

FİNANSAL İŞLEMLERDE DOLANDIRICILIK TESPİTİ: PAYSIM VERİ SETİ ÜZERİNDE SINIFLANDIRMA VE ANOMALİ ANALİZİ

BİTİRME PROJESİ RAPORU

Makine Öğrenmesi ile İkili Sınıflandırma ve Anomali Tespiti

Derya Kalay

Ağustos, 2026

İÇİNDEKİLER

1. GİRİŞ	3
1.1. Projenin Amacı	3
1.2. Araştırma Soruları ve Hipotezler	3
1.3. Proje Kısıtları	3
2. MATERYAL VE YÖNTEM	4
2.1. Kullanılan Veri Seti	4
2.2. Geliştirme Ortamı ve Kütüphaneler	4
2.3. Hedef Değişken: isFraud	4
2.4. Başarım Ölçütlerinin Belirlenmesi	5
2.5. Yöntem Akışı	5
3. UYGULAMA	6
3.1. Veri Hazırlama	6
3.1.1. Veri Yükleme ve İlk Kontroller	6
3.1.2. Hedef Sızıntısının Önlenmesi	6
3.1.3. Modelleme İşlem Tiplerinin Seçilmesi	6
3.1.4. Türetilen Değişkenler	7
3.1.5. Eğitim / Validation / Test Ayrımı	7
3.2. Keşifsel Veri Analizi	8
3.2.1. Hedef Değişken Dağılımı	8
3.2.2. İşlem Tipi Kırılımı	8
3.2.3. İşlem Tutarı Kırılımı	9
3.2.4. isFlaggedFraud Alanının İncelenmesi	9
3.3. Modelleme	10
3.3.1. Özellik Seçimi ve Ön İşleme	10
3.3.2. Random Forest	11
3.3.3. Isolation Forest	12
3.3.4. Model Karşılaştırması ve Threshold Analizi	13
3.4. Hipotezlerin Değerlendirilmesi	14
4. SONUÇ	15
5. KAYNAKÇA	16

1. GİRİŞ

1.1. Projenin Amacı

Finansal dolandırıcılık, dijital ödeme ve para transferi sistemlerinde hem doğrudan finansal kayıp hem de müşteri güveni açısından önemli bir risk alanıdır. İşlem hacminin yüksek, fraud işlemlerinin ise toplam hacim içindeki payının çok düşük olması; klasik doğruluk ölçütlerinin yanıltıcı olmasına ve model değerlendirmesinde azınlık sınıfına odaklanılmasına neden olmaktadır.

Bu çalışmanın amacı, PaySim finansal işlem veri setini kullanarak bir işlemin fraud olup olmadığını işlem gerçekleşmeden önce veya işlem anında bilinebilecek bilgilerden tahmin etmektir. Final modele işlem sonrasında oluşan bakiye alanları bilinçli olarak verilmemiş; böylece gerçek zamanlı fraud tespiti senaryosuna daha yakın bir deney tasarımı kurulmuştur.

Çalışmada iki farklı yaklaşım karşılaştırılmıştır. Random Forest, geçmiş fraud etiketlerinden öğrenen gözetimli bir sınıflandırma modeli olarak; Isolation Forest ise fraud etiketini eğitim sırasında kullanmadan olağan dışı işlemleri arayan denetimsiz bir anomali tespit modeli olarak ele alınmıştır.

1.2. Araştırma Soruları ve Hipotezler

Çalışma kapsamında aşağıdaki sorulara yanıt aranmıştır:

- İşlem öncesinde bilinen tutar, işlem tipi ve bakiye bilgileri fraud ile normal işlemleri ayırmak için yeterli sinyal taşımakta mıdır?
- Fraud işlemleri tüm işlem tiplerine eşit biçimde mi dağılmaktadır, yoksa belirli işlem tiplerinde mi yoğunlaşmaktadır?
- Etiketli fraud örneklerinden öğrenen bir sınıflandırma modeli, etiketsiz anomali tespit yaklaşımına göre daha güçlü sonuç üretmekte midir?
- Karar eşiğinin (threshold) değiştirilmesi yanlış alarm ve kaçırılan fraud sayıları üzerinde nasıl bir ödünleşim oluşturmaktadır?

H0: İşlem öncesi / işlem anı değişkenleri fraud ve normal işlemleri pratik kullanım için yeterli düzeyde ayıramaz.

H1: İşlem öncesi / işlem anı değişkenleri fraud ve normal işlemleri ayıran güçlü bir tahmin sinyali içerir.

