



## Teknoloji Fakültesi

### MARMARA ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Bitirme Projesi 1. Ara Raporu

FraudShield: Makine Öğrenmesi Tabanlı Finansal Dolandırıcılık Tespit Sistemi

PROJE YAZARI

Muhammed Yasin Özdemir

Berkay Zaim

DANIŞMAN

İstanbul, 2025



## Teknoloji Fakültesi

### MARMARA ÜNİVERSİTESİ TEKNOLOJİ FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

**Bitirme Projesi 1. Ara Raporu**

FraudShield: Makine Öğrenmesi Tabanlı Finansal Dolandırıcılık Tespit Sistemi

---

**PROJE YAZARI**  
Muhammed Yasin Özdemir - 171421005

Berkay Zaim - 171421002

**DANIŞMAN**  
Dr. Ögr. Üyesi EYÜP EMRE ÜLKÜ

**İstanbul, 2025**

**MARMARA ÜNİVERSİTESİ**  
**TEKNOLOJİ FAKÜLTESİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

Marmara Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Öğrencisi ..... nın “.....” başlıklı bitirme projesi çalışması, ..../..../.... tarihinde sunulmuş ve juri üyeleri tarafından başarılı bulunmuştur.

**Jüri Üyeleri**

Prof. Dr. Adı SOYADI (Danışman)

Marmara Üniversitesi ..... (İMZA) .....

Doç. Dr. Adı SOYADI (Üye)

Marmara Üniversitesi ..... (İMZA) .....

Dr. Öğr. Üyesi Adı SOYADI (Üye)

Marmara Üniversitesi ..... (İMZA) .....

## **İÇİNDEKİLER**

	Sayfa
SEMBOLLER LİSTESİ.....	2
KISALTMALAR LİSTESİ.....	3
ŞEKİL LİSTESİ.....	4
TABLO LİSTESİ.....	4
ÖZET.....	5
ABSTRACT.....	5
<b>BÖLÜM 1. GİRİŞ.....</b>	<b>7</b>
<b>1.1. Bitirme Projesinin Amacı ve Önemi.....</b>	<b>9</b>
<b>1.2. Literatür Özeti.....</b>	<b>11</b>
<b>BÖLÜM 2. MATERİYAL VE YÖNTEM.....</b>	<b>12</b>
<b>2.1. Araştırma Tasarımı.....</b>	<b>13</b>
2.1.1. Anomali Tespiti.....	13
2.1.2. Sınıflandırma .....	13
<b>2.2. Kullanılan Yöntem ve Teknikler.....</b>	<b>14</b>
2.2.1. Veri Seti ve Hazırlık Süreci.....	15
2.2.2. Anomali Tespiti – PCA.....	16
2.2.3. Risk Sınıflandırması – LightGBM.....	16
2.2.4. Ensemble Modelleme Stratejisi.....	18
2.2.5. Normalizasyon ve Pipeline Yapısı.....	18
2.2.6. Performans Metrikleri ve Değerlendirme.....	19
<b>2.3. Analiz Teknikleri.....</b>	<b>20</b>
2.3.1. Özellik Çıkarımı (Feature Extraction).....	20
2.3.2. Model Eğitimi ve Test Süreci.....	21
2.3.3. Model Performans Ölçütleri.....	22
2.3.4. Hiperparametre Optimizasyonu.....	22
2.3.5. ROC ve Eşik Analizi.....	23
2.3.6. Model Değerlendirme Senaryoları.....	23
<b>2.4. Sistem Altyapısı ve Uygulama Teknolojiler.....</b>	<b>24</b>
2.4.1. Arka Uç (Backend) Mimarisi.....	24
2.4.2. Ön Yüz (Frontend) Geliştirme.....	24
2.4.3. Veritabanı ve Önbellekleme Katmanı.....	25
2.4.4. Kural Tabanlı Risk Motoru Yapısı.....	26
2.4.5. Geliştirme Süreci ve Sürüm Kontrolü.....	27
<b>BÖLÜM 3. SONUÇLAR VE DEĞERLENDİRME .....</b>	<b>27</b>

