında olaylara müdahil olan kişilerin genel olarak ortaöğretim mezunu ve genç yaşta olduğu görülmüştür. Adli delil niteliği taşıyan verilerin silinmesinden kaynaklı meydana gelen bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun ise çalışmada tespit edilen en yüksek doğruluk oranına sahip suç türü olduğu anlaşılmıştır.

2. BİLİŞİM SUÇLARI

Günümüzde bilişim sistemleri ile borsa, sosyal medya, dijital haberleşme, elektronik imza (e-imza), e-nabız, elektronik devlet (e-devlet) ve otonom araçlar gibi pek çok yenilik tüm insanlığın hayatını kolaylaştırmıştır. Bu sayede bilişim teknolojileri hayatın her alanında önemli bir yere sahip olmuştur. Gelişen teknolojilerin çok hızlı ve ulaşılabilir olması nedeniyle tüm insanlık tarafından daha fazla tercih edilir duruma gelmiştir. Bu teknolojilerin günümüz dünyasında böylesine vazgeçilmez bir unsur haline gelmesi meydana gelebilecek bilişim suçlarının çeşitliliğini de arttırmıştır. Bilişim suçları; bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde, gayri kanuni, gayri ahlaki veya yetki dışı olarak gerçekleştirilen her türlü davranış olarak tanımlanabilir (Kaçan, 2023).

Kanun koyucuların bilişim suçları konusunda gecikmeksizin harekete geçerek gerekli hukuki düzenlemeleri yapmaları gerekmektedir. Ancak gerek uluslararası hukuk gerekse Türk Ceza Kanunu (TCK) değişen ve gelişen çağa uyum sağlamakta zorluklar yaşamaktadır. Sosyal medya gibi platformlarda özel hayatın gizliliğine yapılan tecavüzler artmış ve bilgisayar korsanlarının yaygınlaşmasıyla kişisel veriler çalınarak insanların dolandırılmalarına sebep olmuştur (Kaçan, 2023). Aynı zamanda tüm dünyada çok önemli bir sorun olan terörizm faaliyetleri bilişim teknolojileri kullanılarak, sanal dünyaya taşınmış ve sempatizanlık kitlesini arttırmıştır.

Bilişim suçlarında, elektronik ve manyetik alanlara kaydedilen veriler dijital delil olarak adlandırılmaktadır. Dijital ortamda oluşturulmuş ve saklanmış her türlü belge, yazılım ve veri ceza yargılamasında delil olarak kullanılabilmektedir. Dijital delillerin farklı tipleri bulunmaktadır.

Bunlardan bazıları şunlardır;

- Veri dosyaları,
- Sunucu kayıt dosyaları,
- E-postalar,
- Fotoğraflar,
- Videolar,
- İnternet geçmişi,
- Web sayfaları şeklinde sıralanabilir (Dogan ve Dijle, 2011).

2.1. Bilişim Yoluyla İşlenen Suçların Yapısı

Bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçların meydana gelebilmesi için belirli bir bilgi birikimine sahip olunması gerekmektedir. Bilişim teknolojileri ile işlenen olayların içeriği ve işleniş biçimleri itibariyle diğer suç türlerine göre daha karmaşık yapıya sahiptir. Bilişim suçlarının müdahili olan mağdurlar her kesimden olabilirken, şüpheliler belli bir teknolojik altyapı ve bilgi birikimine sahip kişilerden oluşmaktadır.

Bilişim suçlarının genel ortak özellikleri;

- Suçun işlenmesinde dijital teknolojilerin kullanılması,
- Yeni suç türleri olması sebebiyle gerekli kanun ve düzenlemelerin yetersiz kalması,
- En az riskle yüksek kazanç elde edilmesine olanak sağlaması,
- Kanuni mevzuatlar yeterli olsa bile uygulamada yetersiz kalınması,
- Diğer suç türlerine kıyasla, bilişim suçlarının maddi ve manevi sonuçlarının daha ağır olması,
- Şüphelilerin işledikleri bilişim suçlarının cezai yaptırımlarının olmamasından cesaret alarak eylemlerinin cezasız kalacağına güvenmeleri,
- Mağdurların yeterli bilgi birikimine sahip olmaması,
- Mağdurların takip edilmesi gereken prosedürlere yeteri kadar hâkim olmaması,
- Mağdurların kamu kurumu ve kurumsal firmalar olması durumunda saygınlıklarını kaybetme düşüncesi,
- Şüphelilerin genellikle genç nüfusa sahip kişilerden oluşması,
- Suçun işleniş biçimlerinin çok hızlı değişip gelişebilmesi,
- Şüphelilerin çoğunluğunun işlenen suçların deşifre olmaması için ihbar edilmeyeceğini düşünmeleri,
- Ekonomik kaybın büyük olması durumunda mağdurların meydana gelen olayları güvenlik güçlerine bildirmemesi,
- Çevresel faktörlerin olumsuz etkileri,
- Şüphelilerin bireysel kişilerden oluşabileceği gibi organize suç şebekelerinden de oluşabilmesi,

- Bilişim suçları ile mücadelede bilinçlendirme çalışmalarının organize edilmesinin uzun bir süreç olarak görülmesi,
- Bilişim suçunun işleniş biçimiyle uluslararası boyutlara da taşınabilmesidir (Kaçan, 2023).

2.2. Bilişim Suçu Türleri

Bilişim teknolojilerindeki gelişmeler birçok alanda insanların yaşam şartlarını değiştirmiştir. Tüm bu ilerlemelerle birlikte bilişim teknolojileriyle ilişkili suç türleri de ortaya çıkmıştır (Er Avukatlık ve Hukuk Bürosu, 2022).

Meydana gelen bilişim suçlarının bazıları;

- Bilgisayar yoluyla dolandırıcılık
- Bilişim sistemleri ile sahtecilik
- Bilgisayar sabotajları
- Bilgisayar sistemlerine yetkisiz erişim
- Yazılımların izinsiz kullanılması
- Kişisel bilgileri ele geçirmek
- Kanuna aykırı yayınlar
- Terörizm faaliyetleri
- Teknoloji sistemleri yoluyla fuhuş
- Çocuk pornografisi
- Bilişim sistemleri yoluyla uyuşturucu satışı veya temini
- Kredi kartı bilgilerinin çalınması
- E-posta adresinin çalınması
- Yetkisiz dinleme
- Siber savaşlar
- Sahte hesap oluşturma
- Bilişim sistemleri yoluyla hakaret ve korkutmak
- Sahte evrak düzenlemek

- Hacking (Kaçan, 2023; Kalemci, 2021).

2.3. Bilişim Suçlarının Tespiti Maksadıyla Yapılan Araştırma Türleri

Bilişim teknolojilerinin hızla gelişmesiyle birlikte bilişim suç çeşitliliği ve oranlarında da artışlar gözlemlenmektedir. Tüm dünyada olduğu gibi Türkiye de hızla gelişen bu çağa ayak uydurabilmek için hukuki altyapısını sürekli güncellemektedir ve meydana gelen bilişim suçlarının tüm maddi delilleriyle doğru bir şekilde adli mercilere sunulmasını sağlamaya çalışmaktadır. Bilişim suçlarının tespiti için yapılan araştırma türlerinin bazıları şunlardır;

2.3.1. Açık kaynak araştırması

Açık kaynak şekil 2.1'de gösterildiği gibi, herkes tarafından incelenebilen, düzenlenebilen ve geliştirilebilen veriler bütünü olup, genellikle ücretsiz olarak kullanılmaktadır. Bu tür yazılımlar açık ve şeffaf olması nedeniyle kullanıcılarına iyi bir güvenlik ve yenilikçilik sağlar. Açık kaynak istihbaratı genellikle televizyon, gazete, dergi, radyo ve sosyal medya gibi uygulamalar üzerinden yapılmaktadır.

Şekil 2.1. Açık kaynak istihbaratı

İstihbarat çalışmalarının yaklaşık olarak %80'lik kısmı açık kaynak verileri üzerinden yapılmaktadır. Bu sistem her alanda kullanılabilecek birçok değerli ve kullanılabilir bilgiyi kullanıcılarına sunar. Yapılmakta olan araştırma faaliyetleri bu bilgilerden yararlanarak doğru bir araştırma raporu sunulmasına olanak sağlar.

2.3.2. Bilgi çarpıtma (dezenformasyon) araştırması

Bilgi çarpıtma kasıtlı olarak zarar vermek amacıyla gerçeklerle ilgisi olmayan bilgiler üreterek yayma sürecidir (Teyit, 2023). Genellikle insanlara, gruplara, şirket ve kurumlara

kasıtlı olarak zarar vermek amacıyla kullanılmaktadır. Dijital dünyanın bilgiye kolay ulaşılması, haberlerin hızlı bir şekilde yayılması gibi sağladığı kolaylıkların yanında, özellikle kişilerin kullanmakta olduğu sosyal medya mecralarında paylaşılan sahte haberlerin yayılması doğru bilgiye ulaşılmasını engellemektedir.

Günümüzde tüm dünya üzerinde sosyal medya üzerinden paylaşılmakta olan haberlerin yayılması ve okunması diğer medya uygulamalarına göre daha hızlıdır. Bu algının bu denli küresel çapta yaygın olduğu düşünüldüğünde sosyal medya kullanıcılarının doğru bilgiye ulaşması için haber güvenliğini sağlamak önemli bir hal almıştır. Bir bilginin yanıltıcı olarak kabul görmesi için genel bazı şartları taşıması gerekmektedir. Bunlar;

- Bilginin gerçeği yansıtmaması ve ülke huzurunu bozmaya yönelik olması
- Kamu sağlığı ve güvenlik ile ilgili yanıltıcı bilgi olması
- İnsanlar arasında korku ve endişeye sebep olması
- Yanıltıcı haberin herkes tarafından görülebilir nitelikte olmasıdır.

2.3.3. Derin sahte (deepfake) araştırması

Derin sahte, mevcut bir ses kaydı veya videoda yer alan bir kişinin, yapay zekâ ve makine öğrenmesi teknikleri kullanılarak bir başka kişiyle değiştirildiği video veya ses kaydı manipülasyon tekniğidir (Datamarket, 2024). Kısaca sahte video veya ses verileri olarak tanımlanmaktadır.

Derin sahte yapmak için iki algoritma kullanımına ihtiyaç duyulmaktadır. İlk algoritma birleştirilmesi gereken iki görüntünün ortak özelliklerini arar, ardından ikinci algoritma bunları yeni oluşturulan görüntüye aktarır. Birinci algoritmaya üretici de denilmektedir. Çünkü kişinin vücudu, yüzü ve gözleri gibi ayırt edici özellikleri birleştiren görüntüleri oluşturur. İkinci algoritma, üretici tarafından sağlanan görüntülerin doğruluğunu denetleyen bir ayırıcı özellik taşır.

Ülkemizde son yıllarda ortaya çıkmış olan derin sahte sosyal medya ve haber sitelerinin hızla yayılmaya başlamasıyla çeşitli amaçlar için de kullanılmaya başlamıştır. Bunlar;

- Eğlenmek
- Kişi veya kurumları tuzağa düşürmek
- Aşağılayarak alay etmek

- Siyasi provokasyonlara sebep olmak
- Sahte bilgiler üzerinden tartışma başlatmaktır.

Derin sahte uygulamalarının hızla yayılmaya başlamasıyla farklı risk ve tehdit unsurları ortaya çıkmaktadır. Bundan dolayı insanlar bilinçlendirilmeli, özellikle sosyal medya mecralarında dolaşan ses kaydı, fotoğraf, videolara hemen itibar edilmemeli ve doğruluğu teyit edilmelidir.

2.4. TCK'da Düzenlenen Bilişim Suçları

Türkiye'de bilişim suçları ile ilgili ilk düzenleme, 1991 yılında 765 sayılı TCK'ya eklenen "...bilgileri otomatik işleme tabi tutan sistem..." ibaresiyle yapılmıştır. Bu düzenlemenin ardından, bilişim suçlarıyla ilgili birçok kanunda değişiklik ve eklemeler yapılmıştır, çünkü bu alanda ortaya çıkan ihtiyaçlar sürekli olarak değişmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2019; Ekin Hukuk Bürosu, 2023; Yıldırım, 2023).

5237 sayılı TCK'nın yürürlüğe girmesiyle birlikte, 26 Eylül 2004 tarihinde "TCK Bilişim Suçları" başlığı altında özel olarak düzenlemeler yapılmıştır. Kanunun "Topluma Karşı Suçlar" başlığı altında üçüncü kısım onuncu bölümde, "Bilişim Sistemlerine Karşı Suçlar" adı altında 243 ile 245. maddeler arasında yer almaktadır. TCK'da bilişim suçları, doğrudan (gerçek) bilişim suçları ve dolayısıyla bilişim suçları olmak üzere iki ana kategoriye ayrılmıştır. Doğrudan (gerçek) bilişim suçları, "Bilişim Alanında İşlenen Suçlar" başlığı altında 243 ile 245. maddeler arasında düzenlenirken, dolayısıyla bilişim suçları ise TCK'nın çeşitli maddelerinde dağınık bir şekilde düzenlenmiştir (Türk Ceza Kanunu, 2004).

3. LİTERATÜR ARAŞTIRMASI

Bilişim suçlarının işlenme oranlarındaki artışın sebepleri arasında işsizlik, gelir seviyesi, yaş, cinsiyet ve eğitim durumu gibi etkenler büyük bir etkiye sahiptir. Adli bilişim alanında gerçekleştirilen çalışmalarda yapay zekânın alt dalı olan makine öğrenmesi ve derin öğrenme yöntemleri kullanılmıştır. Son beş yıl içerisinde bu alanda yapılmış olan çalışmalar literatür araştırmasında sunulmuştur.

Bilişim suçları ve psikolojik etkileri açısından Türkiye'de telefon dolandırıcılığının analizine ilişkin yapılan çalışmada; dijital teknolojilerin hızla gelişmesiyle birlikte kişilere ait bilgilerin elektronik ortamlarda bulunabilir ve erişilebilir duruma geldiği belirtilmiştir. Bu durumun dolandırıcılık olaylarının meydana gelmesinin en büyük sebeplerinden bir tanesi olduğu öne sürülmüştür. Bilişim dünyasında dolandırıcıların kendilerini mağdurları ikna etmek için kamu ve özel sektöre ait çeşitli meslek gruplarından biri gibi tanıttıkları, insanların zaafları ve korkularından faydalanarak maddi ve manevi zarar verdiklerini gözlemlemişlerdir. Teknolojik yeniliklerin artmasıyla bilirlikte meydana gelen bilişim suçları çeşitliğinin de arttığı ancak hukuki altyapının aynı hızda değişkenlik gösterememesinden dolayı dolandırıcıların hukuki boşlukları kullandıklarını tespit etmişlerdir. Bu çalışmada, veri madenciliği kullanılarak ülkemizde meydana gelen telefon dolandırıcılığı olayları incelenmiş ve meydana gelen olaylar arasında ilişkiler ve bağlantılar ortaya konmuştur. Kullanılan verilerde 63 polis, 33 savcı, 19 pazarlamacı, 2 asker, 12 MİT personeli, 20 banka çalışanı ve 3 sigortacı telefon dolandırıcılığı ile ilişkilendirilmiş, bu kişilerin 123 tanesinin erkek ve 29 tanesinin de kadın olduğu ifade edilmiştir. Dolandırıcılar tarafından hedef alınan meslek gruplarına göre kişilerin dağılımları ise şu şekildedir; 40 özel sektör çalışanı, 34 kamu çalışanı, 29 işsiz, 38 emekli, 5 çocuk ve 6 öğrenci olarak belirlenmiştir. Son olarak, bu dolandırıcılık faaliyetlerinde dolandırıcıların elde ettikleri başarı oranları 94 kez başarılı ve 58 kez başarısız olarak değerlendirilmiştir (Tekkanat ve diğ., 2018).

Bu çalışmanın sonucunda dolandırılan insanların kişisel zaafları ve maddi menfaat gözetmeleri gibi durumlardan dolayı kişisel bilgilerini kendi istekleri doğrultusunda dolandırıcılara verdikleri anlaşılmıştır. Kanuni boşlukların olması hızla gelişen teknolojilerin insan hayatına sağlamış olduğu kolaylığın yanında özel bilgilerin internet ortamında korunmasının yeteri kadar mümkün olmadığından dolayı büyük bir güvenlik zafiyetinin oluştuğu belirlenmiştir. Yaşlı nüfusun genç nüfusa göre dolandırılma ihtimallerinin daha yüksek olduğu, gelişen teknolojilerin beraberinde getirdiği birçok sorunun yanında güvenlik zafiyetlerini de ortaya çıkardığı görülmüştür. Güvenlik açıklarının farkında olmayan veya

gerekli önlemleri almayan insanların dolandırıcılar tarafından kolayca ikna edilebildiği anlaşılmıştır.

Nüfus yoğunluğunun çok fazla olduğu yerlerde meydana gelen; olayların tespiti, nesne tespiti, olaylardaki şiddetin derecesinin tespiti ve kalabalık alanların analizi konularında çalışma yapılmıştır. Analizin yapılmasında Evrişimli Sinir Ağları (ESA), Destek Vektör Makineleri (DVM) ve K-En Yakın Komşular (IBK) algoritmalarından faydalanılmıştır. Çalışmalar kapsamında kullanılan analiz ve video tespitleri uygulamalarının birbirlerine engel olduğu, hava şartları gibi etkenlerin de hesaba katılması durumunda yapılan çalışmaların büyük çoğunluğunda görüntü verilerinin analiz edilmesinde yetersiz kalındığı gözlemlenmiştir. Video analizinde kullanılmakta olan uygulamaların gerçek dünya şartlarının da ele alınmasıyla birlikte çözüm ürettiği, meydana gelen sebeplerin yanında aksi durumların hepsinin oluşması durumunda da tespiti yapılacak problemlerin çözümünü yapabilecek bir analiz uygulamasının olmadığı belirtilmiştir (Sreenu ve Durai, 2019).