Alt hipotezler: (H2) Fraud belirli işlem tiplerinde yoğunlaşır. (H3) Random Forest, aynı işlem-öncesi özellikleri kullanan Isolation Forest'tan daha yüksek fraud tespit başarımları gösterir. (H4) Threshold değişimi Precision–Recall dengesini ve operasyonel hata türlerini belirgin biçimde değiştirir.

1.3. Proje Kısıtları

Sentetik veri. PaySim gerçek banka veya ödeme kuruluşu müşteri verisi değil, mobil para işlemlerini taklit eden sentetik bir veri setidir. Bu nedenle elde edilen performans değerleri gerçek üretim ortamına doğrudan genellenmemelidir.

Sınıf dengesizliği. Fraud işlemler toplam verinin yalnızca yaklaşık %0,13'ünü oluşturmaktadır. Bu yapı, Accuracy ölçütünün tek başına kullanılmasını uygun olmaktan çıkarmıştır.

Hesaplama maliyeti. Keşifsel analiz 6,36 milyon satırın tamamında yapılmış; model eğitiminde fraud oranını koruyan 500.000 satırlık örneklem kullanılmıştır.

2. MATERYAL VE YÖNTEM

2.1. Kullanılan Veri Seti

Çalışmada tek veri kaynağı olarak PaySim kullanılmıştır. Veri seti mobil para işlemlerini sentetik olarak üretmekte; işlem tipi, işlem tutarı, gönderici ve alıcının işlem öncesi/sonrası bakiyeleri ile fraud etiketlerini içermektedir.

Veri Kaynağı	İçerik	Kullanım Amacı
PaySim	6.362.620 finansal işlem; işlem tipi, tutar, bakiye alanları ve fraud etiketi	Ana veri seti; EDA, fraud sınıflandırması ve anomali analizi

Tablo 2.1.1. Çalışmada kullanılan veri kaynağı

PaySim’de hedef değişken isFraud olup 0 normal, 1 fraud işlemi ifade etmektedir. Veri setindeki isFlaggedFraud alanı ise mevcut bir kural motorunun çıktısıdır; doğrudan hedefi temsil etmediği hâlde fraud kararını önceden işaretleyen bir sistem çıktısı olduğundan final model girdisi olarak kullanılmamıştır.

2.2. Geliştirme Ortamı ve Kütüphaneler

Bileşen	Sürüm / Açıklama
Geliştirme ortamı	Jupyter Notebook / Google Colab uyumlu Python çalışma ortamı
Programlama dili	Python 3
Veri işleme	pandas, numpy
Görselleştirme	matplotlib
Makine öğrenmesi	scikit-learn
Modeller	RandomForestClassifier, IsolationForest

Tablo 2.2.1. Geliştirme ortamı ve kullanılan kütüphaneler

2.3. Hedef Değişken: isFraud

Hedef değişken isFraud ikili bir etikettir. Veri setindeki 6,362,620 işlemin 8,213 tanesi fraud, 6,354,407 tanesi normaldir. Fraud oranı yalnızca %0.1291 olduğundan hedef değişken ileri derecede dengesizdir.

isFraud	Anlam	Kayıt Sayısı	Oran
0	Normal işlem	6,354,407	%99.8709
1	Fraud işlem	8,213	%0.1291
Toplam	-	6,362,620	%100,0000

Tablo 2.3.1. Hedef değişkenin sınıf dağılımı

2.4. Başarım Ölçütlerinin Belirlenmesi

Sınıf dağılımının ileri derecede dengesiz olması nedeniyle doğruluk (Accuracy) tek başına yanıltıcıdır. Bir model tüm işlemleri normal olarak tahmin etse dahi yaklaşık %99,87 doğruluk elde edebilir; ancak hiçbir fraud işlemi yakalayamaz. Bu nedenle değerlendirme fraud sınıfına odaklanan ölçütlerle yapılmıştır.

Precision, modelin fraud olarak işaretlediği işlemlerin ne kadarının gerçekten fraud olduğunu; Recall ise gerçek fraud işlemlerinin ne kadarının yakalandığını gösterir. F1 skoru bu iki ölçüt arasındaki dengeyi tek değerde özetler. PR-AUC, azınlık sınıfının çok seyrek olduğu problemlerde Precision-Recall davranışını bütünsel olarak değerlendirdiği için özellikle önemlidir.

Ölçüt	Kullanım Gerekçesi
Precision	Yanlış alarm seviyesini ve fraud tahminlerinin doğruluğunu gösterir.
Recall	Gerçek fraud işlemlerinin ne kadarının yakalandığını gösterir.
F1	Precision ve Recall arasındaki dengeyi ölçer.
PR-AUC	Dengesiz fraud probleminde azınlık sınıfı performansını bütünsel değerlendirir.
Balanced Accuracy	Normal ve fraud sınıflarına daha dengeli ağırlık verir.
ROC-AUC	Modelin sınıfları genel olarak ayırma yeteneğini destekleyici biçimde gösterir.