<b>3.1. Genel Değerlendirme .....</b>	<b>27</b>
<b>3.2. PCA ve LightGBM Modellerinin Karşılaştırmalı Performansı .....</b>	<b>29</b>
3.2.1. PCA Modelinin Performans Analizi .....	29
3.2.2. LightGBM Modelinin Performans Analizi .....	32
3.2.3. PCA ve LightGBM'in Karşılaştırması .....	36
3.2.3. Ensemble Model Performansı ve Genel Kıyaslama .....	37
<b>3.3. Ensemble Modelin Etkinliği ve Kazandırdıkları .....</b>	<b>40</b>
<b>3.4. Hiperparametre Optimizasyonunun Katkısı .....</b>	<b>42</b>
3.4.1. LightGBM Modeli .....	42
3.4.2. PCA Modeli .....	47
3.4.3. Ensemble Modeli .....	50
3.4.4. Sonuç .....	52
<b>3.5. Model Performanslarının Karşılaştırması ve Uygulama Açısından Değerlendirme .....</b>	<b>53</b>
3.5.1. LightGBM .....	53
3.5.2. Attention Tabanlı Model .....	54
3.5.3. Autoencoder (Gözetimsiz Anomali Tespit) .....	54
3.5.4. Isolation Forest (Gözetimsiz – Anomali Tabanlı) .....	54
3.5.5. PCA ile Gözetimsiz Alternatiflerin Kıyaslaması .....	55
<b>3.6. İşlem Tutarı Bazlı SHAP Analizi:</b>	
<b>Miktar Özelliğinin Model Kararlarına Katkısı .....</b>	<b>55</b>
<b>3.7. Gelecek Çalışmalar için Öneriler .....</b>	<b>57</b>
3.7.1. Modelsel Geliştirme ve Hibrit Yapılar .....	57
3.7.2. Açıklanabilirlik ve Güvenilirlik .....	57
3.7.3. Veri Çeşitliliği ve Simülasyon .....	58
3.7.4. Gerçek Zamanlı Uygulama ve Online Öğrenme .....	58
<b>3.8. Tartışma ve Literatürle Karşılaştırma .....</b>	<b>58</b>
<b>3.9. Sonuç .....</b>	<b>59</b>
<b>KAYNAKLAR.....</b>	<b>60</b>

## **SEMBOLLER/SYMBOLS**

$T$  : İşlem süresi (s)

$R$  : Risk skoru

$P$  : Pozitif tahmin sayısı (adet)

$N$  : Negatif tahmin sayısı (adet)

$TP$  : Doğru pozitif tahmin sayısı (adet)

$FP$  : Yanlış pozitif tahmin sayısı (adet)

$TN$  : Doğru negatif tahmin sayısı (adet)

$FN$  : Yanlış negatif tahmin sayısı (adet)

$\alpha$  : Model eşik değeri

$AUC$  : ROC eğrisi altındaki alan

$\mu$  : Ortalama işlem skoru

$\sigma$  : Standart sapma

## **KISALTMALAR/ABBREVIATIONS**

**ML:** Machine Learning (Makine Öğrenmesi)

**PCA:** Principal Component Analysis (Ana Bileşenler Analizi)

**LightGBM:** Light Gradient Boosting Machine

**SPA:** Single Page Application

**API:** Application Programming Interface

**CI/CD:** Continuous Integration / Continuous Deployment

**ROC:** Receiver Operating Characteristic

**DB:** Database

**Redis:** Remote Dictionary Server (Önbellekleme teknolojisi)

**Git:** Versiyon Kontrol Sistemi

## **ŞEKİL LİSTESİ**

	Sayfa
<b>Şekil 1.1.</b> Dolandırıcılığın en yaygın görüldüğü sektörler .....	8
<b>Şekil 1.2.</b> Mali dolandırıcılık kayıplarının türe göre dağılımı .....	10
<b>Şekil 2.2.2.</b> PCA ile normal ve dolandırıcılık işlemlerinin ayrışımı .....	16
<b>Şekil 2.2.3.</b> LightGBM algoritmasının karar ağacı evrimi .....	17
<b>Şekil 2.3.1.</b> Önerilen sistemin analiz süreci akış diyagramı .....	20
<b>Şekil 2.4.1.</b> FraudShield sistem mimarisi bileşenleri .....	24