Dijital görüntü manipülasyonunun tespiti tekniklerine ilişkin yapılan çalışmada; teknolojilerin gelişmesiyle birlikte çok sayıda dijital fotoğrafların oluşturduğu verilerin meydana geldiği belirtilmiştir. Bununla birlikte mevcutta bulunan fotoğraf düzenleyici programlar sayesinde görüntüler üzerinde değişiklik yapmanın çok basit hale geldiği gözlemlenmiştir. Tahrip edilmiş görüntülerin suçlular tarafından insanları yanıltmak ya da meydana gelen suçlarla ilgili soruşturmaların akıbetini değiştirmek amacıyla kullanıldığı tespit edilmiştir. Görüntüler üzerinde çok kez oynandıktan sonra dijital veri üzerinde bıraktığı izlerin yok edilmesinin orijinal görüntü verilerinin ortaya konulma sürecini çok zorlaştırdığı gözlemlemişlerdir. Bu çalışma ile görüntüler üzerinde yapılan manipülasyonların tespitini yapmak amacıyla derin öğrenme yöntemleri kullanılmış, görüntüler üzerinde yapılabilecek çeşitli görüntü sahteciliği ve görüntü manipülasyonu tespitinin yapılması ele alınmıştır. Çalışma kapsamında ImageNet ile farklı derin öğrenme algoritmaları kullanılmıştır. Görüntüler üzerinde yapılan manipülasyon ve sahteciliğin tespit edilmesinde kullanılabilecek yazılım programlarının oluşturulmasının zor ve zaman aldığı belirtilmiştir. Görüntüler üzerindeki manipülasyon yöntemlerinin sürekli değişip geliştiği, bu değişikliğe ve gelişmeye paralel olarak meydana gelen sahteciliklerin ortaya konulmasını sağlayacak sistem ve yazılımların geliştirilmesi gerektiği ortaya konulmuştur (Thakur ve Rohilla, 2020).

Video ve görüntü analizi ile ilgili yapılan çalışmada; gelişmiş teknolojilerin tüm insanlığa fayda sağladığı, insanlığın büyük buluşlar yapmasına olanak sağladığı ifade edilmiştir. Bunlara örnek olarak görüntü ve video çekebilen üst düzey mobil cihazlar ve dijital

kameraların bulunduğu ancak bu teknolojilerin kullanımının da beraberinde büyük riskler getirdiği tespit edilmiştir. Mobil cihazlar ve dijital kameralarda depolanan görüntü ve videolar genellikle insanlar tarafından sosyal medya platformlarında paylaşılmakta ve bu durum her türlü manipülasyona açık olduğundan sosyal medya kullanıcılarını zor durumda bırakabileceği değerlendirilmiştir. Bu çalışmayla sosyal medya platformlarında yer alan ve hukuki süreçte delil olarak kullanılması muhtemel 3GP, MOV ve MP4 formatına sahip görsellerin orijinal görsellik yapıları bozularak görüntü ve videolar üzerinde oynandığını ortaya koyabilen yeni bir yöntem ortaya konulmuştur. Görüntü ve videolar üzerinde yapılan düzenlemeler ile arkada bıraktığı izler makine öğrenmesi yöntemleri ile analiz edilerek hangi görüntü ve videolar üzerinde düzenlemenin yapıldığı ortaya çıkarılmaya çalışılmıştır. Çalışmada 4979 adet orijinali ile oynanmış video görüntüsü kullanılmıştır. Sonuçların değerlendirilmesinde rastgele orman (RO) algoritmasının en iyi başarıyı gösterdiği tespit edilmiştir. Hukuki süreç içerisinde delil niteliği taşıyan görüntü ve videoların üzerinde oynanması nedeniyle suçsuz kişiler suçlu durumuna sokulabilirken bir suçluyu da tüm suç unsurlarından arındırabileceği gözlemlenmiştir. Bu nedenle tüm bu hukuki süreçlerde doğru karar verebilmek adına adli tıp biliminin geliştirilmesi gerektiği önerilmiştir (Orozco ve diğ., 2020).

Makine öğrenmesi algoritmaları ile terör olaylarının tahmin edilmesi ile ilgili yapılan çalışmada; günümüzün en önemli tehditlerinden bir tanesinin terörizm olduğu, ayrıca terörizmin tüm dünyada iş gücü ve güvenlik harcamalarını arttırarak ülkelerin eğitim ve sağlık gibi alanlara aktarması gereken fonları terörizm faaliyetlerinden dolayı güvenliğe aktarmak zorunda kaldıkları belirtilmiştir. Tüm bunların yanı sıra terörizmin çok sayıda can kaybına sebep olduğundan dolayı insanoğlunun sosyal yaşamlarını olumsuz yönde etkilediği gözlemlenmiştir. Teknolojilerin gelişmesiyle birlikte bilgiye ulaşılması kolaylaşmış, bu sayede ülkeler için öngörülebilirlik derecelerinin arttığı, stratejik karar mercilerinin, güvenlik ve istihbarat gibi alanlarda karar almalarının kolaylaştığı değerlendirilmiştir. Bu çalışmada meydana gelen terör olaylarının hangi terörist grubu veya grupları tarafından yapıldığı ile ilgili tahminde bulunulmuş ve incelemelerin detaylandırılması için makine öğrenmesi yöntemleri ile yeni modeller oluşturulmuştur. Sonuçlar değerlendirildiğinde, yapay sinir ağları (YSA), RO, lojistik regresyon ve karar ağacı algoritmalarının uygun olduğu görülmüştür (Görmez, 2021).

Adli bilişim inceleme süreçlerinde yapay zekâ kullanımı ile ilgili yapılan çalışmada; teknolojilerin hızla gelişmesine bağlı olarak bilgiyi depolayan ve kullanan bilişim cihazları ve

uygulamaların kullanım oranlarının arttığı gözlemlenmiştir. Dijital cihazlarda depolanan verilerin artması, suç oranlarının artmasına sebep olduğu tespit edilmiştir. Dijital dünyanın gelişmesiyle bilişim suçlarındaki veri miktarının artış gösterdiği bu durumun verinin doğru analizini zorlaştırdığı anlaşılmıştır. İşlenen verilerin artmasının yargılama süreçlerini de olumsuz etkilediği belirtilmiştir. Çalışmada toplam 4000 adet veri kullanılırken bu rakamın 2000 adedini tabanca görüntüleri, 2000 adedini bıçak görüntüleri oluşturmuştur. Elde edilen sonuçlara göre model ile %97.8 oranında doğruluk elde edilmiştir. Elde edilen sonuç, derin öğrenme alanında gerçekleştirilen sınıflandırma çalışmaları ile karşılaştırılmıştır (Dilber, 2022).

Ses incelemeleri için yapay zekâ ile cinsiyet tespiti modelinin geliştirilmesiyle ilgili yapılan çalışmada; analiz aşamalarında doğruluğun arttırılması ve insan müdahalesinin minimum seviyeye indirgenmesi adına görsel verileri yüksek doğruluk oranı ile sınıflandırmayı sağlayan VGG16 ağ tabanlı bir model önerilmiştir. Suç kapsamında elde edildiği varsayılan veriler, TensorFlow ve Keras derin öğrenme kütüphaneleri desteği ile FloydHub geliştirme ortamında önerilen model ile teste tabi tutulmuş ve söz konusu veriler üzerinde sınıflandırma işlemleri gerçekleştirilmiştir. Sonuç olarak suçların ortaya çıkarılması aşamalarında yapılan çalışmanın bir etken olabileceği ancak suç delillerinin ortaya konulmasında tek başına yeterli olmadığı anlaşılmıştır. Teknolojik ses cihazlarının gelişmesiyle birlikte insan hayatını her alanda kolaylaştıran ses verilerine rastlamakta olduğu gözlemlenmiş, ses verileri ile işlenen suçların tespitinin yapılabilmesi için ses tanıma sistemlerinin geliştirilmesi gerektiği belirtilmiştir. Bu sistemler sayesinde cinsiyet, yaş ve insanların duygu durumlarına dair birçok özelliğin tespitinin yapıldığı anlaşılmıştır. Tespiti yapılan bu tür özellikler sayesinde konuşmacıların veya ses kayıtlarındaki kişilerin tüm özellikleri veri haline dönüştürülerek meydana gelen bilişim suçlarında delil niteliği taşıyabileceği aktarılmıştır. Bu çalışmada yapay zekâda kullanılan sınıflandırma yöntemleri karşılaştırılmış toplanan veriler ile konuşmacının sesinden cinsiyet tespitinde kullanılabilecek bir model geliştirilmiştir (Demirel, 2022).

Ses verilerinin, düşük maliyet, veri girişi kolaylığı, uzaktan kolayca erişilebilmesi gibi konularda avantaj sağladığından dolayı bu konudaki çalışmaların artmasına sebep olduğu anlaşılmıştır. Modelde yaş ortalaması 28.6 olan kadın ve 37.4 olan erkeklerden youtube üzerinden toplanan 170 ses verisi ile veri seti oluşturulmuş, bu veri seti kullanılarak cinsiyet sınıflandırmasında kullanılabilecek bir model geliştirilmiştir. Bilişim suçlarında yapay zekâ yöntemleri kullanılarak elde edilen ses delilleri ile kişilerin yaşı ve cinsiyeti gibi özelliklerinin

tespit edilmesinin çok önemli olduğu görülmüştür. Değişik yaş ve cinsiyet grupları arasında uygulanan modelin doğruluk oranlarında değişiklikler yaşandığı gözlemlenmiştir. Modelde makine öğrenmesi modellerinden DVM kullanılmış, çalışmada doğruluk oranının %99.59 olarak hesaplandığı tespit edilmiştir (Demirel, 2022).

Kablosuz ağlar üzerinden gerçekleştirilen siber tehditlerin analizi ile ilgili yapılan çalışmada; teknolojilerin gelişmesiyle birlikte kullanmakta olduğumuz cihazların siber suç oranlarının artmasıyla tehdit altında olduğu belirtilmiştir. Birbirleri ile etkileşim halinde bulunan cihazlardan herhangi birinin tehdit unsurlarına maruz kalmasının diğer etkileşim halindeki cihazları da tehlikeye düşürebildiği aktarılmıştır. Çalışmada kablosuz ağlar üzerinde, sistemleri tehdit edebilecek muhtemel tüm saldırılar gerçekleştirilmiş, sınıflandırma için Navie Bayes, DVM, gradyan arttırma ve IBK algoritmaları kullanılmıştır. Sınıflandırma algoritmalarının uygulanması sonucunda veri setinin elde ettiği skorlar toplanmış, en iyi skoru 0.91'le gradyan arttırma algoritmasının verdiği gözlemlenmiştir. Uygulanan tüm farklı saldırıların ağlarda farklı sonuçlara yol açmakta olduğu, bununda elde edilen verilerin birbirinden farklı olmasını sağladığı gözlemlenmiştir. Uygulanan bazı saldırıların özelliklerinin belirlenemediği gözlemlenmiştir. Bu nedenle meydana gelebilecek saldırıların tüm özelliklerini belirleyebilecek bir yazılıma ihtiyaç olduğu ya da halihazırda performansı daha yüksek yazılımların kullanılması gerektiği tespit edilmiştir. Gerçekleştirilen siber saldırıların çeşitliğinin ve sayısının arttırılarak çalışmanın genişletilmesi, farklı makine öğrenmesi algoritmaları ile performansların artabileceği önerilmiştir. Hızla gelişmekte olan teknolojiyle birlikte siber suç çeşitliliği ve oranlarında artış meydana gelmekte olduğundan bu hususta bilimsel araştırmaların arttırılarak siber güvenlik konusunda bilinçli insan sayısının arttırılması gerektiği aktarılmıştır (Kaçan, 2023).

4. YALOVA İLİNDE MEYDANA GELEN ADLİ BİLİŞİM SUÇLARININ DEĞERLENDİRİLMESİ

Yalova ili Marmara bölgesinde yer almakta olup 06 Haziran 1995 yılında il olmuştur. İlin yüzölçümü 799 km^2'den oluşmaktadır. Yalova ili nüfusu 2022 verilerine göre 296.333'tür. Bu nüfus, 147.904 erkek (%49.91) ve 148.429 kadından (%50.09) oluşmaktadır. Bulunduğu konum itibariyle nüfus yoğunluğu fazla olan İstanbul, Bursa ve Kocaeli gibi büyükşehirlerin merkezinde bulunmaktadır. Gemi tersaneciliği, bitki seraları ve organize sanayi bölgeleri ile ekonomisinin hızla gelişmekte olmasından dolayı Türkiye'nin çeşitli illerinden göç almaktadır. Bu durum nüfusu her yıl hızla arttırmaktadır.

Ancak nüfusun bu denli hızlı ve plansız bir şekilde artması bazı sorunları da beraberinde getirmektedir. Çarpık kentleşme, altyapı, sağlık, eğitim, işsizlik ve geçim kaygısı gibi problemleri ortaya çıkarmaktadır. Ülkemizin uygulamakta olduğu sosyal politikalar gereği insanlara sunmak zorunda olduğu altyapı, sosyal alanlar, eğitim ve sağlık gibi alanlarda nüfusun hızla ve plansız bir şekilde artmasından dolayı yetersiz kalınmaktadır. Bu durum insanlarda güvensizliğe sebep olmakta, beraberinde güvenlik zafiyetlerini arttırmaktadır.

Bu tür zafiyetler insanları meydana gelen problemlere karşı yeni çözümler bulmaya yönlendirmektedir. İşsizlik ve geçim sıkıntısı yaşayan kişilerle, kolay yoldan para kazanmayı düşünen insanların hızla artması bilişim suçlarındaki olay sayılarını hızla arttırmaktadır. Özellikle Yalova iline Arap ülkelerinden göç eden insanların ülke kültürüne yabancı olmaları, dil sorunu yaşamaları, ülkemizde bulunan hukuki süreçlerin işleyişini bilmemeleri ve ülkeden gönderilme gibi kaygılarının olması gibi nedenler bilişim suçu mağduru olmalarına ortam sağlamaktadır. Yalova ilçeleri Şekil 4.1'de gösterilmiştir.

Şekil 4.1. Yalova ilçeleri

Yalova'da bulunan ilçelerin nüfus yoğunluğuyla ilgili Tablo 4.1 incelendiğinde; Altınova ilçesinde gemi tersaneciliği ve bitki seralarının olması, Armutlu ilçesinde doğa turizmi ve tarımın gelişmiş olması, Çınarcık ilçesinde bitki seralarının bulunması, Çiftlikköy ilçesinde organize sanayi bölgesinin olması, Merkez ilçesinde kültür ve doğa turizminin olması, Termal ilçesinde sağlık ve kültür turizminin bulunması nüfus yoğunluğunu etkilemektedir. Tablo 4.1'de Yalova ili ilçelerinin nüfus yoğunlukları gösterilmiştir.

Tablo 4.1. Yalova ili nüfusu

İLÇE	**NÜFUS 2022**
Altınova	32.207
Armutlu	10.843
Çınarcık	38.600
Çiftlikköy	50.974
Merkez	156.732
Termal	6.977
Yalova	296.333

4.1. Bilişim Suçlarında Makine Öğrenmesi Uygulamaları

Makine öğrenmesi, bilgisayarların algısal veri veya veri tabanları gibi veri türlerinden öğrenme yapabilmesini sağlayan algoritmaların tasarım ve geliştirme süreçlerini konu alan bir bilim dalıdır. Algoritmaların belirli bir görevi gerçekleştirmek için veriler üzerinde genel kurallar ve örüntüler belirlemesine ve bu örüntüleri kullanarak gelecekte oluşabilecek verilerin tahmin edilmesine olanak sağlar. Bilgisayarların programlanmadan görevlerini nasıl yerine getirebileceğini bulur ve uygular. Kısaca algoritmalar kullanılarak verilerin ayrıştırılması, ayrıştırılan verilerin öğrenilmesi sonucunda konu hakkında belli bir tahmin yapılma sürecidir (Aylak ve diğ., 2020).

Çalışmada 2020-2023 yılları arasında Yalova ilinde meydana gelen bilişim suçları ile ilgili veriler elde edilerek makine öğrenmesi yöntemleri ile analizi gerçekleştirilmiştir.

4.1.1. Makine öğrenmesi algoritmaları

Makine öğrenmesi algoritmaları, veri madenciliği, istatistiksel analiz ve matematiksel modellemeleri kullanarak veriye dayalı öngörülerde bulunur. Bilgisayar sistemlerinin deneyim ve veriye dayalı olarak kendilerini geliştirmesine olanak tanır. Yapay zekâ ve veri bilimi alanında ciddi bir araştırma ve uygulama alanı oluşturmaktadır. Özellikle büyük veri setlerinin işlenmesi ve analiz edilmesi süreçlerinde kullanılarak çeşitli alanlarda verimlilik ve hızlı karar alma süreçlerine önemli katkılar sağlamaktadır. Finansal analiz, tıbbi teşhis, otomotiv ve güvenlik gibi alanlarda etkin bir şekilde kullanılmaktadır.

Makine öğrenmesi algoritmaları, denetimli ve denetimsiz öğrenme olmak üzere iki kategoriye ayrılmaktadır. Denetimli öğrenme, algoritmanın tespiti yapılmış veri kümesinden öğrenerek ileriye dönük tahminler yapmasını sağlar. Çalışmamızda da kullanacağımız sınıflandırma algoritmaları için idealdir. Denetimsiz öğrenme ise veri setindeki örüntüleri belirleyerek gruplandırma yapar.

Sınıflandırma algoritmaları, bir veri kümesindeki örnekleri belirli bir sınıfa atamak için kullanılan makine öğrenimi teknikleridir. Veri setinde bulunan bilgilerden öğrenme işlemini yapar ve bu öğrenimleri birkaç sınıfa veya gruba ayırarak sınıflandırır. Bu sınıflandırmalar, etiketler/kategoriler olarak çağrılabilir (Neighbor, 2021).

Uygulanmakta olan sınıflandırmanın temel amacı elimizde bulunan verinin hangi sınıfa ait olduğunu belirtmektir. Sınıflandırıcı olarak adlandırılan kavram, girdi olarak verilen verileri belirli bir kategoriye göre eşleyen algoritma iken; sınıflandırma modeli, eğitim için verilen girdi verilerini değerlendirerek bazı sonuçlar ortaya çıkarmaya çalışan yapılar olarak tanımlanabilmektedir (Garg, 2018).