Tablo 2.4.1. Model değerlendirmesinde kullanılan ölçütler

2.5. Yöntem Akışı

Çalışma, veri yüklemekten nihai model karşılaştırmasına kadar aşağıdaki aşamalarda yürütülmüştür.

Aşama	İçerik
1	PaySim verisinin yüklenmesi, veri tiplerinin düzenlenmesi ve genel kalite kontrolü
2	Keşifsel veri analizi: hedef dağılımı, işlem tipleri, tutar ve mevcut fraud flag alanının incelenmesi
3	Fraud görülen TRANSFER ve CASH_OUT işlemlerinin modelleme evreni olarak seçilmesi
4	İşlem-anı özelliklerinin türetilmesi ve hedef sızıntısı taşıyan alanların çıkarılması
5	Train / validation / test ayrımı ve ön işleme
6	Random Forest ve Isolation Forest modellerinin eğitilmesi
7	Validation setinde threshold seçimi; test setinde nihai değerlendirme
8	Model karşılaştırması, confusion matrix ve threshold duyarlılık analizi

Tablo 2.5.1. Çalışma akışı

Test seti threshold seçimi veya model ayarı için kullanılmamış; yalnızca nihai başarımın ölçülmesi amacıyla devreye alınmıştır. Böylece model seçim sürecinde test verisine ait bilginin eğitime sızması engellenmiştir.

3. UYGULAMA

3.1. Veri Hazırlama

3.1.1. Veri Yükleme ve İlk Kontroller

PaySim dosyasının tamamı veri çerçevesine alınmış ve analizde kullanılacak sütunların veri tipleri bellek kullanımını azaltacak biçimde düzenlenmiştir. Toplam 6,362,620 satırda eksik değer sayısı 0 olarak gözlenmiştir. Veri seti EDA aşamasında herhangi bir işlem tipi filtresi uygulanmadan incelenmiştir.

Sütun	Açıklama
step	Simülasyondaki zaman adımı; bir adım yaklaşık bir saati temsil eder.
type	İşlem tipi: PAYMENT, TRANSFER, CASH_OUT, CASH_IN, DEBIT.
amount	İşlem tutarı.
oldbalanceOrg	Göndericinin işlem öncesi bakiyesi.
newbalanceOrig	Göndericinin işlem sonrası bakiyesi.
oldbalanceDest	Alıcının işlem öncesi bakiyesi.
newbalanceDest	Alıcının işlem sonrası bakiyesi.
isFraud	Hedef değişken: 1 fraud, 0 normal.
isFlaggedFraud	Mevcut kural tabanlı fraud işareti.

Tablo 3.1.1.1. Analizde kullanılan temel PaySim sütunları

3.1.2. Hedef Sızıntısının Önlenmesi

Hedef sızıntısı (data leakage), modelin tahmin anında gerçekte erişemeyeceği bir bilgiyi eğitim sırasında kullanmasıdır. Bu durumda test performansı yapay biçimde yüksek görünür ve model üretim ortamında aynı başarıyı gösteremez.

newbalanceOrig ve newbalanceDest alanları işlem tamamlandıktan sonra oluşan bakiye bilgilerini içerdiğinden final model girdisi olarak kullanılmamıştır. isFlaggedFraud da mevcut bir fraud kuralının çıktısı olduğu için modelin kendi tespit yeteneğini ölçebilmek amacıyla dışarıda bırakılmıştır.

3.1.3. Modelleme İşlem Tiplerinin Seçilmesi

Keşifsel analiz sonucunda fraud işlemlerinin yalnızca TRANSFER ve CASH_OUT tiplerinde görüldüğü belirlenmiştir. Fraud bulunmayan PAYMENT, CASH_IN ve DEBIT işlemlerinin modele eklenmesi, işlem tipini çok kolay bir ayırım kuralına dönüştürebileceğinden final modelleme evreni TRANSFER + CASH_OUT ile sınırlandırılmıştır.

3.1.4. Türetilen Değişkenler

Ham PaySim alanlarından, yalnızca işlem anında bilinebilecek bilgiler kullanılarak yeni değişkenler türetilmiştir. Amaç, modele işlem davranışını açıklayabilecek oran ve durum bilgileri kazandırmaktır.