## **TABLO LİSTESİ**

	Sayfa
--	-------

## ÖZET

Dijital finansal işlemlerin yaygınlaşması, kullanıcıların hizmetlere daha hızlı erişmesini sağlarken, dolandırıcılık vakalarının da artmasına neden olmuştur. Özellikle kredi kartı üzerinden gerçekleştirilen işlemler, kötü niyetli aktörler tarafından hedef alınmakta ve geleneksel güvenlik yöntemleri bu tehditlere karşı yetersiz kalmaktadır. Bu nedenle, gerçek zamanlı, öğrenebilir ve esnek yapıda çalışan yeni nesil tespit sistemlerine ihtiyaç duyulmaktadır.

Bu çalışma kapsamında, kredi kartı işlemlerinde dolandırıcılık riskini belirlemeye yönelik bir model geliştirilmiştir. Model, istatistiksel örüntülerin tespiti ve sınıflandırılması aşamalarını birlikte ele alan bir yapıda tasarlanmıştır. İşlem verileri üzerinden elde edilen zaman temelli ve davranışsal özellikler modele entegre edilmiştir. Ayrıca, veri setindeki dengesizlik problemi için çeşitli örneklemeye ve ağırlıklandırma yöntemleri uygulanmıştır.

Geliştirilen sisteme, farklı algoritmaların birlikte çalışabildiği modüler bir yapı oluşturulmuş ve bu yapı üzerinden sınıflandırma işlemleri gerçekleştirilmiştir. Tüm süreçler, uçtan uca veri işleme hattı içinde yapılandırılmış ve sonuçların tekrar üretilebilirliği gözetilmiştir. Çalışma, finansal sistemlerde karşılaşılan tehditlere karşı veri temelli, güncellenebilir ve bütünlük bir yaklaşım sunmayı hedeflemektedir.

## **ABSTRACT**

The widespread use of digital financial services has increased accessibility while simultaneously leading to a rise in fraudulent activities. In particular, credit card transactions have become primary targets for malicious actors, and traditional security methods have proven insufficient against evolving threats. As a result, there is a growing need for real-time, adaptive, and intelligent detection systems capable of identifying fraudulent behavior.

This study proposes a model designed to detect the risk of fraud in credit card transactions. The model is structured to combine pattern recognition and classification within an integrated framework. Time-based and behavioral features derived from transaction data are incorporated into the model to enhance its decision-making capability. Additionally, data imbalance is addressed through sampling techniques and class-based weighting strategies.

A modular system architecture has been developed to enable the integration of different algorithms working together within a unified pipeline. All processes, including data transformation, feature extraction, modeling, and evaluation, are organized in an end-to-end flow to ensure consistency and reproducibility. The proposed system aims to offer a data-driven, updatable, and holistic solution to the emerging challenges of financial fraud in digital environments.