- **RO algoritması**

RO algoritması, birbirinden bağımsız olarak çalışan birçok karar ağacının bir araya gelerek en yüksek puanı alan değeri seçmesi ile çalışır. Kullanım kolaylığı ve esnekliği nedeniyle yaygın olarak benimsenmiştir. Algoritma, birden fazla karar ağacı oluşturarak sınıflandırma işlemi sırasında sınıflandırma doğruluğunu artırmayı amaçlar. Bu yöntem, veri kümesi üzerinde çeşitli modeller oluşturarak, kümenin yeniden ve daha ayrıntılı incelenmesini sağlar (Akdağlı, 2021; Öztürk, 2022).

RO sınıflandırma ve regresyon problemleri kullanılan güçlü bir makine öğrenmesi algoritmasıdır. Birden fazla modelin birleşimini kullanarak en iyi performans elde etmeye çalışır. Algoritmada eğitim süreci tamamlandıktan sonra, her ağaç bağımsız olarak tahminler

yapar. Sınıflandırma problemlerinde, her ağacın tahmin ettiği sınıf bir oy olarak değerlendirilir ve en çok oyu alan sınıf nihai tahmin sonucu olarak seçilir. Regresyon problemlerinde ise, her ağacın tahmin ettiği değerlerin ortalaması alınarak nihai tahmin sonucu elde edilir. RO algoritmasının avantaj ve dezavantajları bulunmaktadır.

Avantajları:

- ✓ Yüksek performans; çeşitli öğrenme ağaçlarının bir araya getirilmesi, karmaşık ilişkileri modellemek ve tahmin etmek için geniş bir kapasite sağlar.
- ✓ Daha az aşırı uyum**;** tek bir karar ağacı yerine birçok karar ağacının topluluğunu kullanır. Bu, aşırı uyumu azaltır, modelin eğitim veri setine aşırı uyması ve genelleme yapamaması riskini azaltır.
- ✓ Dayanıklılık; aykırı değerlere ve eksik verilere dayanıklıdır.
- ✓ Genelleme gücü; çeşitli veri tiplerini ve yapılarını işleyebilir ve genelleme yapabilir bu da çeşitli uygulama alanlarında kullanılabilirliğini artırır.
- ✓ Veri boyutuna ve öznitelik sayısına dayanıklılık; genellikle büyük boyutlu ve yüksek boyutlu özniteliklere sahip veri setleriyle iyi performans gösterir. Yüksek boyutlu veri setleri, modelin doğruluğunu azaltabilir veya hesaplama maliyetlerini artırabilir ancak RO algoritması bu zorlukları aşabilir.
- ✓ Eğitim süresi ve hızlı tahmin**;** RO algoritması paralel hesaplama yeteneklerinden yararlanarak eğitim süresini azaltabilir.

Dezavantajları:

- ✓ Büyük bellek kullanımı; birden çok karar ağacını eğitmek ve tahmin yapmak için büyük miktarda bellek kullanır.
- ✓ Yavaş eğitim; birçok karar ağacının eğitilmesi gerektiğinden, eğitim süresi diğer bazı basit algoritmalara göre daha uzun olabilir. Özellikle büyük veri setleri üzerinde eğitim yaparken eğitimi oldukça zaman alabilir.
- ✓ Yüksek tahmin maliyeti; tahmin yapmak için birçok karar ağacının tahminlerini birleştirmesi gerektiğinden, tahmin maliyeti diğer basit algoritmalara göre daha yüksek olabilir.
- ✓ Modelin anlaşılabilirliği**;** birçok karar ağacının bir araya getirilmesiyle oluşturulduğu için karar ağaçları karmaşık olabilir ve bu nedenle modelin nasıl tahminler yaptığını anlamak ve yorumlamak zor olabilir.

- **DVM algoritması**

DVM algoritması bir sınıflandırma modelidir. Vektörler yardımı ile verileri birbirinden ayırt etmemizi sağlar**.** İstatistiksel öğrenim teorisine dayanır. Regresyon analizi yapan bir modeldir. Temel amacı, veri noktalarını sınıflandırmak veya bir doğru veya eğri ile regresyon yapmaktır. Bir düzlemdeki noktaları ayırmak için bir doğru çizer ve bu doğrunun iki sınıfın noktalarına olan uzaklığını maksimum yapmayı hedefler. Bu yöntem, karmaşık ancak küçük ve orta ölçekli veri setleri için uygundur. Özellikle lineer olmayan ve ayrılamaz veri kümelerini sınıflandırmak için etkilidir. DVM algoritmasının amacı sınıfları birbirinden ayıran bir karar sınırı oluşturmaktır. (Akca, 2020; Şener, 2021).

DVM algoritmasının avantaj ve dezavantajları bulunmaktadır.

Avantajları:

- ✓ Yüksek doğruluk**; s**ınıflandırma ve regresyon problemlerinde yüksek doğruluk sağlar.
- ✓ Etkin boyut ilişkisi kullanımı; yüksek boyutlu öznitelik uzaylarında iyi performans gösterir.
- ✓ Aykırı değerlere dayanıklılık; aykırı değerlere karşı dayanıklıdır ve genellikle modelin performansını etkilemez. Destek vektörlerinin etrafındaki diğer veri noktalarına odaklanır bundan dolayı aykırı değerlerin etkisi sınırlı kalır.
- ✓ Esnek çekirdek fonksiyonları; farklı çekirdek fonksiyonlarını kullanarak farklı problemler için esneklik sağlar.
- ✓ Düşük hata oranı; yanlış sınıflandırma veya regresyon tahminleri nadirdir.
- ✓ Çoklu sınıf desteği; çoklu sınıf problemlerini çözmek için kullanılabilir.
- ✓ Hiper parametre optimizasyonu; rastgele arama gibi teknikler kullanılarak, doğru hiper parametreler seçilerek modelin performansı optimize eder.

Dezavantajları:

- ✓ Hassas parametre ayarı; doğru performans için çeşitli hiper parametrelerin hassas bir şekilde ayarlanması gerekebilir.
- ✓ Hesaplama karmaşıklığı; eğitimi büyük veri setlerinde ve yüksek boyutlu öznitelik uzaylarında hesaplama açısından karmaşıktır.
- ✓ Aşırı uyum riski; eğitim veri setine aşırı uyma eğilimindedir.
- ✓ Yüksek hiper parametre hassasiyeti; performansı kullanılan hiper parametrelerin hassas seçimine bağlıdır.

- ✓ Çoklu sınıf desteği; doğrudan çok sınıflı sınıflandırma problemlerini çözmek için tasarlanmamıştır.

DVM algoritmasının kernel fonksiyonları:

1. Linear Kernel; veri setini yüksek boyutlu uzaylara dönüştürmeden doğrudan lineer olarak ayrılabilir durumlar için kullanılır.

2. Polinom Kernel; veri setini yüksek boyutlu uzaylara dönüştürerek polinom derecesine göre ayrılabilir hale getirir.

3. Radyal Basis Function (RBF) Gaussian Kernel; her bir veri noktasını etkileyen bir Gaussian dağılımı ile hesaplanan bir mesafe ölçüsünü temsil eder. Bu kernel, lineer olmayan ve karmaşık yapıları olan veri setlerini işlemek için kullanılır.

4. Sigmoid Kernel; veri noktalarını yüksek boyutlu uzaylara dönüştürmek için sigmoid fonksiyonunu kullanır.

- **Çok katmanlı yapay sinir ağları (Çok katmanlı YSA) algoritması**

Çok katmanlı algılayıcılar, bir dizi girdiden bir dizi çıktı üreten ileri beslemeli yapay sinir ağlarıdır. Çok katmanlı YSA algoritması sınıflandırma ve regresyon gibi birçok görevde kullanılabilir. Giriş ve çıkış katmanları arasında yönlendirilmiş bir grafik olarak bağlanan birden fazla gizli katman içerir. Ağın eğitiminde geri yayılım algoritmasını kullanır ve derin öğrenme yöntemlerinden biri olarak kabul edilir (Kaynar ve diğ.,2016; Işıkhan, 2020).

Çok katmanlı YSA algoritması en az bir gizli katman içeren birçok katmandan oluşur. Her bir katman, birbirine bağlı bir dizi nöron içerir. Girdi verilerini işleyerek bir çıktı üretir. Gizli katmanlar, girdi verilerini temsil etmek için ara katmanlardır ve genellikle özelliklerin karmaşıklığını öğrenmek için kullanılır. Algoritmada her bir bağlantı arasında bir ağırlık bulunur. Bu ağırlıklar, modelin veri setini temsil etmek için öğrenmesi gereken parametrelerdir. Ayrıca her bir nöronun bir bias değeri vardır. Bu bias değerleri, nöronların aktivasyon eşiğini belirler ve ağın esnekliğini artırmaktadır. Görüntü tanıma, tıbbi teşhis, finansal tahminler, otomotiv endüstrisi ve video oyunları gibi birçok alanda kullanılmaktadır.

Çok katmanlı YSA algoritmasının avantaj ve dezavantajları bulunmaktadır.

Avantajları:

- ✓ Esneklik ve uyarlanabilirlik; çeşitli veri setleri ve problemleri için esnek bir şekilde uyarlanabilir. Farklı tipte verilerle çalışabilir ve farklı tipte problemleri çözebilir. Bu nedenle geniş bir uygulama alanı sağlar.
- ✓ Karmaşık ilişkilerin modellemesi; karmaşık ilişkileri modelleyebilir.

- ✓ Yüksek doğruluk; doğru şekilde eğitilmesi durumunda yüksek doğruluk sağlayabilir.
- ✓ Özniteliklerin otomatik öğrenilmesi; öznitelikleri otomatik olarak öğrenir ve veri setindeki gizli desenleri ortaya çıkarabilir. Bu özellik veri setlerinin karmaşıklığını azaltır.
- ✓ Ölçeklenebilirlik; veri setinin boyutu ve karmaşıklığı arttıkça ölçeklenebilirlik gösterir. Büyük veri setleriyle veya karmaşık problemlerle çalışırken, performansı genellikle yüksektir.

Dezavantajları:

- ✓ Hiper parametre hassasiyeti; performansı, bir dizi hiper parametrenin doğru bir şekilde ayarlanmasına bağlıdır. Yanlış parametre ayarı, modelin performansını olumsuz yönde etkileyebilir.
- ✓ Aşırı uyum eğilimi; özellikle eğitim veri setiyle uyum sağlamak için aşırı öğrenme olabilir ve model yeni verilere genelleme yapma yeteneğini kaybedebilir.
- ✓ Yüksek hesaplama gücü gereksinimi; eğitim ve tahmin yapmak için yüksek hesaplama gücü gerektirir.
- ✓ Veri seti boyutuna hassasiyet; küçük veri setlerinde veya düşük boyutlu veri setlerinde, performansı sınırlı olabilir.
- ✓ Hiper parametre optimizasyonu; doğru performansı için bir dizi hiper parametrenin ayarlanması gerekmektedir. Bu, zaman alıcı bir süreç olabilir ve bazı durumlarda uygun hiper parametreleri belirlemek için çapraz doğrulama gibi teknikler kullanılmalıdır.
- ✓ Eğitim zamanı; derin ağ yapıları veya büyük veri setleri ile çalışırken, eğitim süresi önemli ölçüde artabilir.

- **IBK Algoritması**

IBK algoritması anlaşılması en kolay sınıflandırma algoritmalarından biridir. Geniş bir kullanım alanına sahiptir. Bu sınıflandırma algoritmasında, örnek verilerin veri özniteliklerinin sayısı olduğu n boyutlu bir uzayda çizilmektedir. n boyutlu uzaydaki her nokta, sınıf değeri ile etiketlenmektedir. Sınıflandırılmamış bir verinin sınıflandırılmasını keşfetmek için, n boyutlu uzayda çizilir ve en yakın k veri noktasının sınıf etiketleri not edilir. Genellikle k bir tek sayıdır. En yakın k veri noktası arasında maksimum sayıda oluşan sınıf, yeni veri noktasının sınıfı olarak alınır. Yani, karar k komşu noktanın oylanmasıyla verilmektedir. (Pandya, 2016; Arslan, 2020).

IBK algoritması temel olarak temel veri noktalarının etrafındaki "komşuları" kullanarak bir tahmin veya sınıflandırma yapmak için kullanılan bir makine öğrenmesi algoritmasıdır. Veri noktaları arasındaki mesafeyi hesaplayarak yeni bir veri noktasını sınıflandırır veya tahmin eder. Sınıflandırma ve regresyon problemleri için kullanılabilir. Eğitim aşaması yoktur. Sadece eğitim veri seti, modelin tahmin yaparken kullanacağı veri noktalarını içerir. Tıbbi teşhis, pazar analizi, görüntü tanıma, sosyal ağ analizi, spam filtreleme ve malzeme bilimi gibi birçok alanda kullanılmaktadır.

IBK algoritmasının avantaj ve dezavantajları bulunmaktadır.

Avantajları:

- ✓ Basit ve kolay anlaşılır; basit ve kolay anlaşılır olduğu için çok tercih edilen bir algoritmadır.
- ✓ Öğrenme süresi yok veya düşük; eğitim süresi yoktur. Sadece veri setinin depolanması gerekir. Model eğitimi sırasında hesaplama veya öğrenme işlemi gerçekleştirilmediğinden eğitim süresi önemli değildir.
- ✓ Parametrelerin ayarlanmasına gerek yoktur.
- ✓ Dirençlilik; veri setindeki gürültüye ve aykırı değerlere oldukça dirençlidir.
- ✓ Gerçek zamanlı tahminler; yeni örneklerle yapılan tahminler için hızlıdır ve gerçek zamanlı uygulamalarda kullanılabilir.
- ✓ Kullanım alanının genişliği; sınıflandırma, regresyon ve örüntü tanıma gibi birçok farklı problemin çözümünde kullanılabilir.,

Dezavantajları:

- ✓ Yüksek tahmin maliyeti; her yeni tahmin için, tüm veri seti üzerinde mesafe hesaplamaları yapılmalıdır. Büyük veri setleri için bu hesaplama maliyeti yüksek olabilir ve gerçek zamanlı uygulamalarda pratik olmayabilir.
- ✓ Depolama ihtiyacı; tüm eğitim veri setini hafızada saklar ve tahmin yaparken bu veriye erişim sağlar.
- ✓ Boyutluluğun laneti; özellikle yüksek boyutlu öznitelik uzaylarında boyutluluğun laneti olarak bilinen bir durumla karşılaşabilir.
- ✓ Aşırı öğrenme eğilimi; veri setindeki her bir noktayı kendi sınıfına ait olduğunu düşünerek kullanır.
- ✓ Eşitlik ve denge; veri setinde sınıf dengesizliği varsa, yani bir sınıf diğerlerine göre daha fazla temsil ediliyorsa, performansı etkilenebilir.

4.1.2. Performans metrikleri

Çalışmada, sınıflandırma modellerinin başarısını ölçmek için kullanılan performans metriklerinden aşağıda bahsedilmiştir. Tablo 4.2' de gösterilen karışıklık matrisi kullanılarak çalışmada uygulanan modellerde yapılan hatalar ve doğruluk oranları hakkında bilgi vermektedir.

Tablo 4.2. Karışıklık (confusion) matrisi

		TAHMİN EDİLEN DEĞERLER	
		Pozitif	Negatif
GERÇEK DEĞERLER	Pozitif	Doğru Pozitif (TP)	Yanlış Negatif (FN)
	Negatif	Yanlış Pozitif (FP)	Doğru Negatif (TN)

- **Doğru Pozitif (TP)**

Veri setinde kullanılan özellikler içerisinde nitelikli dolandırıcılık suçuna karışmış bir kişinin kullanılan sınıflandırma modeli tahmini sonucunda da nitelikli dolandırıcılık suçuna karışmış olarak çıkmasıdır.

- **Yanlış Pozitif (FP)**

Veri setinde kullanılan özellikler içerisinde bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna karışmamış bir kişinin kullanılan sınıflandırma modeli tahmini sonucunda bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna karışmış olarak çıkmasıdır.

- **Yanlış Negatif (FN)**

Veri setinde kullanılan özellikler içerisinde kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçuna karışmış bir kişinin kullanılan sınıflandırma modeli tahmini sonucunda kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçuna karışmamış olarak çıkmasıdır.

- **Doğru Negatif (TN)**

Veri setinde kullanılan özellikler içerisinde banka veya kredi kartlarını kötüye kullanmak suçuna karışmamış bir kişinin kullanılan sınıflandırma modeli tahmini sonucunda da banka veya kredi kartlarını kötüye kullanmak suçuna karışmamış olarak çıkmasıdır.

Tablo 4.2'den yola çıkarak kesinlik (precision) değeri denklem-1'deki formülle hesaplanmaktadır. Kesinlik değeri; pozitif olarak tahmin edilen örneklerin toplam veri sayısına bölünmesidir.

$$\text{Kesinlik(Precision)} = \frac{\text{TP}}{\text{TP+FP}} \tag{4.1}$$

Tablo 4.2'den yola çıkarak duyarlılık (recall) değeri denklem-2'deki formülle hesaplanmaktadır. Duyarlılık değeri; pozitif olarak tahmin edilmesi gereken verilerin oransal olarak kaçının doğru tahmin edildiğini göstermektedir.

$$\text{Duyarlılık(Recall)} = \frac{\text{TP}}{\text{TP+FN}} \tag{4.2}$$

Tablo 4.2'den yola çıkarak doğruluk (accuracy) değeri denklem-3'teki formülle hesaplanmaktadır. Doğruluk değeri; uygulanan modellerin tüm veri üzerinde ne kadar doğru tahmini yapıldığını göstermektedir.