Değişken	Kaynak	Açıklama
hour	step	Adım bilgisinin 24 saatlik döngüye dönüştürülmesi.
amount_to_orig_balance	amount, oldbalanceOrg	İşlem tutarının göndericinin işlem öncesi bakiyesine oranı.
orig_insufficient_balance	amount, oldbalanceOrg	İşlem tutarı gönderici bakiyesinden büyükse 1.
dest_zero_balance	oldbalanceDest	Alıcının işlem öncesi bakiyesi sıfırsa 1.
type_TRANSFER	type	TRANSFER işlemi için ikili kodlama.

Tablo 3.1.4.1. Türetilen değişkenler

Bu özellik mühendisliği adımlarının hiçbirisi işlem sonrası bakiye bilgisini kullanmamaktadır. Böylece model, fraud kararını işlem gerçekleşmeden önce elde bulunan bilgiyle vermek zorundadır.

3.1.5. Eğitim / Validation / Test Ayrımı

TRANSFER ve CASH_OUT filtrelemesi sonrasında 2,770,409 işlem kalmıştır. Bu alt kümede 8,213 fraud kayıt bulunmakta ve fraud oranı %0.2965 olmaktadır. Hesaplama maliyetini makul tutmak amacıyla sınıf oranını koruyan 500,000 satırlık stratified örneklem oluşturulmuştur.

Küme	Satır Sayısı	Fraud Sayısı	Fraud Oranı
Eğitim	300,000	889	%0,2963
Validation	100,000	297	%0,2970
Test	100,000	296	%0,2960

Tablo 3.1.5.1. Eğitim, validation ve test kümesi boyutları

Bölme işleminde stratify kullanılarak fraud oranının her kümede korunması sağlanmıştır. random_state=42 ile sonuçların yeniden üretilebilir olması hedeflenmiştir. Threshold seçimi yalnızca validation kümesinde yapılmış; test kümesine nihai değerlendirmeye kadar bakılmamıştır.

3.2. Keşifsel Veri Analizi

3.2.1. Hedef Değişken Dağılımı

Fraud sınıfı toplam işlemlerin yalnızca %0.1291'ünü oluşturmaktadır. Bu oran yaklaşık her 774 işlemten yalnızca birinin fraud olduğu anlamına gelir. Dolayısıyla modelin genel doğruluğundan ziyade fraud sınıfını yakalama kapasitesi değerlendirilmelidir.

Sınıf	Kayıt Sayısı	Oran
Normal	6,354,407	%99.8709
Fraud	8,213	%0.1291

Tablo 3.2.1.1. Fraud / normal işlem dağılımı

3.2.2. İşlem Tipi Kırılımı

İşlem tipi kırılımı, fraud davranışının veri setinde belirli türlerde yoğunlaştığını açık biçimde göstermektedir.

İşlem Tipi	İşlem Sayısı	Fraud Sayısı	Fraud Oranı (%)
CASH_OUT	2,237,500	4,116	0,183955
TRANSFER	532,909	4,097	0,768799
CASH_IN	1,399,284	0	0,000000
PAYMENT	2,151,495	0	0,000000
DEBIT	41,432	0	0,000000

Tablo 3.2.2.1. İşlem tipine göre fraud dağılımı

Fraud işlemlerin tamamı TRANSFER ve CASH_OUT kategorilerinde yer almaktadır. TRANSFER işlemlerinde fraud oranı yaklaşık %0,7688, CASH_OUT işlemlerinde ise %0,1840'tır. Bu bulgu H2 hipotezini desteklemektedir.

PAYMENT, CASH_IN ve DEBIT türlerinde fraud bulunmaması, tüm işlem tiplerini modele vermenin problemi gereğinden fazla kolaylaştırabileceğini göstermektedir. Bu nedenle model, yalnızca fraud görülme ihtimali bulunan işlem tipleri üzerinde eğitilmiştir.

3.2.3. İşlem Tutarı Kırılımı

İşlem tutarı fraud ve normal gruplar arasında belirgin bir fark göstermektedir. Fraud işlemlerde hem ortalama hem de medyan işlem tutarı normal işlemlere göre daha yüksektir.

Sınıf	Kayıt	Ortalama Tutar	Medyan Tutar	Maksimum Tutar
Normal	6,354,407	178,197.00	74,684.72	92,445,520.00
Fraud	8,213	1,467,967.00	441,423.44	10,000,000.00

Tablo 3.2.3.1. Fraud durumuna göre işlem tutarı özeti

Normal işlemlerin medyan tutarı yaklaşık 74,7 bin iken fraud işlemlerin medyanı yaklaşık 441,4 bindir. Ortalama fraud tutarının yaklaşık 1,47 milyon olması, amount değişkeninin fraud ayırımında güçlü bir sinyal olabileceğini göstermektedir. Bununla birlikte yalnızca yüksek tutar kullanılarak fraud kararı vermek yeterli değildir; bakiye ve işlem tipi bilgileriyle birlikte değerlendirme yapılmıştır.