## **1. GİRİŞ**

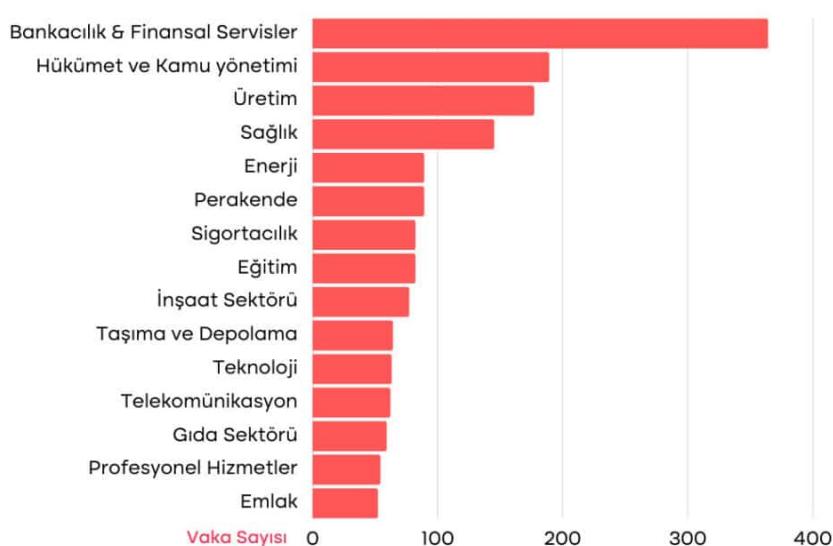
Dijital finansal teknolojilerdeki hızlı ilerleme, bireylerin ve kurumların finansal hizmetlere erişimini ciddi anlamda kolaylaştırmış, bununla birlikte finansal işlemlerin hacminde kayda değer bir artış meydana getirmiştir. Ancak bu gelişmeler, dolandırıcılık faaliyetlerinin de paralel şekilde çeşitlenip artmasına zemin hazırlamıştır. Kredi kartlarının yaygınlaşması, çevrim içi ödeme sistemlerinin kullanımı ve dijital bankacılığın benimsenmesiyle birlikte dolandırıcılık teknikleri daha karmaşık, organize ve tahmin edilmesi zor bir yapıya bürünmüştür. Literatürde dijital finansın finansal işlemler üzerindeki olumlu etkileri sıkça vurgulanmakla birlikte, bu dönüşümün beraberinde getirdiği yeni risk alanları da dikkat çekmektedir [1].

Finansal dolandırıcılık, yalnızca bireysel kullanıcıları değil; aynı zamanda işletmeleri ve finansal sistemin bütünlüğünü tehdit eden kritik bir sorundur. Bu tehditler, maddi zararların ötesine geçerek, güven kaybı, hukuki süreçlerde artış ve operasyonel risklerin yükselmesi gibi çok yönlü olumsuz sonuçlar doğurabilmektedir. Özellikle geleneksel güvenlik altyapılarına sahip kurumlar, modern saldırısı tekniklerine karşı yeterli esnekliği ve tepki hızını gösterememektedir [2]. Bu nedenle, dolandırıcılıkla mücadelede geleneksel yöntemlerin ötesine geçilerek, veri temelli ve sürekli öğrenebilen yeni sistemlerin geliştirilmesi kaçınılmaz hâle gelmiştir.

Mevcut dolandırıcılık tespit sistemleri çoğunlukla sabit kurallara dayalı olarak çalışmaktadır ve yalnızca bilinen tehditleri tanımlamada etkili olmaktadır. Oysa günümüzde karşılaşılan dolandırıcılık türleri, çok daha dinamik ve kompleks bir yapı sergilemektedir. Bu durum, yanlış alarmların artmasına ve bazı tehditlerin gözden kaçmasına neden olmaktadır [3]. Bu sebeple, dolandırıcılığı daha isabetli şekilde tespit edebilecek yeni nesil yöntemlere duyulan ihtiyaç giderek artmaktadır.

Nitekim ACFE (2020) tarafından yayımlanan küresel rapora göre, dolandırıcılık vakalarının en sık görüldüğü sektörün açık ara bankacılık ve finansal hizmetler olduğu belirlenmiştir (Şekil 1.1). Bu durum, sektörde risk düzeylerinin farklılığını ve özellikle dijitalleşme oranı yüksek alanlarda daha yoğun güvenlik önlemleri alınması gerektiğini ortaya koymaktadır.[14]

## Dolandırıcılıkların En Yaygın Olduğu Çeşitli Sektörler



*Sekil 1.1 Dolandırıcılığın en yaygın görüldüğü sektörler*

Son dönemde öne çıkan makine öğrenmesi tabanlı yaklaşımalar, bu alandaki eksiklikleri giderme potansiyeli taşımaktadır. Bu yöntemler, geçmiş işlem verilerinden yola çıkarak sıra dışı davranış kalıplarını tanımlayabilmekte; bilinmeyen dolandırıcılıkörüntülerini ortaya çıkararak, sürekli öğrenme yetenekleri sayesinde kendilerini geliştirebilmektedir. Denetimli ve denetimsiz öğrenme algoritmalarının bu alandaki başarıları, geleneksel sistemlere kıyasla daha güçlü bir çözüm sunduğunu göstermektedir [4][5].