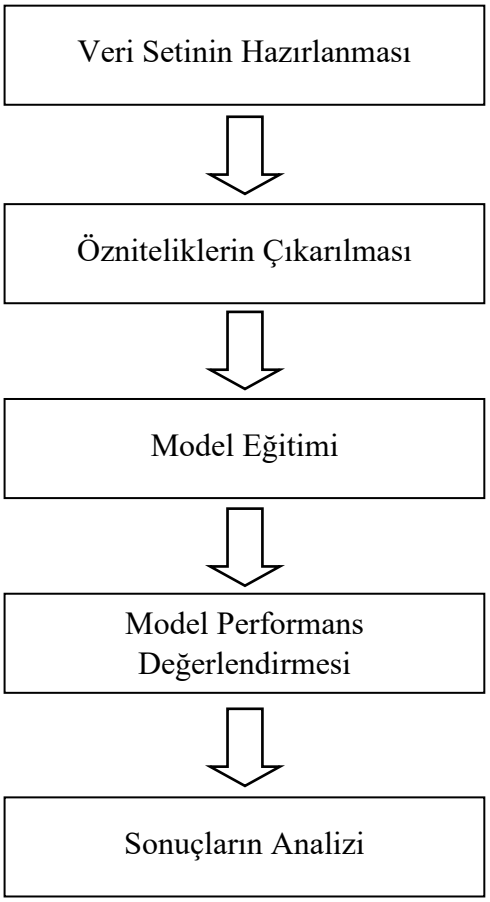
$$\text{Doğruluk(Accuracy)} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{4.3}$$

Tablo 4.2'den yola çıkarak F1 skorunun değeri denklem-4'teki formülle hesaplanmaktadır. F1 skoru; kesinlik ve duyarlılık değerlerinin harmonik ortalamasının alınmasıdır. F1 skoru en yüksek 1, en düşük olarak da 0 değerini alır. (Grandini ve diğ.,2020)

$$\text{F}_1 = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision+Recall}} \tag{4.4}$$

4.2. Sistem Metotları

Bu çalışmada ilk adım veri setinin hazırlanması olarak planlanmıştır. Bir sonraki adımda veri setine ait özniteliklerin çıkarılması bulunmaktadır. Çıkarılan özniteliklerin ve modelin eğitilmesi metodun üçüncü adımını oluşturmaktadır. Sonraki adımlarda ise modelin performans değerlendirmesi çıkarılarak sonuçların analiz edilmesi bulunmaktadır. Yapılan çalışmanın sistemine ilişkin metotlar Şekil 4.2'deki gibidir.



Şekil 4.2 Uygulanan metot

Yapılan çalışmada, 2020-2023 yılları arasında Yalova'da meydana gelen bilişim suçlarının tespit edilmesiyle 2500 adet veri toplanmıştır. Bu veriler üzerinde 11 özellik belirlenmiştir. Tüm bu işlemler tamamlandıktan sonra veri seti; RO, DVM, çok katmanlı YSA ve IBK gibi makine öğrenmesi algoritmalarıyla analiz edilmiştir.

Veri seti dosyasının okuma işlemi gerçekleştirildikten sonra veri seti içerisindeki kategorik değişkenler sayısallaştırılmıştır. Sayısallaştırılmış veriler içerisinde bulunan eksik veya hatalı verilere filtreleme işlemi uygulanmıştır. Veri seti (x ve y) eğitim ve test olarak ayrılmıştır. Train_test_split fonksiyonu kullanılarak x ve y veri kümesi rastgele seçilen veriler ile %80 eğitim ve %20 test verisi olarak bölünmüştür.

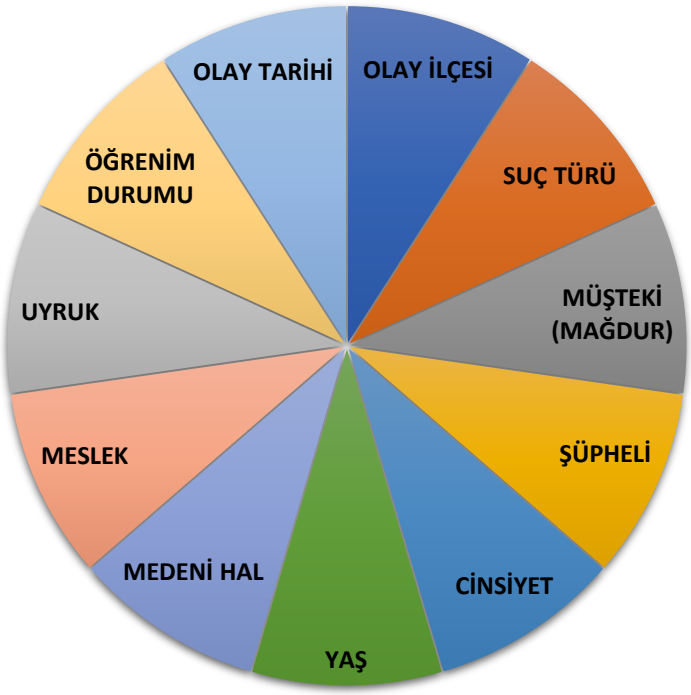
Model oluşturma işlemi RO, DVM, çok katmanlı YSA ve IBK makine öğrenmesi algoritmaları için uygulanmış ve eğitim işlemi gerçekleştirilmiştir. Eğitim veri seti (x_train ve y_train) üzerinden eğitilmiştir. Eğitilen model kullanılarak test veri kümesi üzerinden tahminler yapılmıştır. Tahmin sonuçları ve kullanılan modellerin doğruluğu hesaplanarak ekrana yazdırılmış ve karşılaştırma yapmak için gerekli performans değerleri elde edilmiştir.

4.3. Veri Analizi

Bu tez çalışmasında kullanılan veri seti Yalova ili sınırları içerisinde 2020-2023 yılları arasında meydana gelen bilişim suçlarını kapsamaktadır. Veri setinin oluşturulması safhasında Yalova Cumhuriyet Başsavcılığı siber suçlarla mücadele savcısı ile görüşülmüş ve meydana gelen bilişim suçları ile ilgili,

- Yalova ilinde meydana gelen bilişim suçu türleri,
- Bilişim suçlarına müdahil olan kişilerin genel özellikleri,
- Bilişim suçları tespitinin nasıl yapıldığı,
- Meydana gelen suçların aydınlatılma aşamaları,
- Bilişim suçlarının ortaya çıkartılmasında ne tür bilgilere ihtiyaç duyulduğu,
- Bilişim suçları analizinde kullanılan yöntemler hakkında bilgi alınmıştır.

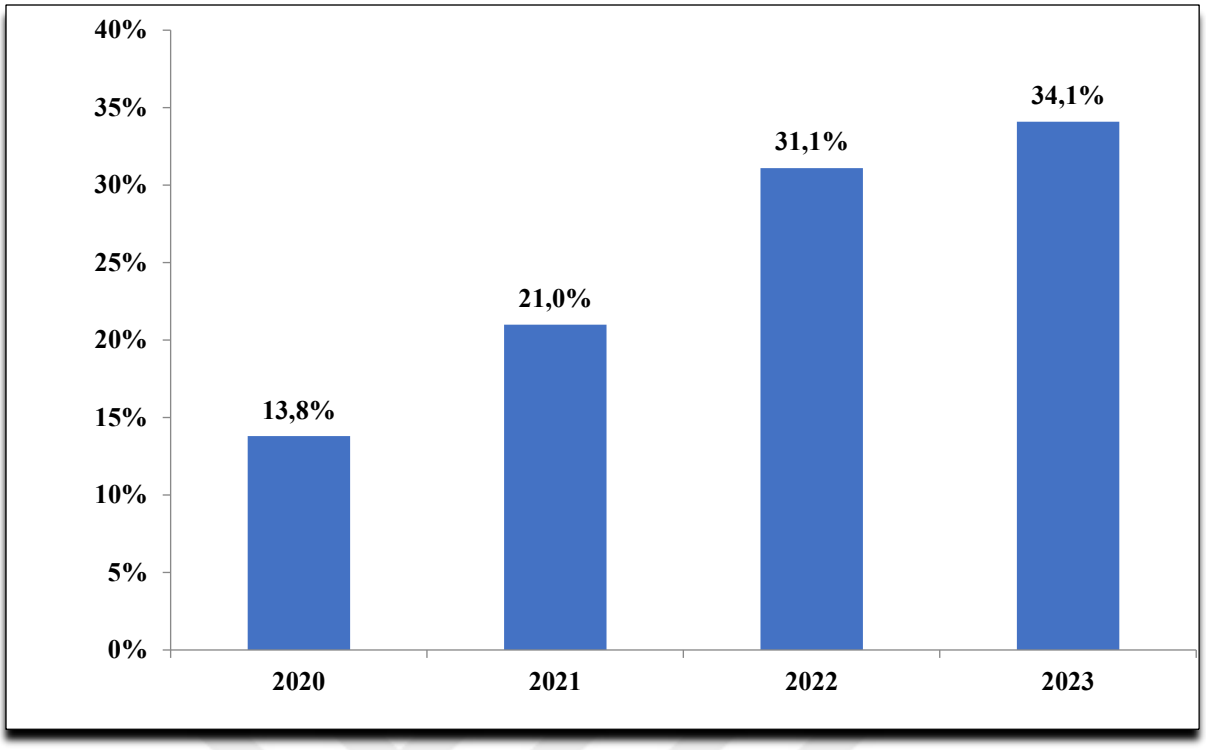
Alınan bilgiler doğrultusunda çalışmada kullanılmak üzere belirlenen özellikler Şekil 4.3'te verilmiştir.



Şekil 4.3. Veri setine ait özellikler

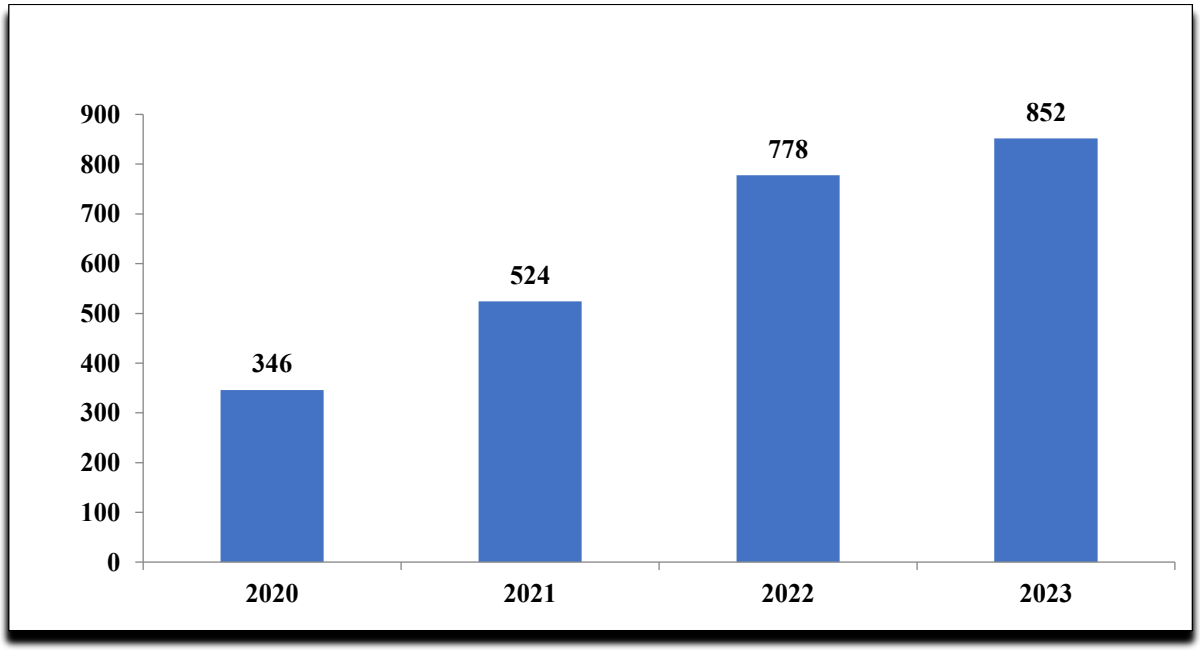
Yalova Cumhuriyet Başsavcılığı siber suçlarla mücadele savcısı koordinesinde tespit edilmiş olan; olay tarihi, olay ilçesi, suç türü, müşteki(mağdur), şüpheli, cinsiyet, yaş, medeni hal, meslek, uyruk, öğrenim durumu özniteliklerini de kapsayacak şekilde düzenlenen toplam 2500 adet veri, özel hayatın gizliliğini ihlal etmeyecek şekilde hazırlanarak Yalova Cumhuriyet Başsavcılığı tarafından çalışmada kullanılmak üzere verilmiştir.

Çalışma kapsamında kullanılan veri setinde Yalova ilinde 2020-2023 yılları arasında meydana gelen bilişim suçlarının yıllara göre dağılımına bakıldığında; 2020 yılı oranı %13.8, 2021 yılı oranı %21, 2022 yılı oranı %31.1, 2023 yılı oranı %34.1 olduğu Şekil 4.4'te gösterilmiştir.



Şekil 4.4. Meydana gelen bilişim suçu olaylarının yıllara göre dağılım oranları

Bilişim suçu olaylarının veri seti içerisindeki yıllara göre dağılımı incelendiğinde; 2020'de 346, 2021'de 524, 2022'de 778 ve 2023'te 852 olayın meydana geldiği Şekil 4.5.'te gösterilmiştir.

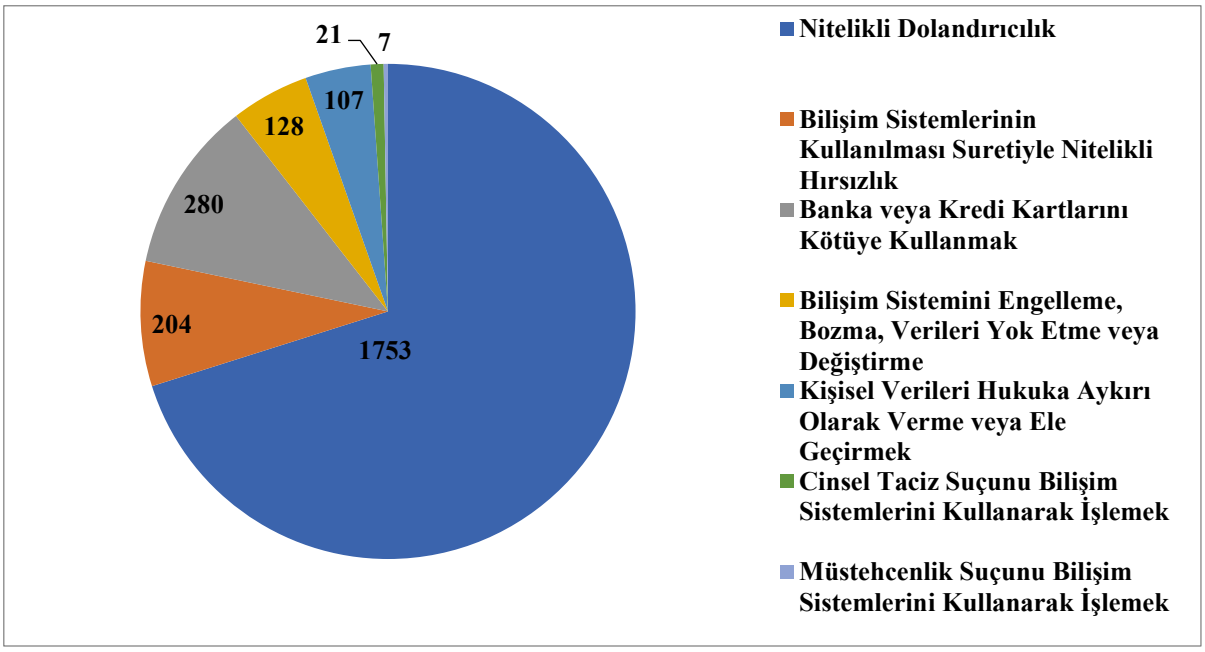


Şekil 4.5. Bilişim suçu olaylarının yıllara göre dağılımı

2020-2023 yılları arasında Yalova ilinde meydana gelen bilişim suçu türlerinin dağılımına bakıldığında; nitelikli dolandırıcılık suçu oranı %70.12, bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçu oranı %8.16, banka veya kredi kartlarını kötüye kullanmak suçu oranı %11.2, bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçu oranı %5.12, kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçu oranı %4.28, cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek suçu oranı %0.84 ve müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçu oranı %0.28 olduğu görülmüştür.

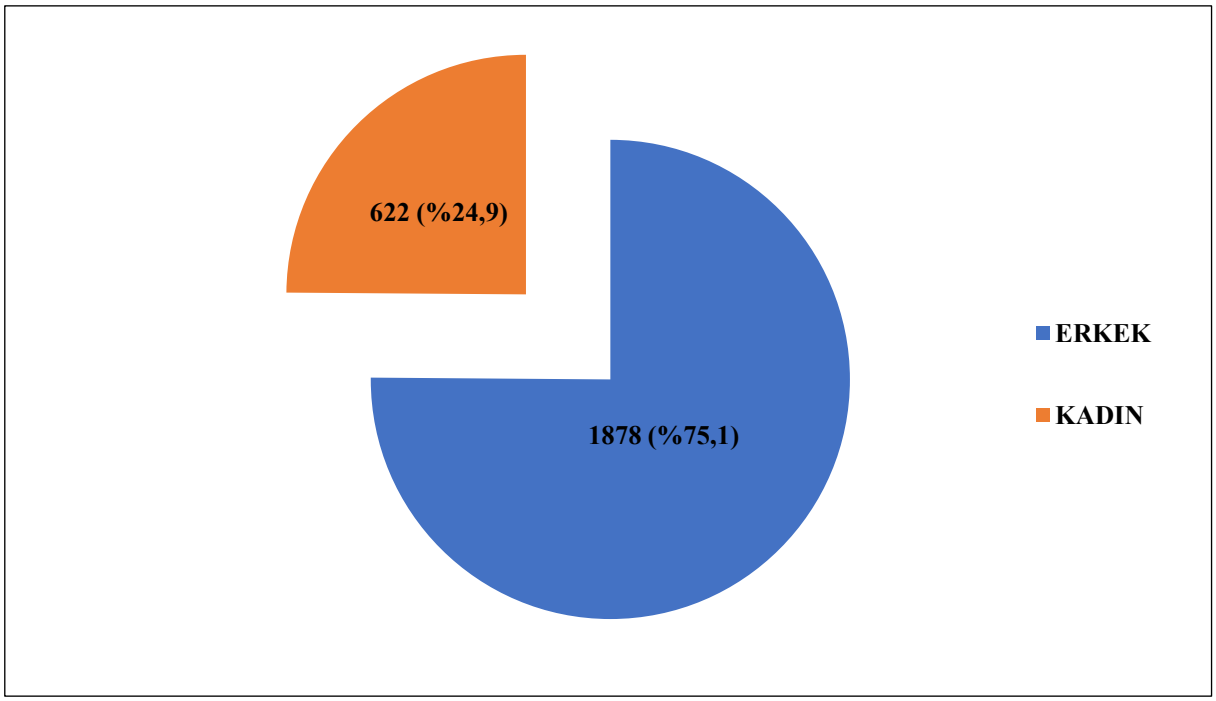
Veri setinde;

- ✓ 1753 adet nitelikli dolandırıcılık,
- ✓ 204 adet bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık,
- ✓ 280 adet banka veya kredi kartlarını kötüye kullanmak,
- ✓ 128 adet bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme,
- ✓ 107 adet kişisel verileri hukuka aykırı olarak verme veya ele geçirmek,
- ✓ 21 adet cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek,
- ✓ 7 adet müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçu olmak üzere toplam 2500 adet veri olduğu tespit edilmiştir. Bilişim suçu türlerinin dağılımı Şekil 4.6.'da verilmiştir.