3.2.4. isFlaggedFraud Alanının İncelenmesi

PaySim içindeki isFlaggedFraud, veri setinin kendi kural tabanlı fraud işaretidir. Bu alanın gerçek isFraud etiketiyle çapraz tablosu aşağıdadır.

isFlaggedFraud	Normal	Fraud	Toplam
0	6,354,407	8.197	6,362,604
1	0	16	16
Toplam	6,354,407	8,213	6,362,620

Tablo 3.2.4.1. isFlaggedFraud ve isFraud çapraz tablosu

isFlaggedFraud tarafından işaretlenen 16 işlemin tamamı fraud olsa da toplam 8.213 fraud işlemin yalnızca çok küçük bir bölümü yakalanmıştır. Bu alan yüksek precision ancak çok düşük recall üreten basit bir kural çıktısı gibi davranmaktadır. Model girdisi olarak kullanılmamasının nedeni, geliştirilen modelin bu mevcut kuralı kopyalamasını engellemektir.

3.3. Modelleme

3.3.1. Özellik Seçimi ve Ön İşleme

Final modelde kullanılan özellikler işlem öncesi ve işlem anı bilgileriyle sınırlandırılmıştır. Kimlik niteliğindeki nameOrig ve nameDest gibi yüksek kardinaliteli alanlar modele alınmamıştır. İşlem sonrası bakiye alanları hedef sızıntısı riski nedeniyle dışarıda bırakılmıştır.

Özellik	Tür	Kullanım Gerekçesi
step	Sayısal	Zaman içindeki işlem davranışını temsil eder.
hour	Sayısal	Gün içindeki saat döngüsünü temsil eder.
type_TRANSFER	İkili	TRANSFER ve CASH_OUT ayrımını kodlar.
amount	Sayısal	İşlem tutarı.
oldbalanceOrg	Sayısal	Göndericinin işlem öncesi bakiyesi.
oldbalanceDest	Sayısal	Alıcının işlem öncesi bakiyesi.
amount_to_orig_balance	Sayısal	Tutarın gönderici bakiyesine göre büyüklüğü.
orig_insufficient_balance	İkili	Tutarın bakiye üzerinde olup olmadığını gösterir.
dest_zero_balance	İkili	Alıcının başlangıç bakiyesinin sıfır olup olmadığını gösterir.

Tablo 3.3.1.1. Final model özellikleri

Sayısal değişkenlere StandardScaler uygulanmıştır. Ön işleme istatistikleri yalnızca eğitim verisi üzerinde öğrenilmiş ve validation/test kümelerine aynı dönüşüm uygulanmıştır. Bu adım, test verisine ait bilginin ön işleme aşamasında eğitime sızmasını engellemektedir.

Random Forest ölçeklemeye zorunlu olarak ihtiyaç duymasa da aynı işlenmiş özellik uzayının Isolation Forest ile paylaşılması karşılaştırmayı sadeleştirmiştir. Isolation Forest yalnızca eğitim kümesindeki normal işlemler üzerinde fit edilerek normal davranış profilini öğrenmeye yönlendirilmiştir.

3.3.2. Random Forest

Random Forest, birbirinden farklı karar ağaçlarının tahminlerini birleştiren ağaç tabanlı bir topluluk yöntemidir. Doğrusal olmayan ilişkileri ve değişkenler arası etkileşimleri yakalayabilmesi, fraud davranışının yalnızca tek bir değişkenle açıklanamadığı bu problem için uygun bir yapı sunmaktadır.

Parametre	Değer	Gerekçe
n_estimators	60	Birden fazla ağacın oylamasıyla daha kararlı tahmin üretmek.
max_depth	16	Ağaç derinliğini sınırlayarak aşırı öğrenmeyi azaltmak.
min_samples_leaf	2	Tekil kayıtlar için aşırı özel kuralların oluşmasını sınırlamak.
class_weight	balanced_subsample	Azınlık fraud sınıfına eğitim sırasında daha fazla ağırlık vermek.
max_samples	0,20	Her ağaçta örneklem kullanarak hesaplama maliyetini ve korelasyonu azaltmak.
random_state	42	Sonuçların yeniden üretilebilirliğini sağlamak.

Tablo 3.3.2.1. Random Forest model parametreleri

Modelin olasılık çıktısı doğrudan 0,50 eşiğiyle kullanılmamış; validation kümesinde F1 skorunu en yüksek yapan threshold seçilmiştir. Seçilen eşik yaklaşık 0,4225'tir. Test kümesi bu seçim sırasında kullanılmamıştır.