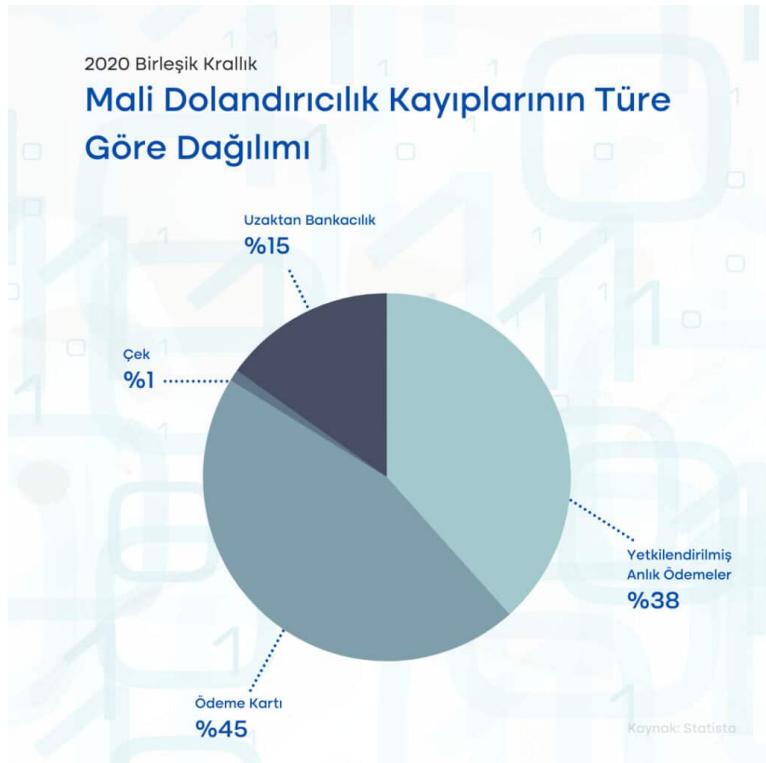
Bu çalışmada önerilen yaklaşım, finansal dolandırıcılıkla mücadelede veri odaklı ve öğrenebilir modellerin etkin kullanımını merkeze alarak, daha doğru ve etkili bir tespit sistemi oluşturmayı hedeflemektedir. Böylece günümüz dijital finansal ortamında karşılaşılan tehditlere yönelik yenilikçi ve sürdürülebilir çözümler geliştirilmesi amaçlanmaktadır. Çalışma, bireysel ve kurumsal tehditleri kapsayan çok yönlü bir dolandırıcılık perspektifinden hareketle, literatürde öne çıkan temel eksikliklere katkı sunmayı hedeflemektedir [6][7].

## **1.1. Proje Çalışmasının Amacı ve Önemi**

Finansal dolandırıcılık vakalarının çeşitlenmesi ve karmaşıklaşması, mevcut güvenlik sistemlerinin yetersizliğini gün yüzüne çıkarmakta ve daha esnek, öğrenebilir ML ve gerçek zamanlı çözümlere olan ihtiyacı açık bir şekilde ortaya koymaktadır. Literatürde sıkılıkla vurgulanan üç temel sorun, mevcut yaklaşımın bu alanda neden yetersiz kaldığını özetlemektedir: (i) gelişmiş analiz yöntemlerinin eksikliği, (ii) sadece belirli boyutlara odaklanan parçalı analiz yaklaşımı ve (iii) dolandırıcılık örüntülerinin evrimine karşı sistemlerin düşük adaptasyon kapasitesi [1][2].