Şekil 4.6. Bilişim suçu türlerinin dağılımı

2020-2023 yılları arasında Yalova ilinde meydana gelen bilişim suçu türlerinin cinsiyet dağılımı incelendiğinde bilişim suçunu işleyen 1878 adet erkek, 622 kadın olduğu görülmektedir. Erkeklerin veri setindeki oranı %75.1, kadınların ise %24.9 olduğu Şekil 4.7'de verilmiştir.

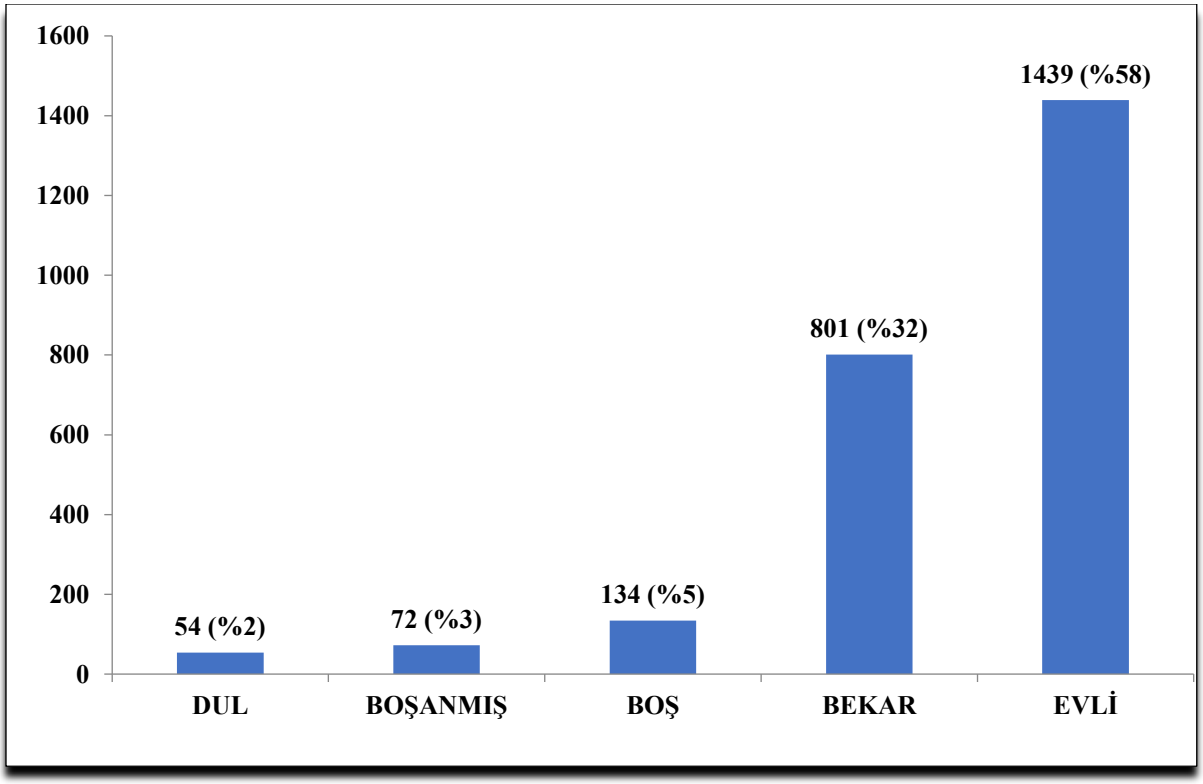


Şekil 4.7. Bilişim suçlarına karışan kişilerin cinsiyet dağılım ve oranları

- Olaylara karışan 1878 erkeğin;
  - ✓ 1369 tanesi nitelikli dolandırıcılık,
  - ✓ 151 tanesi bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık,
  - ✓ 206 tanesi banka veya kredi kartlarını kötüye kullanmak,
  - ✓ 70 tanesi bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme,
  - ✓ 64 tanesi kişisel verileri hukuka aykırı olarak verme veya ele geçirmek,
  - ✓ 13 tanesi cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek,
  - ✓ 5 tanesi müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.
- Olaylara karışan 622 kadının;
  - ✓ 384 tanesi nitelikli dolandırıcılık,
  - ✓ 53 tanesi bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık,
  - ✓ 74 tanesi banka veya kredi kartlarını kötüye kullanmak,
  - ✓ 58 tanesi bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme,

- ✓ 43 tanesi kişisel verileri hukuka aykırı olarak verme veya ele geçirmek,
- ✓ 8 tanesi cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek,
- ✓ 2 tanesi müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.

Veri setinin medeni durumlarına göre dağılımları incelendiğinde; 1439 evli, 801 bekar, 134 medeni durumu belli olmayan (boş), 72 boşanmış ve 54 dul kişilerden oluştuğu tespit edilmiştir. Evlilerin veri seti içerisindeki oranı %58, bekarların %32 medeni durumu belli olmayanların (boş) %5, boşanmışların %3 ve dulların %2 olduğu anlaşılmış medeni durum dağılımları Şekil 4.8.'de verilmiştir.

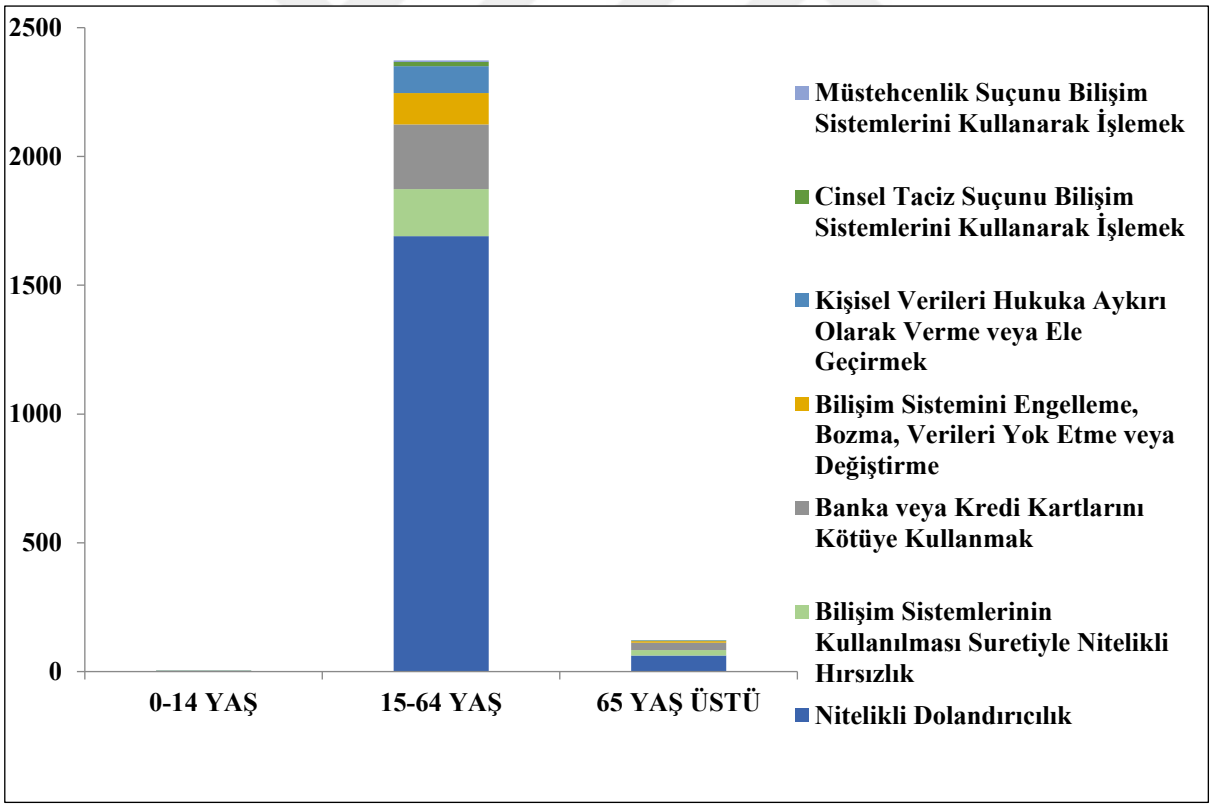


Şekil 4.8. Medeni durum dağılımı

2020-2023 yılları arasında meydana gelen bilişim suçlarına karışan kişilerin yaş dağılımına bakıldığında;

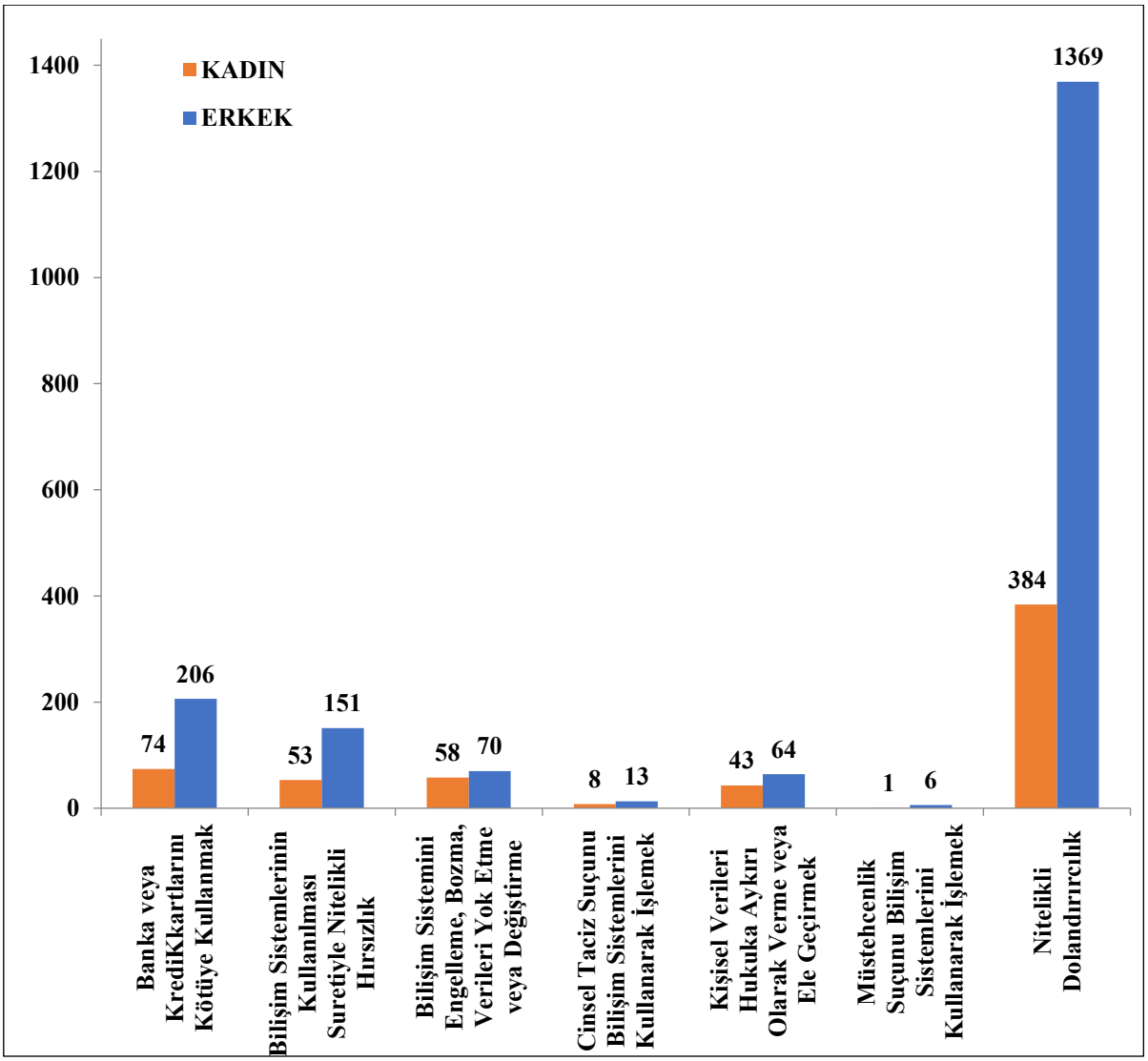
- 0-14 yaş aralığında olaylara karışan 5 kişinin; 1 tanesinin nitelikli dolandırıcılık, 3 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 1 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karıştığı anlaşılmıştır.

- 15-64 yaş aralığında olaylara karışan 2373 kişinin; 1690 tanesinin nitelikli dolandırıcılık, 183 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 251 tanesinin banka veya kredi kartlarını kötüye kullanmak, 122 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 104 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 17 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 6 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karıştığı anlaşılmıştır.
- 65 yaş ve üzeri olaylara karışan 122 kişinin; 62 tanesinin nitelikli dolandırıcılık, 21 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 29 tanesinin banka veya kredi kartlarını kötüye kullanmak, 6 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 3 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 1 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek suçlarına karıştığı anlaşılmıştır. Bilişim suçlarına karışan kişilerin yaş grup dağılımları Şekil 4.9.'da verilmiştir.



Şekil 4.9. Bilişim suçlarına karışan kişilerin yaş grupları

2020-2023 yılları arasında Yalova ilinde meydana gelen bilişim suçları içerisinde; banka veya kredi kartlarını kötüye kullanmak suçuna karışan erkek sayısı 206, kadın sayısı 74, bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçuna karışan erkek sayısı 151, kadın sayısı 53, bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna karışan erkek sayısı 70, kadın sayısı 58, cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek suçuna karışan erkek sayısı 13, kadın sayısı 8, kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçuna karışan erkek sayısı 64, kadın sayısı 43, müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçuna karışan erkek sayısı 6, kadın sayısı 1, nitelikli dolandırıcılık suçuna karışan erkek sayısı 1369, kadın sayısı 384'dür. Bilişim suçları içerisindeki cinsiyet dağılım ve sayıları Şekil 4.10.'da verilmiştir.



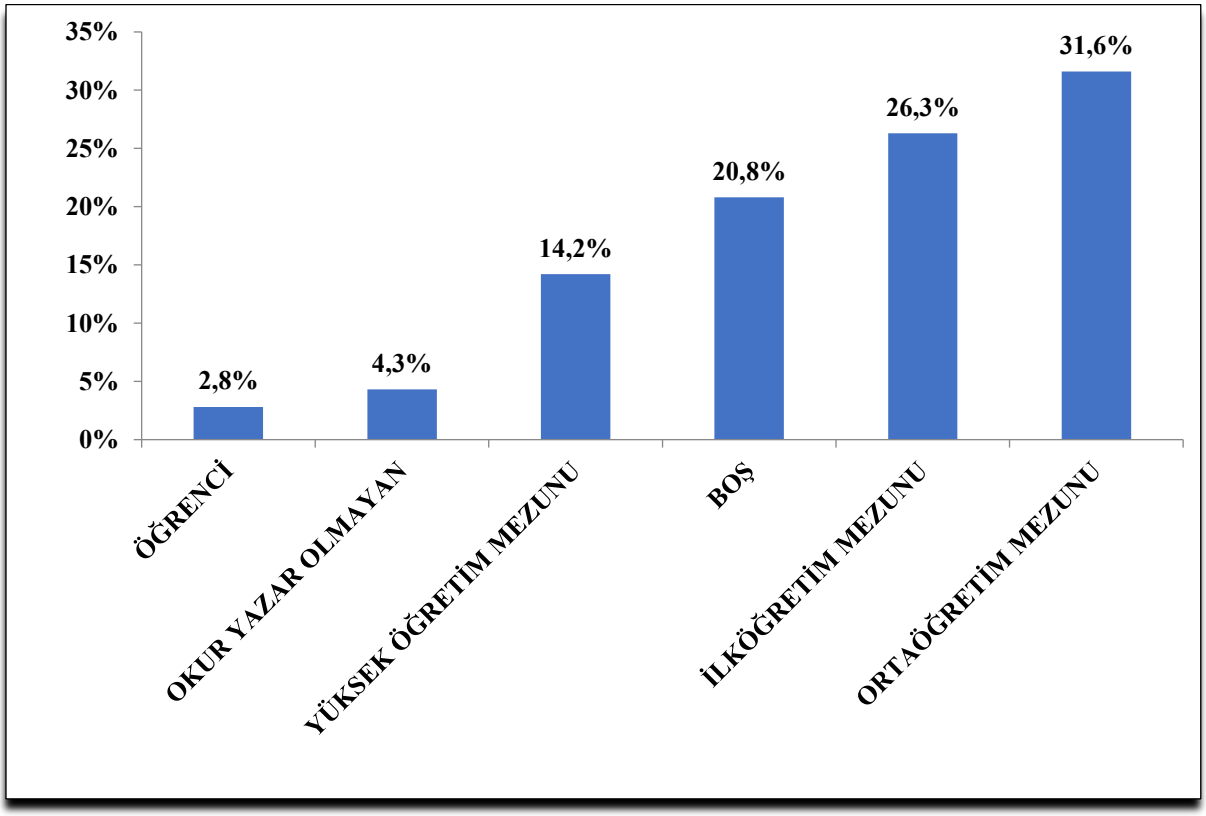
Şekil 4.10. Bilişim suçları içerisindeki cinsiyet dağılımı ve sayıları

Çalışmada bilişim suçlarına karışan kişilerden; 108 tanesinin okur yazar olmadığı, 657 tanesinin ilköğretim mezunu, 790 tanesinin ortaöğretim mezunu, 355 tanesinin yükseköğretim mezunu, 71 tanesinin öğrenci olduğu görülmüştür.