Ölçüt	Test Sonucu
Accuracy	0.9993
Balanced Accuracy	0.9053
Precision	0.9486
Recall	0.8108
F1	0.8743
ROC-AUC	0.9973
PR-AUC	0.9101

Tablo 3.3.2.2. Random Forest test başarımı

Random Forest test kümesindeki 296 gerçek fraud işlemin 240 tanesini yakalamış, 56 tanesini kaçırmıştır. Normal işlemler içinde yalnızca 13 yanlış alarm üretmiştir. Precision değerinin 0,9486 olması, fraud olarak işaretlenen işlemlerin büyük bölümünün gerçekten fraud olduğunu göstermektedir.

3.3.3. Isolation Forest

Isolation Forest denetimsiz bir anomali tespit yöntemidir. Temel varsayımı, olağan dışı gözlemlerin rastgele bölmelerle normal gözlemlere kıyasla daha kısa yollarda izole edilebilmesidir. Model eğitim sırasında isFraud etiketini kullanmamıştır.

Normal davranış profilinin öğrenilmesini güçlendirmek amacıyla Isolation Forest yalnızca eğitim kümesindeki normal işlemler üzerinde fit edilmiştir. Validation ve test aşamalarında her işlem için anomali skoru hesaplanmış; yüksek skor daha anomalik işlem olarak yorumlanmıştır.

Parametre	Değer	Gerekçe
n_estimators	80	Birden fazla izolasyon ağacından kararlı anomali skoru üretmek.
max_samples	50.000	Hesaplama maliyetini azaltırken yeterli normal davranış örneği kullanmak.
contamination	auto	Modelin varsayılan karar sınırını eğitimde sabit bir fraud oranına bağlamamak.
random_state	42	Sonuçların yeniden üretilebilirliği.

Tablo 3.3.3.1. Isolation Forest model parametreleri

Ölçüt	Test Sonucu
Accuracy	0.9978
Balanced Accuracy	0.8052
Precision	0.6307
Recall	0.6115
F1	0.6209
ROC-AUC	0.9931
PR-AUC	0.6192

Tablo 3.3.3.2. Isolation Forest test başarımı

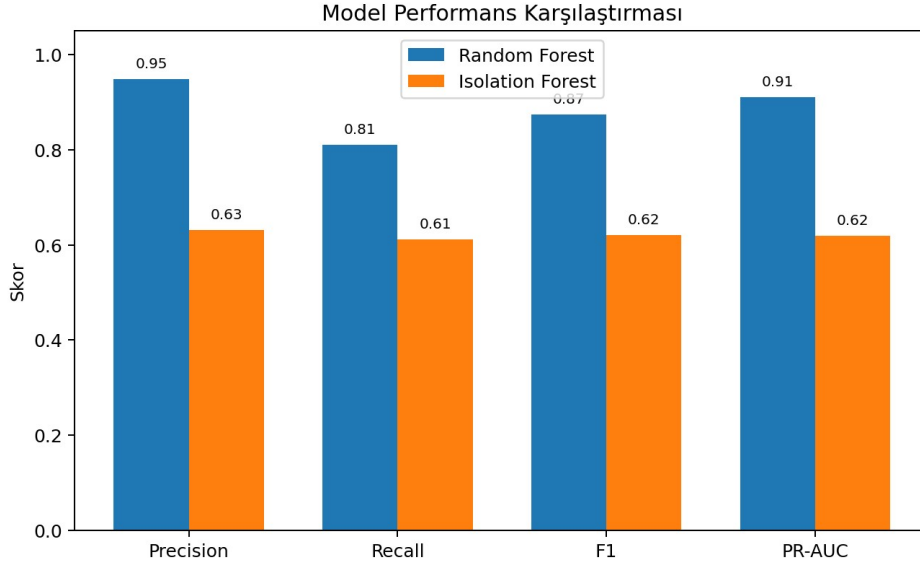
Isolation Forest 296 gerçek fraud işlemin 181 tanesini yakalamış, 115 tanesini kaçırmış ve 106 normal işlem için yanlış alarm üretmiştir. $F1=0,6209$ ve $PR-AUC=0,6192$ değerleri Random Forest'ın gerisindedir. Bununla birlikte modelin fraud etiketini görmeden bu performansa ulaşması, anomali skorunun tamamlayıcı risk sinyali olarak kullanılabileceğini göstermektedir.

Bu nedenle Isolation Forest'ın amacı ana sınıflandırma modelini geçmek değil, geçmişte etiketlenmemiş veya bilinen örüntülere tam olarak uymayan sıra dışı işlemleri ek bir kontrol katmanında işaretlemektir.