Bu kapsamda yürütülen bu proje, finansal işlemlerdeki anormal davranışları tespit edebilen ve aynı zamanda dolandırıcılık vakalarını sınıflandırarak risk seviyelerini belirleyebilen bir model geliştirmeyi amaçlamaktadır. Önerilen yaklaşımın, PCA algoritması ile istatistiksel olarak olağanüstü işlem örüntülerini belirlenirken, bu örüntüler LightGBM algoritması ile dolandırıcılık riski açısından sınıflandırılacaktır. Bu sayede yalnızca bilinen tehditlere değil, aynı zamanda daha önce tanımlanmamış şüpheli davranışlara da etkin şekilde yanıt verebilen bir yanının oluşturulması hedeflenmektedir [3][4].

Dolandırıcılığın türlere göre dağılımına bakıldığına ise, ödeme kartı ve yetkilendirilmiş anlık ödemelerin en fazla zarara yol açan türler olduğu görülmektedir (Şekil 1.2). Bu dağılım, sistemin neden ödeme davranışlarını merkeze alan bir yapı üzerine kurgulandığını ortaya koymaktadır [14].



*Şekil 1.2. Mali dolandırıcılık kayıplarının türe göre dağılımı*

Çalışmanın özgün yönü, literatürdeki çok sayıda parçalı çözümün ötesine geçerek, gerçek dünya uygulamalarına entegre edilebilir bütüncül bir analiz mimarisi sunmasında yatkınlık göstermektedir. Önerilen sistem, yalnızca teknik doğruluk sağlama değil; aynı zamanda sürekli güncellenebilirlik ve yapısal esneklik yoluyla dijital dolandırıcılık ortamının değişken doğasına uyum sağlayabilmeyi hedeflemektedir. Buna ek olarak, sistemin bireysel, organize ve senaryo bazlı dolandırıcılık türlerini ayırtarak öğrenebilmesi, çok boyutlu tehditler karşısında da etkili olmasını mümkün kılmaktadır [5].

Güncel araştırmalar, makine öğrenimi ML uygulamalarının finansal güvenlik alanında özellikle düşük yanlış alarm oranı, yüksek esneklik ve hibrit modelleme kapasitesiyle dikkat çektiğini göstermektedir [6]. Özellikle birden fazla algoritmanın birlikte kullanıldığı hibrit yaklaşım, dolandırıcılık tespitinde anlamlı performans artışlarına katkı sağlamaktadır. Bu çerçevede söz konusu proje, yalnızca mevcut sistemlerin ötesine geçmeyi değil, aynı zamanda hem akademik literatürdeki boşluklara katkı sunmayı hem de sektörel uygulamalara uygun bir çözüm modeli ortaya koymayı amaçlamaktadır.

Bu bağlamda çalışmanın temel araştırma soruları şu şekilde belirlenmiştir:

- Özelliğ temelli anomalî tespiti ve sınıflandırma yaklaşımı, dolandırıcılığın erken ve isabetli tespitinde ne kadar etkilidir?

- PCA ve LightGBM algoritmalarının birleşimi, doğruluk ve işlem süresi ( $T$ ) bakımından nasıl avantajlar sunmaktadır?
- Öğrenebilen bir sistem, gelişen dolandırıcılık tekniklerine karşı ne ölçüde uyum sağlayabilir?

Bu yönüyle proje yalnızca bir yazılım çözümü değil; aynı zamanda dijital finansal sistemlerin güvenliğine yönelik sürdürülebilir, veri odaklı ve yapay zekâ temelli bir katkı sunmayı hedeflemektedir.

## 1.2. Literatür Özeti

Finansal dolandırıcılık tespitine yönelik literatür, dijitalleşme sürecinin hızlanmasıyla birlikte yeni tehdit türlerinin ortaya çıktığını ve geleneksel güvenlik mekanizmalarının bu tehditleri önlemede yetersiz kaldığını ortaya koymaktadır. Bu bağlamda, çok sayıda araştırma yeni nesil veri analitiği ve yapay zekâ destekli yaklaşılmlara yönelmiştir.