- Okuryazar olmayan 108 kişinin; 78 tanesinin nitelikli dolandırıcılık, 20 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 5 tanesinin banka veya kredi kartlarının kötüye kullanılması suçuna, 5 tanesinin ise bilişim sistemlerini engelleme, bozma, verileri yok etme veya değiştirme suçlarına karışmıştır.
- İlköğretim mezunu 657 kişinin; 427 tanesinin nitelikli dolandırıcılık, 46 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 107 tanesinin banka veya kredi kartlarını kötüye kullanmak, 32 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 35 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 8 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 2 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.
- Ortaöğretim mezunu 790 kişinin; 571 tanesinin nitelikli dolandırıcılık, 53 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 77 tanesinin banka veya kredi kartlarını kötüye kullanmak, 43 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 39 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 6 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 1 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.
- Yükseköğretim mezunu 355 kişinin; 262 tanesinin nitelikli dolandırıcılık, 15 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 47 tanesinin banka veya kredi kartlarını kötüye kullanmak, 13 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 16 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 2 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.
- Öğrenci olan 71 kişinin; 44 tanesinin nitelikli dolandırıcılık, 1 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 7 tanesinin banka veya kredi kartlarını kötüye kullanmak, 9 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 9 tanesinin kişisel verileri hukuka aykırı olarak verme veya

ele geçirmek, 1 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek suçlarına karışmıştır.

Veri seti içerisinde; okur yazar olmayanların oranı %4.32, ilköğretim mezunlarının oranı %26.28, ortaöğretim mezunlarının oranı %31.6, yükseköğretim mezunlarının oranı %14.2, öğrencilerin oranı %2.84 olduğu, tespit edilmiştir. Veri seti içerisindeki kişilerin eğitim durum oranları Şekil 4.11.'de verilmiştir.

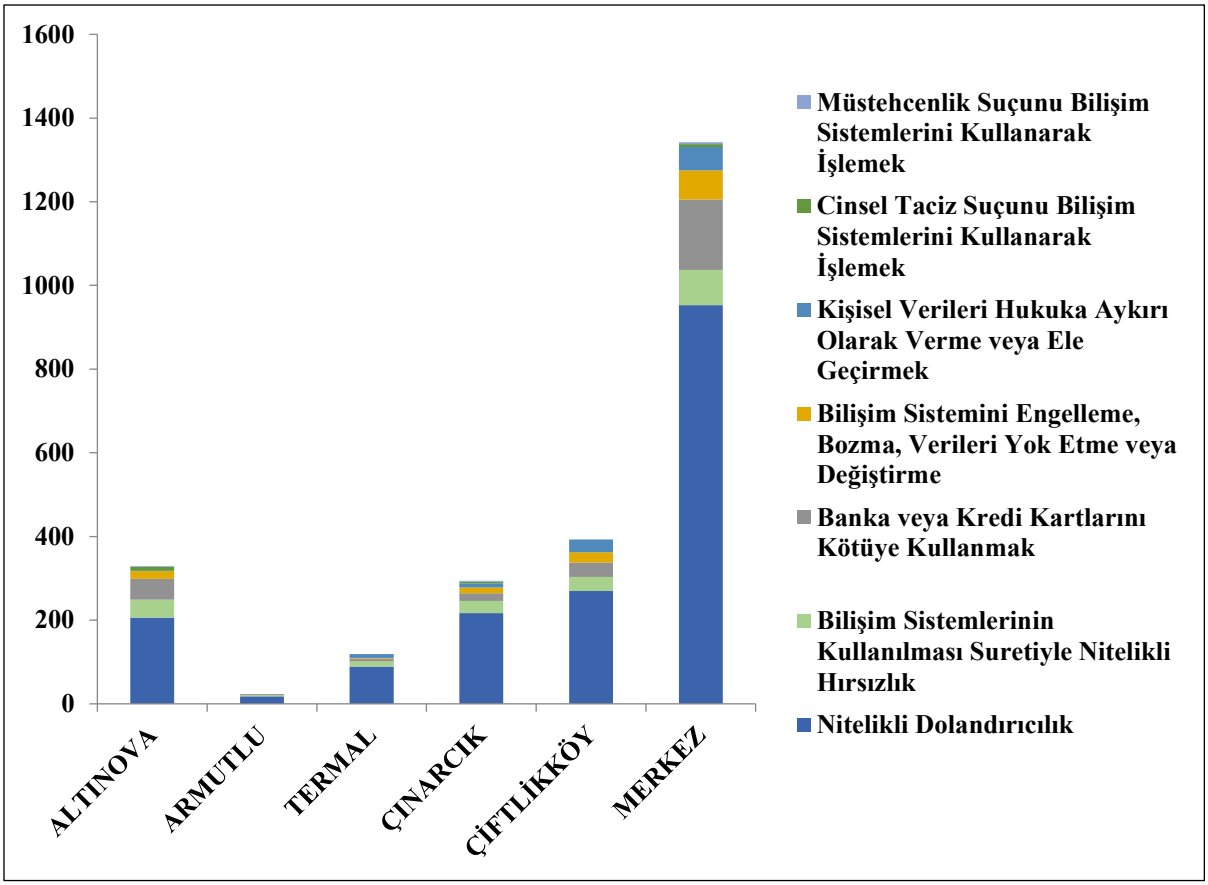


Şekil 4.11. Veri seti içerisindeki kişilerin eğitim durumları

Yalova ilçelerinde meydana gelen bilişim suçlarının dağılımına bakıldığında;

- Altınova ilçesinde meydana gelen 329 olayın; 206 tanesinin nitelikli dolandırıcılık, 43 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 50 tanesinin banka veya kredi kartlarını kötüye kullanmak, 18 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 1 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 10 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 1 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçları olduğu görülmüştür.

- Armutlu ilçesinde meydana gelen 23 olayın; 18 tanesinin nitelikli dolandırıcılık, 3 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 2 tanesinin banka veya kredi kartlarını kötüye kullanmak suçları olduğu görülmüştür.
- Merkez ilçesinde meydana gelen 1342 olayın; 953 tanesinin nitelikli dolandırıcılık, 84 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 168 tanesinin banka veya kredi kartlarını kötüye kullanmak, 70 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 56 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 7 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 4 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçları olduğu görülmüştür.
- Termal ilçesinde meydana gelen 119 olayın; 89 tanesinin nitelikli dolandırıcılık, 12 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 7 tanesinin banka veya kredi kartlarını kötüye kullanmak, 2 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 9 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçları olduğu görülmüştür.
- Çınarcık ilçesinde meydana gelen 294 olayın; 217 tanesinin nitelikli dolandırıcılık, 29 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 18 tanesinin banka veya kredi kartlarını kötüye kullanmak, 14 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 10 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek, 4 tanesinin cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek, 2 tanesinin müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçları olduğu görülmüştür.
- Çiftlikköy ilçesinde meydana gelen 393 olayın; 270 tanesinin nitelikli dolandırıcılık, 33 tanesinin bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, 35 tanesinin banka veya kredi kartlarını kötüye kullanmak, 24 tanesinin bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, 31 tanesinin kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçları olduğu görülmüştür. Yalova ili ilçelerinde meydana gelen bilişim suçlarının dağılımı Şekil 4.12.'de verilmiştir.



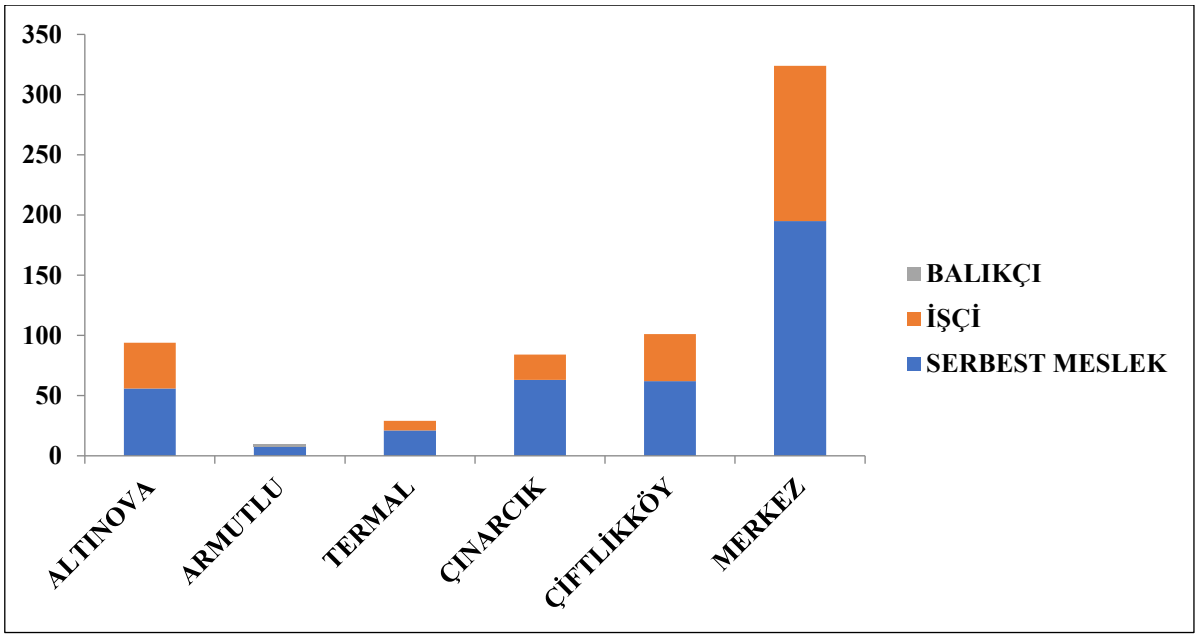
Şekil 4.12. Yalova ili ilçelerinde meydana gelen bilişim suçlarının dağılımı

Yalova ilçelerinde 2020-2023 yılları arasında meydana gelen bilişim suçlarına ait olaylara karışan en çok hangi iki meslek grubu olduğuna dair dağılımına bakıldığında;

- Altınova ilçesinde toplam 329 olayın meydana geldiği, bunlar içerisinde en fazla 206 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 56 kişiyle serbest meslek ve 38 kişiyle işçi meslek gruplarından olduğu belirlenmiştir.
- Merkez ilçesinde toplam 1342 olayın meydana geldiği, bunlar içerisinde en fazla 953 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 195 kişiyle serbest meslek ve 129 kişiyle işçi meslek gruplarından olduğu belirlenmiştir.
- Armutlu ilçesinde toplam 23 olayın meydana geldiği, bunlar içerisinde en fazla 18 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 8 kişiyle serbest meslek ve 2 kişiyle balıkçı meslek gruplarından olduğu belirlenmiştir.

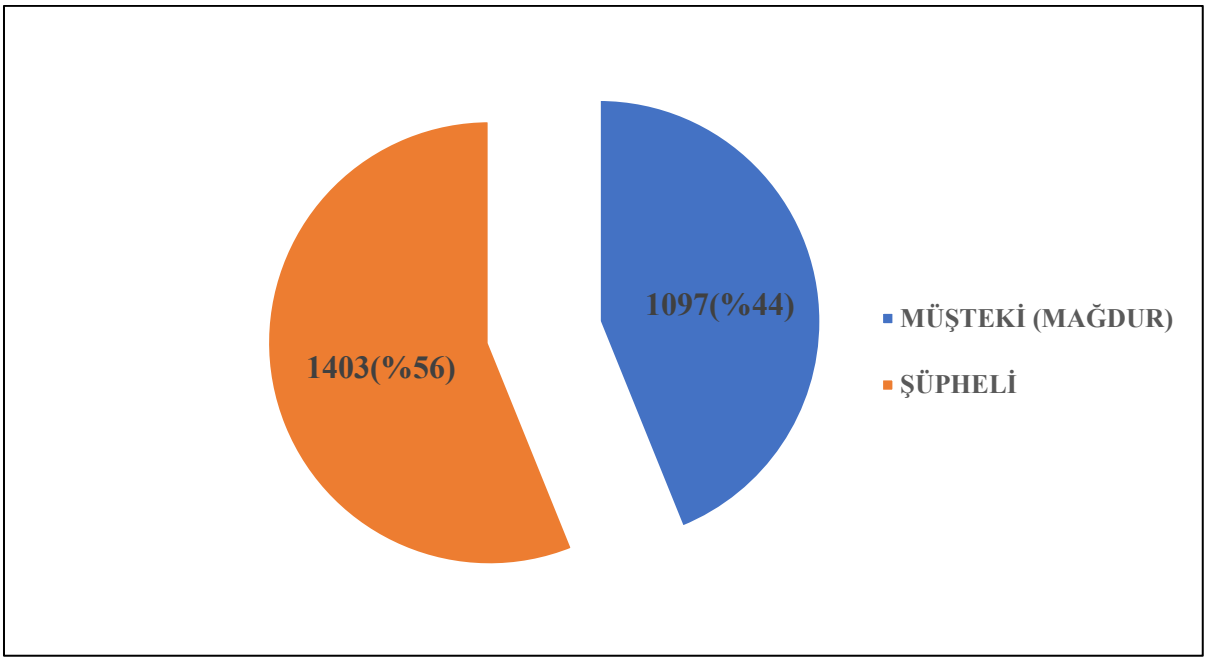
- Termal ilçesinde toplam 119 olayın meydana geldiği, bunlar içerisinde en fazla 89 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 21 kişiyle serbest meslek ve 8 kişiyle işçi meslek gruplarından olduğu belirlenmiştir.
- Çınarcık ilçesinde toplam 294 olayın meydana geldiği, bunlar içerisinde en fazla 217 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 63 kişiyle serbest meslek ve 21 kişiyle işçi meslek gruplarından olduğu belirlenmiştir.
- Çiftlikköy ilçesinde toplam 393 olayın meydana geldiği, bunlar içerisinde en fazla 270 olay ile nitelikli dolandırıcılık suçuna karışıldığı görülmüştür. Nitelikli dolandırıcılık suçuna karışan kişilerin en çok 62 kişiyle serbest meslek ve 39 kişiyle işçi meslek gruplarından olduğu belirlenmiştir.

Yalova ilçelerinde 2020-2023 yılları arasında meydana gelen bilişim suçlarına ait olaylara karışan en çok hangi iki meslek grubu olduğuna dair dağılımı Şekil 4.13.'de verilmiştir.



Şekil 4.13. Yalova ilçelerinde meydana gelen bilişim suçlarının meslek dağılımı

Yalova ilinde meydana gelmiş 2500 adet bilişim suçuna müdahil olan kişilerin müşteki (mağdur) ve şüpheli durum dağılımları incelendiğinde; müştekilerin (mağdur) 1097 adet, şüphelilerin 1403 adet olduğu, müştekilerin (mağdur) veri seti içerisindeki dağılım oranı %44, şüphelilerin ise %56 olduğu Şekil 4.14'de verilmiştir.



Şekil 4.14. Bilişim suçlarına karışan kişilerin olay taraf dağılım ve oranları

5. BULGULAR

2020-2023 yılları arası Yalova ilinde meydana gelmiş bilişim suçlarıyla ilgili olaylara karışan kişilerin; müşteki (mağdur) veya şüpheli olup olmadıkları durumu ile bilişim suçu türlerinden olan; banka veya kredi kartlarını kötüye kullanmak, bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, kişisel verileri hukuka aykırı olarak verme veya ele geçirmek ve nitelikli dolandırıcılık suçlarından hangisine müdahil oldukları durumu makine öğrenmesi algoritmalarından RO, DVM, çok katmanlı YSA ve IBK algoritmalarıyla analiz edilerek performansları test edilmiştir.

Veri seti içerisinde bulunan bilişim suçu türlerinden cinsel taciz suçunu bilişim sistemlerini kullanarak işlemek ve müstehcenlik suçunu bilişim sistemlerini kullanarak işlemek suçlarının veri sayısının az olmasından dolayı performans değerlerini etkilediğinden veri setinden çıkarılmıştır.

Yalova ilinde meydana gelmiş bilişim suçlarına karışan kişilerin, müşteki (mağdur) veya şüpheli olup olmadıkları durumu ile ilgili makine öğrenmesi algoritmalarıyla yapılan analizlerde;

Müşteki (mağdur) özniteliğine ait DVM sınıflandırma algoritmasından radyal temel fonksiyonunun doğruluk değeri 0.79, polinom' un doğruluk değeri 0.69, doğrusalın doğruluk değeri 0.80 ve sigmoid' in doğruluk değeri 0.83 olup en yüksek doğruluk değeri sigmoid de elde edilmiştir. Diğer performans değerleri Tablo 5.1.'de verilmiştir.

Tablo 5.1. DVM algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Radyal Temel Fonksiyonu (RBF)	0.77	0.88	0.82
Polinom (Poly)	0.65	0.96	0.77
Doğrusal (Linear)	0.79	0.88	0.83
Sigmoid	0.82	0.88	0.85

Çok katmanlı YSA algoritmasının doğruluk değeri 0.79'dur. Diğer performans değerleri Tablo 5.2.'de verilmiştir.

Tablo 5.2. Çok katmanlı YSA algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Çok katmanlı YSA Algoritması	0.80	0.84	0.82

RO algoritmasının doğruluk değeri 0.83'tür. Diğer performans değerleri Tablo 5.3.'de verilmiştir.

Tablo 5.3. RO algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
RO Algoritması	0.86	0.84	0.85

IBK algoritmasının doğruluk değeri 0.79'dur. Diğer performans değerleri Tablo 5.4.'de verilmiştir.

Tablo 5.4. IBK algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
IBK Algoritması	0.81	0.82	0.82

Tüm sınıflandırma algoritmalarının performans değerleri Tablo 5.5'te verilmiştir.