3.3.4. Model Karşılaştırması ve Threshold Analizi

Model	Precision	Recall	F1	ROC-AUC	PR-AUC
Random Forest	0.9486	0.8108	0.8743	0.9973	0.9101
Isolation Forest	0.6307	0.6115	0.6209	0.9931	0.6192

Tablo 3.3.4.1. Model karşılaştırma tablosu



Şekil 3.3.4.1. Random Forest ve Isolation Forest performans karşılaştırması

Random Forest tüm fraud odaklı ölçütlerde Isolation Forest'tan daha yüksek sonuç üretmiştir. F1 farkı yaklaşık 0,253, PR-AUC farkı ise yaklaşık 0,291 düzeyindedir. Bu bulgu, etiketli geçmiş fraud örneklerinin bulunduğu durumda gözetimli sınıflandırmanın ana karar modeli olarak daha uygun olduğunu göstermektedir.

Threshold	Precision	Recall	F1	FP	FN	TP
0.3000	0.8557	0.8615	0.8586	43	41	255
0.4000	0.9490	0.8176	0.8784	13	54	242
0.4225	0.9486	0.8108	0.8743	13	56	240
0.5000	0.9700	0.7635	0.8544	7	70	226
0.6000	0.9813	0.7095	0.8235	4	86	210

Tablo 3.3.4.2. Random Forest threshold duyarlılık analizi

Threshold 0,30'a düşürüldüğünde Recall 0,8615'e yükselmekte ve 255 fraud yakalanmaktadır; ancak yanlış alarm sayısı 43'e çıkmaktadır. Threshold 0,60'a yükseltildiğinde Precision 0,9813'e ulaşmakta ve yanlış alarm 4'e düşmekte; buna karşılık yalnızca 210 fraud yakalanmakta ve 86 fraud kaçırılmaktadır.

Bu sonuç, fraud sistemlerinde tek bir teknik "en iyi" eşik bulunmadığını göstermektedir. Eşik; fraud kaynaklı beklenen kayıp, manuel inceleme kapasitesi, yanlış blokaj maliyeti ve müşteri deneyimi birlikte değerlendirilerek belirlenmelidir.

3.4. Hipotezlerin Değerlendirilmesi

Proje kapsamında belirlenen hipotezler, ayrılmış test kümesindeki model performansı ve keşifsel analiz bulguları üzerinden değerlendirilmiştir. Çalışmada klasik istatistiksel anlamlılık testi veya p-değeri hesaplanmamış; “desteklendi” ifadesi model çıktılarının ilgili hipotezle uyumlu olduğunu belirtmek için kullanılmıştır.

Hipotez	Sonuç	Bulguyla İlişkisi
H1	Desteklendi	Random Forest işlem-sonrası bilgi olmadan $F1=0,8743$ ve $PR-AUC=0,9101$ elde etmiştir.
H2	Desteklendi	8.213 fraud işlemin tamamı TRANSFER veya CASH_OUT kategorilerinde gözlenmiştir.
H3	Desteklendi	Random Forest, Isolation Forest’tan $F1$ ve $PR-AUC$ açısından belirgin biçimde daha güçlüdür.
H4	Desteklendi	Threshold 0,30-0,60 aralığında değiştiğinde FP 43’ten 4’e düşerken FN 41’den 86’ya çıkmıştır.

Tablo 3.4.1. Hipotezlerin proje bulgularıyla değerlendirilmesi

Ana null hipotez H_0 , bu proje kapsamındaki test sonuçlarıyla desteklenmemektedir. Final Random Forest modeli, işlem sonrası bakiye alanlarını veya mevcut fraud flag’ini kullanmadan fraud ile normal işlemler arasında güçlü bir ayırım oluşturabilmiştir.

H2 bulgusu model tasarımını doğrudan etkilemiştir. Fraud’un yalnızca iki işlem tipinde görülmesi nedeniyle modelleme TRANSFER ve CASH_OUT ile sınırlandırılmış; aksi hâlde modelin fraud bulunmayan işlem tiplerini çok kolay bir “normal” kuralına dönüştürmesi riski azaltılmıştır.

H3, iki farklı öğrenme yaklaşımının amacının da farklı olduğunu göstermektedir. Random Forest bilinen fraud davranışlarını öğrenmek için daha başarılıdır; Isolation Forest ise etiketsiz sıra dışı davranışları aramak için tamamlayıcıdır.

H4 ise teknik model performansını doğrudan iş kararına bağlamaktadır. Daha düşük threshold daha fazla fraud yakalarken yanlış alarmı artırmakta; daha yüksek threshold müşteri/operasyon yükünü azaltırken daha fazla fraud kaçırmaktadır.