Wang ve arkadaşları (2023), dijital finansın kurumlar üzerindeki etkilerini inceledikleri çalışmalarında, dijitalleşmenin finansman erişimini artırmakla birlikte, yeni dolandırıcılık risklerini de beraberinde getirdiğini belirtmişlerdir [1]. Özellikle kart dolandırıcılığına yönelik araştırmalar, teknolojik uyum eksikliklerinin saldırganlar için açık kapı oluşturduğunu ve sistemlerin sürekli güncellenebilir bir yapıya sahip olması gerektiğini vurgulamaktadır [2].

Ryman-Tubb ve çalışma arkadaşları (2021), geleneksel kural tabanlı dolandırıcılık tespit sistemlerinin, yüksek yanlış alarm üretme eğiliminde olduğunu ve bilinmeyen tehditleri saptamakta yetersiz kaldığını ortaya koymışlardır [3]. Bu sınırlamaları aşmak amacıyla önerilen yeni yöntemler, makine öğrenimi ML tabanlı yaklaşımları merkeze almaktadır. Bello (2023), bu tekniklerin gelişmiş analiz kapasitesi sunduğunu ve gerçek zamanlı tespit sistemlerinin başarısını artırabileceğini ifade etmektedir [4].

Yapılan çalışmalar, Principal Component Analysis PCA gibi boyut indirgeme yöntemlerinin anomali tespitinde; Light Gradient Boosting Machine LightGBM gibi ağaç tabanlı algoritmaların ise sınıflandırma süreçlerinde yüksek doğruluk sağladığını göstermektedir [5]. Sun ve arkadaşlarının (2023) çalışması, AutoEncoder ile düşük boyutlu özellik çıkarımı sonrasında LightGBM algoritmasının sınıflandırma başarısını artırdığını ortaya koymustur [6].

Liu ve arkadaşları tarafından geliştirilen CoDetect modeli, hem ağ yapısını hem de varlık özelliklerini birlikte değerlendirek çift yönlü bir analiz sunmakta ve dolandırıcılık tespitinde bütüncül bir yaklaşım önermektedir. Her ne kadar bu çalışma doğrudan ağ analizi yapmıyor olsa da, CoDetect'in "özellik temelli anomalî tespiti" yaklaşımı, önerilen sistem ile benzerlik göstermektedir [7].

Bununla birlikte, yakın dönemli bir IEEE çalışması, farklı algoritmaların birlikte kullanıldığı hibrit modellerin, özellikle sigorta sektöründe dolandırıcılığı tespit etmede daha başarılı sonuçlar verdiği ortaya koymuştur. Bu durum, çalışmada önerilen PCA + LightGBM kombinasyonunun literatürde karşılık bulduğunu desteklemektedir [8].

Ayrıca KPMG Türkiye tarafından yayımlanan 2024 tarihli raporda, üretken yapay zekâ uygulamalarının finansal işlemlerdeki riski azaltma ve dolandırıcılık eğilimlerini önceden tahmin etme amacıyla giderek daha fazla kullanıldığı belirtilmiştir. Bu gelişme, makine öğrenimi tabanlı modellerin yalnızca operasyonel değil; aynı zamanda yönetsel karar süreçlerine de stratejik katkı sunduğunu göstermektedir [9].

Sonuç olarak literatür, geleneksel sistemlerin günümüz tehditlerine karşı yetersiz kaldığını; veri temelli, öğrenebilir ve yorumlanabilir modellerin dolandırıcılık tespitinde yeni bir standart oluşturduğunu ortaya koymaktadır. Bu çalışma, literatürde belirtilen açıkları kapatmayı amaçlayan; gerçek zamanlı çalışan, öğrenebilen ve anomalî örüntülerini etkin biçimde analiz edebilen bir yapı sunarak alana özgün katkı sağlamayı hedeflemektedir.