Tablo 5.5. Sınıflandırma algoritmalarının performans değerleri karşılaştırması

	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
DVM- Radyal Temel Fonksiyonu (RBF)	0.79	0.77	0.88	0.82
DVM-Polinom (Poly)	0.69	0.65	0.96	0.77
DVM-Doğrusal (Linear)	0.80	0.79	0.88	0,83
DVM-Sigmoid	0.83	0.82	0.88	0.85
Çok Katmanlı YSA	0.79	0.80	0.84	0.82
RO	0.83	0.86	0.84	0.85
IBK	0.79	0.81	0.82	0.82

Yukarıdaki tablo incelendiğinde en yüksek doğruluk değerleri DVM-sigmoid ve RO algoritmalarında alınırken, en düşük doğruluk değeri DVM-polinom algoritmasından alınmıştır.

Yalova ilinde meydana gelmiş bilişim suçlarına karışan kişilerin, bilişim suçu türlerinden;

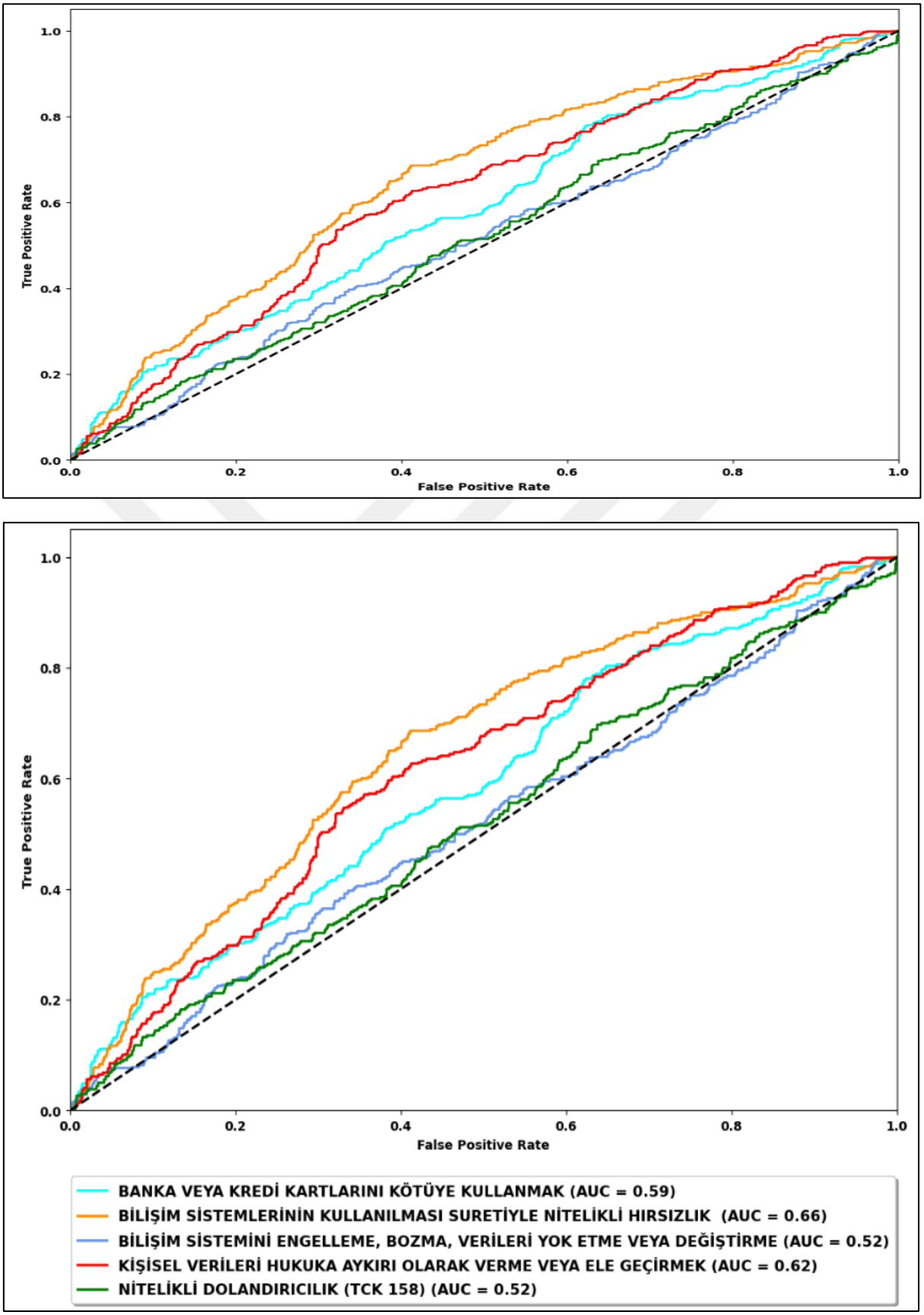
- ✓ Banka veya kredi kartlarını kötüye kullanmak,
- ✓ Bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık,
- ✓ Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme,
- ✓ Kişisel verileri hukuka aykırı olarak verme veya ele geçirmek,
- ✓ Nitelikli dolandırıcılık suçlarından hangisine müdahil oldukları durumuyla ilgili makine öğrenmesi algoritmalarıyla yapılan analizlerde;
- ✓ DVM algoritmasının doğruluk değeri 0.82'dir. Diğer performans değerleri Tablo 5.6.'da verilmiştir.

Tablo 5.6. Bilişim suçu türlerine ait DVM algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Banka veya Kredi Kartlarını Kötüye Kullanmak	0.80	0.85	0.83
Bilişim Sistemlerinin Kullanılması Suretiyle Nitelikli Hırsızlık	0.80	0.87	0.83
Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	0.88	0.89	0.88
Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirmek	0.82	0.89	0.85
Nitelikli Dolandırıcılık	0.77	0.58	0.66

DVM algoritmasına ait çok sınıflı ROC eğrilerinde; banka veya kredi kartlarını kötüye kullanmak (turkuaz), bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık (kahverengi), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (mavi), kişisel verileri hukuka aykırı olarak verme veya ele geçirmek (kırmızı), nitelikli dolandırıcılık (yeşil) suçları bulunmaktadır.

DVM algoritmasına ait çok sınıflı ROC eğrilerinde en yüksek performans (AUC) değeri 0.66 ile bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçundan alınırken, en düşük 0.52 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme ve nitelikli dolandırıcılık suçlarından alınmıştır. DVM algoritmasına ait çok sınıflı ROC eğrileri Şekil 5.1.'de verilmiştir.



Şekil 5.1. DVM algoritması çok sınıflı ROC eğrileri

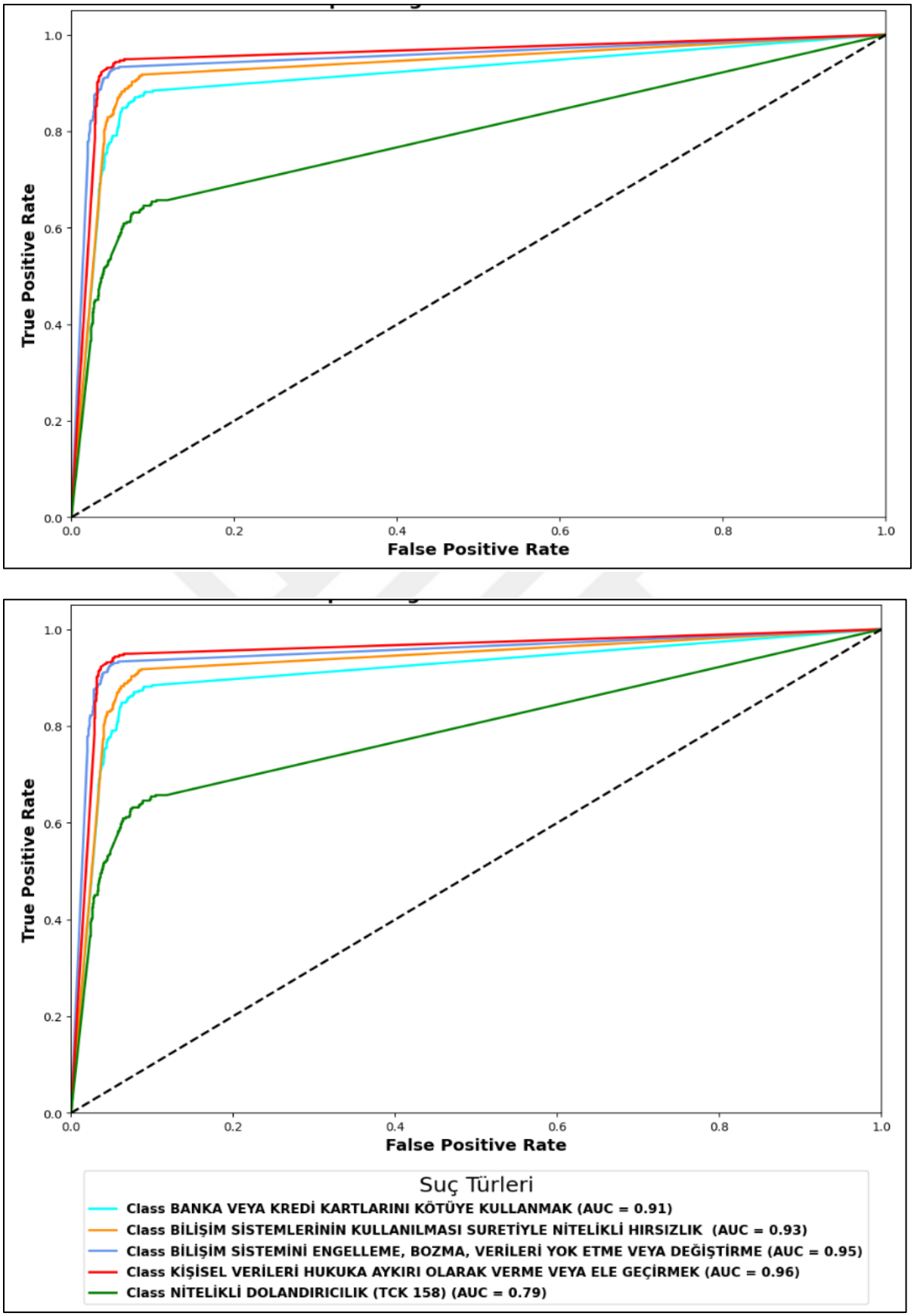
Çok katmanlı YSA algoritmasının doğruluk değeri 0.82'dir. Diğer performans değerleri Tablo 5.7.'de verilmiştir.

Tablo 5.7. Bilişim suçu türlerine ait çok katmanlı YSA algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Banka veya Kredi Kartlarını Kötüye Kullanmak	0.82	0.79	0.81
Bilişim Sistemlerinin Kullanılması Suretiyle Nitelikli Hırsızlık	0.84	0.86	0.85
Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	0.86	0.90	0.88
Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirmek	0.85	0.94	0.89
Nitelikli Dolandırıcılık	0.71	0.60	0.65

Çok katmanlı YSA algoritmasına ait çok sınıflı ROC eğrilerinde; banka veya kredi kartlarını kötüye kullanmak (turkuaz), bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık (kahverengi), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (mavi), kişisel verileri hukuka aykırı olarak verme veya ele geçirmek (kırmızı), nitelikli dolandırıcılık (yeşil) suçları bulunmaktadır.

Çok katmanlı YSA algoritmasına ait çok sınıflı ROC eğrilerinde en yüksek performans (AUC) değeri 0.96 ile kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçundan alınırken, en düşük 0.79 ile nitelikli dolandırıcılık suçundan alınmıştır. Çok katmanlı YSA algoritmasına ait çok sınıflı ROC eğrileri Şekil 5.2.'de verilmiştir.



Şekil 5.2. Çok katmanlı YSA algoritması çok sınıflı ROC eğrileri

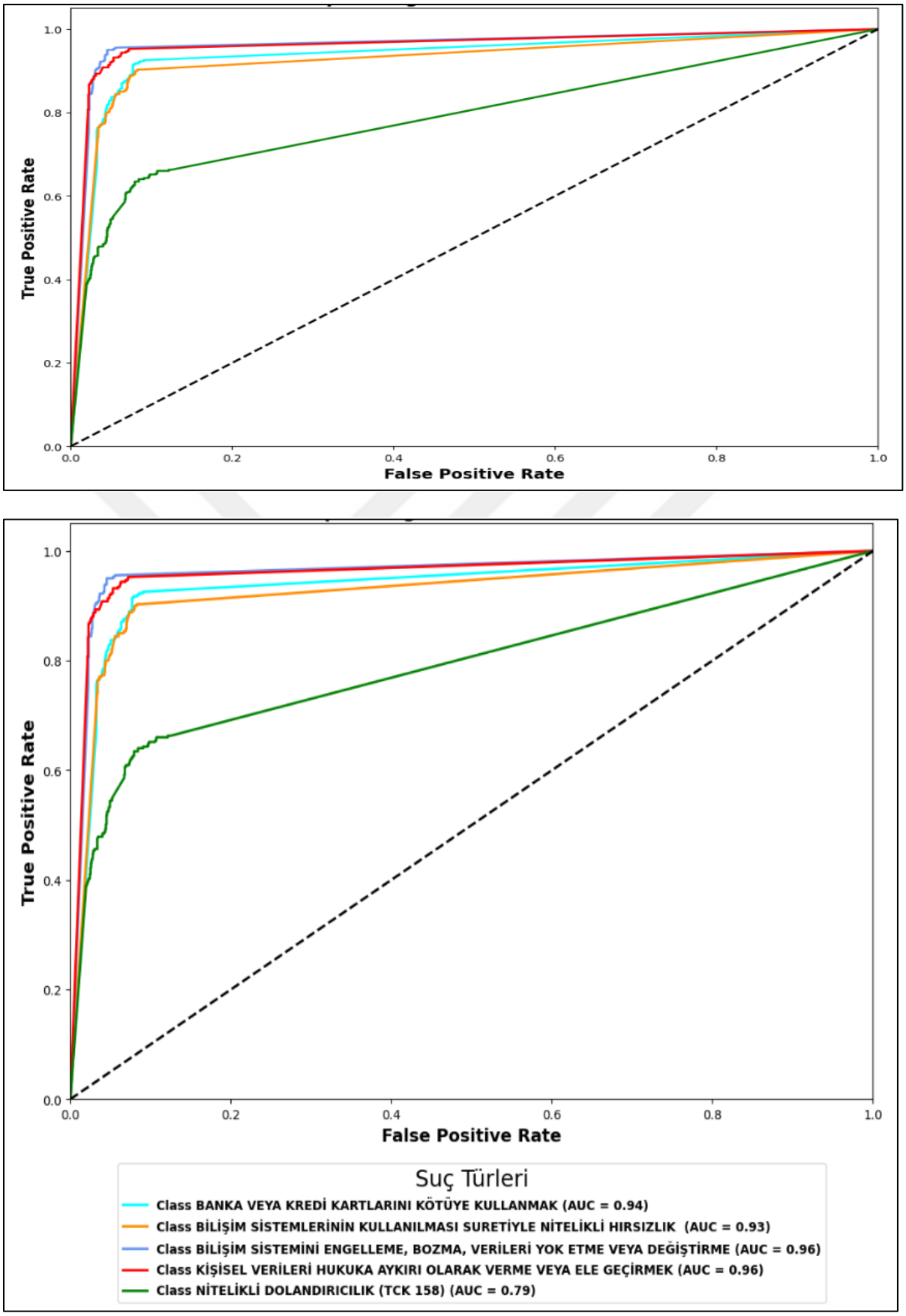
RO algoritmasının doğruluk değeri 0.85'tir. Diğer performans değerleri Tablo 5.8.'de verilmiştir.

Tablo 5.8. Bilişim suçu türlerine ait RO algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Banka veya Kredi Kartlarını Kötüye Kullanmak	0.82	0.85	0.84
Bilişim Sistemlerinin Kullanılması Suretiyle Nitelikli Hırsızlık	0.86	0.82	0.84
Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	0.90	0.90	0.90
Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirmek	0.87	0.91	0.89
Nitelikli Dolandırıcılık	0.80	0.78	0.79

RO algoritmasına ait çok sınıflı ROC eğrilerinde; banka veya kredi kartlarını kötüye kullanmak (turkuaz), bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık (kahverengi), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (mavi), kişisel verileri hukuka aykırı olarak verme veya ele geçirmek (kırmızı), nitelikli dolandırıcılık (yeşil) suçları bulunmaktadır.

RO algoritmasına ait çok sınıflı ROC eğrilerinde en yüksek performans (AUC) değeri 0.96 ile kişisel verileri hukuka aykırı olarak verme veya ele geçirmek ve bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarından alınırken, en düşük 0.79 ile nitelikli dolandırıcılık suçundan alınmıştır. RO algoritmasına ait çok sınıflı ROC eğrileri Şekil 5.3.'de verilmiştir.