Bu sonuçların tamamı PaySim’in sentetik veri üretim mekanizması içinde geçerlidir. Gerçek ödeme sisteminde hipotezlerin yeniden sınanması; müşteri, cihaz, merchant, konum, oturum ve davranış değişkenleriyle modelin tekrar doğrulanması gereklidir.

4. SONUÇ

Bu çalışmada, yalnızca PaySim veri seti kullanılarak finansal dolandırıcılık tespiti için uçtan uca bir makine öğrenmesi süreci yürütülmüştür. 6.362.620 işlem üzerinde keşifsel veri analizi yapılmış; fraud davranışının işlem tipi ve tutar açısından nasıl farklılaştığı incelenmiştir. Fraud işlemlerin tamamının TRANSFER ve CASH_OUT tiplerinde görülmesi, modelleme evreninin bu iki işlem tipine odaklanmasını sağlamıştır.

Model tasarımında gerçek zamanlı kullanım koşulları dikkate alınmıştır. İşlem sonrasında oluşan newbalanceOrig ve newbalanceDest alanları ile mevcut kural çıktısı isFlaggedFraud final modele verilmemiştir. Bunun yerine step, işlem tipi, tutar, işlem öncesi bakiyeler ve bunlardan türetilen oran/durum değişkenleri kullanılmıştır.

Random Forest final testinde 0,9486 Precision, 0,8108 Recall, 0,8743 F1 ve 0,9101 PR-AUC elde etmiştir. Model 296 gerçek fraud işlemin 240'ını yakalarken yalnızca 13 normal işlem için yanlış alarm üretmiştir. Isolation Forest ise fraud etiketini eğitim sırasında kullanmadan 0,6209 F1 ve 0,6192 PR-AUC elde etmiş; ana sınıflandırma modelinden daha düşük performans göstermesine rağmen tamamlayıcı anomali sinyali üretme potansiyeli taşımıştır.

Threshold analizi, fraud tespitinin yalnızca model seçimiyle bitmediğini göstermiştir. Eşiğin düşürülmesi Recall'u artırıp daha fazla fraud yakalarken yanlış alarmı yükseltmekte; eşiğin artırılması ise Precision'u yükseltirken daha fazla fraudun kaçırılmasına yol açmaktadır. Bu nedenle üretim ortamında threshold seçimi teknik bir F1 optimizasyonunun ötesinde, maliyet tabanlı bir iş kararı olarak ele alınmalıdır.

Sınırlılıklar ve Gelecek Çalışmalar

PaySim sentetik bir veri setidir ve gerçek finansal sistemlerde bulunan müşteri kimliği, cihaz, merchant, IP, lokasyon, oturum ve davranış geçmişi gibi önemli risk sinyallerini içermez. Bu nedenle yüksek test performansı gerçek üretim başarısı olarak yorumlanmamalıdır.

Model eğitiminde 2,77 milyon TRANSFER + CASH_OUT işlemin tamamı yerine 500.000 satırlık stratified örneklem kullanılmıştır. Gelecek çalışmalarda tüm modelleme evreni üzerinde yeniden eğitim, maliyet duyarlı threshold optimizasyonu, zaman bazlı validasyon, concept drift izleme ve gradient boosting yöntemleriyle karşılaştırma yapılabilir.

Gerçek bir fraud sisteminde önerilen mimari; Random Forest benzeri gözetimli modelin ana risk skoru olarak, Isolation Forest benzeri anomali modelinin ise ek risk sinyali olarak kullanılmasıdır. Nihai karar, model skorlarının yanında fraud kaybı, manuel inceleme kapasitesi ve müşteri deneyimi maliyetleri dikkate alınarak verilmelidir.

5. KAYNAKÇA

- [1] López-Rojas, E. A., Elmir, A. ve Axelsson, S. (2016). PaySim: A Financial Mobile Money Simulator for Fraud Detection. 28th European Modeling and Simulation Symposium (EMSS).
- [2] Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5-32.
- [3] Liu, F. T., Ting, K. M. ve Zhou, Z.-H. (2008). Isolation Forest. 2008 Eighth IEEE International Conference on Data Mining, 413-422.
- [4] Pedregosa, F. ve diğerleri (2011). Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 12, 2825-2830.
- [5] McKinney, W. (2010). Data Structures for Statistical Computing in Python. Proceedings of the 9th Python in Science Conference, 51-56.
- [6] Harris, C. R. ve diğerleri (2020). Array Programming with NumPy. Nature, 585, 357-362.
- [7] Hunter, J. D. (2007). Matplotlib: A 2D Graphics Environment. Computing in Science & Engineering, 9(3), 90-95.