Şekil 5.3. RO algoritması çok sınıflı ROC eğrileri

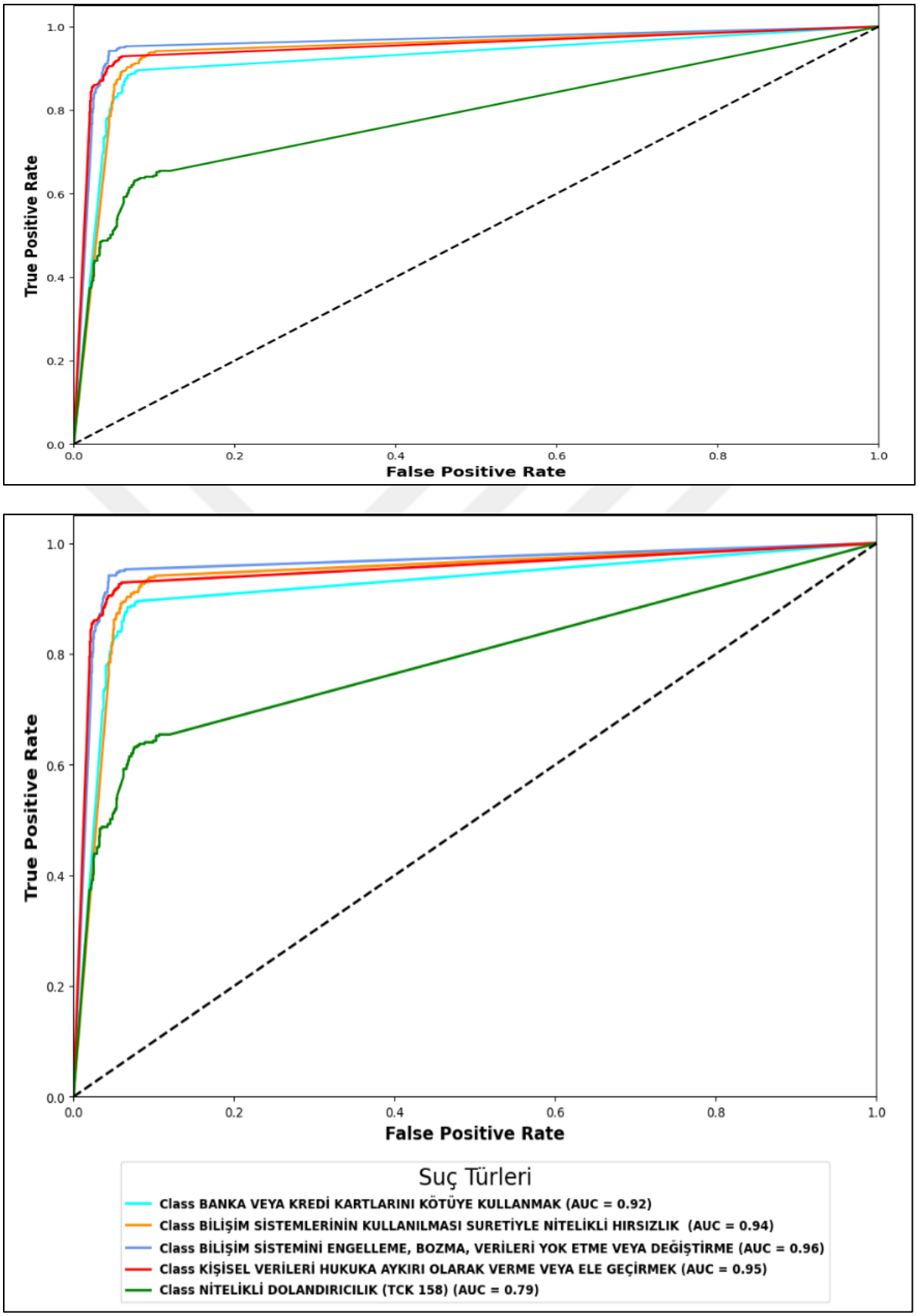
IBK algoritmasının doğruluk değeri 0.81'dir. Diğer performans değerleri Tablo 5.9.'da verilmiştir.

Tablo 5.9. Bilişim suçu türlerine ait IBK algoritması performans değerleri

	Kesinlik	Duyarlılık	F1 Skoru
Banka veya Kredi Kartlarını Kötüye Kullanmak	0.77	0.87	0.82
Bilişim Sistemlerinin Kullanılması Suretiyle Nitelikli Hırsızlık	0.78	0.87	0.82
Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme	0.88	0.90	0.89
Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirmek	0.85	0.87	0.86
Nitelikli Dolandırıcılık	0.75	0.54	0.62

IBK algoritmasına ait çok sınıflı ROC eğrilerinde; banka veya kredi kartlarını kötüye kullanmak (turkuaz), bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık (kahverengi), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme (mavi), kişisel verileri hukuka aykırı olarak verme veya ele geçirmek (kırmızı), nitelikli dolandırıcılık (yeşil) suçları bulunmaktadır.

IBK algoritmasına ait çok sınıflı ROC eğrilerinde en yüksek performans (AUC) değeri 0.96 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçundan alınırken, en düşük 0.79 ile nitelikli dolandırıcılık suçundan alınmıştır. IBK algoritmasına ait çok sınıflı ROC eğrileri Şekil 5.4.'de verilmiştir.



Şekil 5.4. IBK algoritması çok sınıflı ROC eğrileri

6. SONUÇLAR VE ÖNERİLER

Yapılmış olan çalışmada kullanılan makine öğrenmesi modellerinin 2020-2023 yılları arasında Yalova ilinde meydana gelmiş bilişim suçları üzerindeki performansları karşılaştırılmıştır. Bu analiz ile hangi modellerin suç tahmininde daha etkili olduğu ve modeller arasındaki farklılıkların neler olduğu tespit edilmiştir. Bu süreçte meydana gelmiş bilişim suçları ile mücadelede hangi makine öğrenmesi algoritmalarının daha etkili olduğunu belirlenmiştir.

Yalova'da meydana gelmiş bilişim suçu olaylarına karışan kişilerin müşteki (mağdur) mi şüpheli mi olduğuna dair yapılan analiz ile ilgili olarak Tablo 5.5 incelendiğinde müşteki (mağdur) özniteliğine ait;

- ✓ En yüksek doğruluk değerleri 0.83 ile DVM-sigmoid ve RO algoritmalarında alınırken, en düşük doğruluk değeri 0.69 ile DVM-polinom algoritmasından alınmıştır.
- ✓ Kesinlik değerlerine bakıldığında en yüksek 0.86 ile RO algoritmasında alınırken, en düşük 0.65 ile DVM-polinom algoritmasından alınmıştır.
- ✓ Duyarlılık değerlerine bakıldığında en yüksek 0.96 ile DVM-polinom algoritmasından alınırken, en düşük 0.82 ile IBK algoritmasından alınmıştır.
- ✓ F1 skoru değerlerine bakıldığında en yüksek 0.85 ile DVM-sigmoid ve RO algoritmalarından alınırken, en düşük 0.77 ile DVM-polinom algoritmasından alınmıştır.

Yalova ilinde meydana gelmiş bilişim suçlarına karışan kişilerin, bilişim suçu türlerinden banka veya kredi kartlarını kötüye kullanmak, bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık, bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, kişisel verileri hukuka aykırı olarak verme veya ele geçirmek ve nitelikli dolandırıcılık suçlarından hangisine müdahil oldukları durumuyla ilgili olarak Tablo 5.6, Tablo 5.7, Tablo 5.8 ve Tablo 5.9 incelendiğinde;

- ✓ En yüksek doğruluk değeri 0.85 ile RO algoritmasından alınırken, en düşük doğruluk değeri 0.81 ile IBK algoritmasından alınmıştır.
- ✓ En yüksek kesinlik değeri 0.90 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna ait RO algoritmasından alınırken, en düşük 0.71 ile nitelikli dolandırıcılık suçuna ait çok katmanlı YSA algoritmasından alınmıştır.

- ✓ En yüksek duyarlılık değeri 0.94 ile kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçuna ait çok katmanlı YSA algoritmasından alınırken, en düşük 0.54 ile nitelikli dolandırıcılık suçuna ait IBK algoritmasından alınmıştır.
- ✓ En yüksek F1 skoru değeri 0.90 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçuna ait RO algoritmasından alınırken, en düşük 0.62 ile nitelikli dolandırıcılık suçuna ait IBK algoritmasından alınmıştır.
- ✓ En yüksek ROC eğrisi performans (AUC) değeri 0.96 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme ve kişisel verileri hukuka aykırı olarak verme veya ele geçirmek suçlarına ait IBK, RO ve çok katmanlı YSA algoritmalarından alınırken, en düşük 0.52 ile nitelikli dolandırıcılık suçuna ait DVM algoritmasından alınmıştır.

Bu çalışmada bilişim suçu olaylarına karışan kişilerin müşteki (mağdur) mi şüpheli mi durumuyla ilgili yapılan performans değerlendirmesi sonucu müşteki (mağdur) özniteliğine ait en yüksek doğruluk oranı 0.83 ile DVM-sigmoid algoritmasından alınırken, bilişim suçu türlerine ait performans değerlendirmesi sonucu en yüksek doğruluk değeri 0.85 ile RO algoritmasından alınmıştır. RO algoritması içerisinde performans değerlendirmesi yapılan bilişim suçu türleriyle ilgili diğer performans değerlerine bakıldığında, en yüksek skor 0.90 ile bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçundan alınmıştır. Sınıflandırmalar arasındaki doğruluk oranı farklarının az olduğu görülmüştür.

Bu kapsamlı çalışma sayesinde, Yalova'da meydana gelen bilişim suçu olaylarının her yıl hızla artış gösterdiği gözlenmiştir. Olaylara müdahil olan kişilerin genel olarak evli, erkek, ortaöğretim mezunu ve genç yaşa sahip oldukları, meydana gelen bilişim suçu olaylarının ilçelere göre dağılımına bakıldığında olayların genelde Yalova ili Merkez ilçesinde meydana geldiği görülmüştür. Olaylara müdahil olan kişi profillerinin etkin bir şekilde tahminin yapılmasına olanak tanınmıştır.

Bu tahminler gelecekte meydana gelebilecek suçların çözümü ve önlenmesi aşamalarında belirlenecek stratejilerin geliştirilmesine katkı sağlayacaktır. Kullanılmış olan makine öğrenmesi modellerinin başarılı bir performans göstermeleri yeni modellerin geliştirilmesi sürecinde önemli katkılar sunacaktır.

Yapılan çalışmada oluşturulan veri sayısı ve tespiti yapılan özellik sayısının arttırılması uygulanan makine öğrenmesi modellerinin performans değerlerini arttıracağı anlaşılmıştır. Ayrıca kullanılan makine öğrenmesi model sayılarının arttırılması da önerilmektedir.

Sonuç olarak hızla gelişen teknolojilerle birlikte bilişim suçlarının çeşitliliği de artmaktadır. Bu durum elde edilen adli veri delillerini de arttırmakta adli mercilerin iş yükünü arttırmaktadır. Bu nedenle, gelişen teknolojiye paralel olarak gerekli hukuki altyapı oluşturulmalıdır. Bu nedenle, gelişen teknolojiye paralel olarak gerekli hukuki altyapı oluşturulmalıdır. Bilişim suçlarını iyi analiz edebilen bilinçli ve eğitimli bireylerin sayısı arttırılmalı, bu doğrultuda yapılacak eğitim, seminer ve bilimsel çalışmalar desteklenmelidir.

KAYNAKLAR

Akca, M. F. (25 Ağustos 2020). *Nedir bu destek vektör makineleri? (Makine Öğrenmesi Serisi-2).* https://medium.com/deep-learning-turkiye/nedir-bu-destek-vekt%C3%B6r-makineleri-makine-%C3%B6%C4%9Frenmesi-serisi-2-94e576e4223e

Akdağlı, E. (4 Mart 2021). *Makine öğrenmesinde random forest algoritması*. https://ece-akdagli.medium.com/makine-%C3%B6%C4%9Frenmesinde-random-forest-algoritmas%C4%B1-a79b044bbb31

Arslan, E. (29 Mayıs 2020). *Makine Öğrenmesi-KNN (K-Nearest Neighbors) Algoritması Nedir?*. https://arslanev.medium.com/makine-%C3%B6%C4%9Frenmesi-knn-k-nearest-neighbors-algoritmas%C4%B1-bdfb688d7c5f

Aylak L.B., Oral O., & Yazıcı K. (2020). *Yapay Zeka ve Makine Öğrenmesi Tekniklerinin Lojistik Sektöründe Kullanımı*. ECJSE , cilt. 8, hayır. 1, s. 74–93, 2021, doi: 10.31202/ecjse.776314.

Bilgi Teknolojileri ve İletişim Kurumu (11 Haziran 2019). *Bilişim Hukuku ve Bilişim Suçu*. https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu

Bilgi Teknolojileri ve İletişim Kurumu (11 Haziran 2019). *Türkiye'de Bilişim Hukuku*. https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku

Datamarket (2024). *Deepfake.* https://www.datamarket.com.tr/sozluk/deepfake/

Demirel, F.B. (2022). *Adli Bilişim Ses İncelemeleri İçin Yapay Zeka Tabanlı Cinsiyet Tespiti Modeli Geliştirilmesi.* [Yayımlanmış yüksek lisans tezi]. Fırat Üniversitesi.

Dilber, İ. (2022). *Adli Bilişim İnceleme Süreçlerinde Yapay Zeka Kullanımı.* [Yayımlanmış yüksek lisans tezi]. Gazi Üniversitesi.

Dogan, N., & DİJLE, H. (2011). *Türkiye'de Bilişim Suçlarına Eğitimli İnsanların Bakışı.* Bilişim Teknolojileri Dergisi, 4(2).

Ekin Hukuk Bürosu (2023). Siber *Suç Nedir, Bilişim Suçları ve Cezaları Nelerdir.* https://www.ekinlaw.com/siber-suc-nedir-bilisim-suclari-ve-cezalari-nelerdir/

Er Avukatlık ve Hukuk Bürosu (2022). *Bilişim Suçları ve Bilişim Hukuku*. https://er.av.tr/tr/bilisim-hukuku-ve-bilisim-suclari

Ermeydan, D. (2018). *Türk ceza kanunu'nda bilişim suçları.* (Master's thesis, Çağ Üniversitesi Sosyal Bilimler Enstitüsü).

Garg, R. (2018). *Types of classification algorithms.* Analytics India• https://www. analyticsindiamag. com/7-types-classification-algorithms/• Preuzeto, 24, 2019.

Görmez, B. (2021). *Adli Bişimde Makine Öğrenmesi:Makine Öğrenmesi Algoritmaları İle Terör Olaylarının Tahmin Edilmesi Çalışması.* [Yayımlanmış yüksek lisans tezi]. Ankara Üniversitesi.

Grandini, M., Bağlı, E. ve Visani, G. (2020). *Çok sınıflı sınıflandırmaya yönelik metrikler: genel bakış*. arXiv ön baskı arXiv:2008.05756 .

Işıkhan, E. (1 Ocak 2020). *Multi Layer Perceptron (MLP) Nedir?*. https://isikhanelif.medium.com/multi-layer-perceptron-mlp-nedir-4758285a7f15

Kaçan, İ. (2023). *Kablosuz ağlar üzerinden gerçekleştirilen siber tehditlerin makine öğrenmesi yöntemleri ile ağ adli bilişim analizinin gerçekleştirilmesi.* [Yayımlanmış yüksek lisans tezi]. Fırat Üniversitesi.

Kalemci, E. (2021). *Bilişim Suçu Nedir, Çeşitleri Nelerdir*. https://kalemci.av.tr/bilisim-sucu-nedir-cesitleri-nelerdir/

Kaynar, O., Görmez, Y., Yıldız, M., & Albayrak, A. (2016, September). *Makine öğrenmesi yöntemleri ile Duygu Analizi*. In International Artificial Intelligence and Data Processing Symposium (IDAP'16) (Vol. 17, No. 18, pp. 17-18).

Neighbor, K. N. (2021). *Algorithm for Machine Learning—Javatpoint*. URL: https://www. javatpoint. com/k-nearest-neighbor-algorithm-for-machinelearning (visitado 11-07-2022).

Orozco, A.L.S., Huaman, C.Q., Alvarez, D.P., and Villalba, L.J.G. (2020). *A machine learning forensics technique to detect post-processing in digital videos.* Future Generation Computer Systems, 111, 199–212.

Öztürk, M. (13 Nisan 2022). *Python ile sınıflandırma analizleri Rastgele orman algoritması.* https://miracozturk.com/python-ile-siniflandirma-analizleri-rastgele-orman-random-forest-algoritmasi/

Pandya, V. J. (2016, December). *Comparing handwritten character recognition by AdaBoostClassifier and KNeighborsClassifier.* In 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 271-274). IEEE.

Sreenu, G. and Durai, M.A.S. (2019). *Intelligent video surveillance: a review through deep learning techniques for crowd analysis*. J Big Data

Şener, Y. (17 Ocak 2021). *Destek vektör makineleri (Support vector machine/SVM) çalışma mantığı ve python uygulaması.* https://yigitsener.medium.com/destek-vekt%C3%B6r-makineleri-support-vector-machine-svm-%C3%A7al%C4%B1%C5%9Fma-mant%C4%B1%C4%9F%C4%B1-ve-python-uygulamas%C4%B1-992163ff3eec#:~:text=Destek%20vekt%C3%B6r%20makineleri%20(support%20vector%20machine%20%7C%20SVM)%20makine%20%C3%B6%C4%9Frenmesinin,Ancak%20genellikle%20s%C4%B1n%C4%B1fland%C4%B1rma%20i%C3%A7in%20kullan%C4%B1l%C4%B1r.

Tekkanat, E., Topaloğlu, M., & Yılmaz, O (2018) *Bilişim Suçları ve Psikolojik Etkileri Açısından Türkiye'de Telefon Dolandırıcılığının Etkin Analizi*. Ege Eğitim Teknolojileri Dergisi,2(2), 44-54

Teyit (20 Mart 2023). *Teyit Sözlük:Dezenformasyon Nedir.* https://teyit.org/teyitpedia/teyit-sozluk-dezenformasyon-nedir

Thakur, R. and Rohilla, R. (2020). *Recent advances in digital image manipulation detection techniques: A brief review.* Forensic Science International, 312, 110311.

Türk Ceza Kanunu (2004). *5237 Sayılı Türk Ceza Kanunu*. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

Yıldırım, U. (2023). *Bilişim Suçları ve Cezalar.* https://kadimhukuk.com.tr/makale/bilisim-suclari-cezalari/

Yılmaz, E. N., Gönen, S., & Ulus, H. İ. (2016). *Bilişim alanında işlenen suçlar üzerine bir inceleme*. Bilişim Teknolojileri Dergisi, 9(3), 229.

ÖZGEÇMİŞ

İlk ve orta öğrenimini Samsun'da tamamladı. 2008 yılında girdiği Anadolu Üniversitesi Kamu Yönetimi Bölümünden 2012 yılında mezun oldu. 2014 yılından beri Jandarma Genel Komutanlığında Astsubay olarak çalışmaktadır.

TEZDEN TÜRETİLEN YAYIN VE ESERLER

Yurduseven, S. ve Harman G. (2024). Marmara Bölgesinde Bulunan Yalova İlinde Meydana Gelen Bilişim Suçlarının Makine Öğrenmesi Yöntemleriyle Analizi. *Bandırma Onyedi Eylül Üniversitesi, Uluslararası Bilimsel Araştırmalar ve Yenilikçi Çalışmalar Sempozyumu,* ISBN:978-625-94317-1-0

KATKILAR

Yapılan literatür araştırmaları sonucu yayımlanmış tez çalışmaları içerisinde Türkiye'de meydana gelmiş bilişim suçlarına ait gerçek veriler kullanılarak hiçbir çalışma yapılmadığı anlaşılmıştır. Bu tez çalışmasında analizi yapılan veri seti tamamen gerçek verilerden oluşmaktadır.