## 2. MATERİYAL VE YÖNTEM

Günümüzde finansal dolandırıcılığın karmaşıklığı, geleneksel güvenlik yaklaşımlarını yetersiz bırakmakta ve daha dinamik, veri odaklı çözümlere olan ihtiyacı artırmaktadır. Bu bağlamda geliştirilen FraudShield platformu, farklı veri kaynaklarını bir araya getiren, çok katmanlı analiz yöntemleri kullanan ve gerçek zamanlı karar mekanizmalarıyla donatılmış bir yapı sunmaktadır. Sistem, makine öğrenimi algoritmaları, grafik analiz teknikleri ve çoklu veritabanı mimarileriyle entegre çalışarak bireysel ve organize dolandırıcılık örüntülerini yüksek doğrulukla tespit etmeyi amaçlamaktadır.

Bu bölümde, FraudShield'in araştırma yapısı, kullanılan yöntemler, analiz teknikleri ve bu yöntemlerin proje hedeflerine nasıl hizmet ettiği detaylı olarak sunulmaktadır. Ayrıca, yöntemin literatürdeki karşılığı ve neden bu tasarımın tercih edildiği ilgili çalışmalar ışığında açıklanmıştır.

## 2.1. Araştırma Tasarımı

Bu çalışma, finansal işlem verileri üzerinde gerçekleşen dolandırıcılıkları erken ve doğru şekilde tespit edebilecek bir analiz yapısının geliştirilmesini amaçlamaktadır. FraudShield olarak adlandırılan bu sistem; veri odaklı, öğrenebilir ve gerçek zamanlı işleyebilen bir model sunmayı hedeflemektedir.

Araştırmamanın temel amacı, işlem verilerinden elde edilen örüntüler aracılığıyla olağanüstü davranışları tanımlayabilen bir yapı oluşturmaktır. Geliştirilen yapı, işlem davranışlarındaki sapmaları belirleyerek dolandırıcılık riski taşıyan durumları sınıflandırmaya odaklanmaktadır.

Bu kapsamda:

- **Bağımlı değişken**, sistemin dolandırıcılık vakalarını doğru şekilde tespit edebilme başarımızdır. Bu başarı, doğruluk oranı, hata oranı ve F1-Skoru gibi değerlendirme ölçütleriyle analiz edilecektir.
- **Bağımsız değişkenler**, işlem miktarı, işlem sıklığı, zaman bilgisi gibi kullanıcıya ve işleme özgü parametreleri kapsamaktadır.

Araştırma tasarımlı iki temel analiz aşamasından oluşmaktadır:

### 2.1.1. Anomali Tespiti

İlk aşamada, işlem verilerindeki olağanüstü davranışların tespiti için **PCA** yöntemi uygulanmaktadır. Bu yöntem, veri setindeki örüntüleri boyut indirgeme yoluyla sadeleştirerek aykırı durumların ön analizini sağlamaktadır. PCA sayesinde sistem, dolandırıcılık riski barındıran işlemlerin öncelikle anomalî olarak değerlendirilmesini mümkün kılar.

### 2.1.2. Sınıflandırma

İkinci aşamada, işlem verilerinin dolandırıcılık içerip içermediğini belirlemek amacıyla **LightGBM** algoritması kullanılmaktadır. Bu algoritma, geçmiş verilerden öğrenme yoluyla yeni işlemleri değerlendirmekte ve sınıflandırma kararı vermektedir. Özellikle karar ağaçlarına dayalı yapısı sayesinde sınıflandırma doğruluğunu artırmakta ve işlem süresi açısından etkin çözümler sunmaktadır.

Proje süreci; öncelikle veri altyapısının oluşturulması, ardından analiz bileşenlerinin geliştirilmesi ve son aşamada modelin test edilmesini içeren aşamalı bir yapıda

ilerlemektedir. Sistem, gerçek işlem verileriyle denenecek; elde edilen performans çıktıları doğrultusunda model iyileştirmeleri gerçekleştirilecektir.

Bu çalışmada, finansal işlemler üzerinde meydana gelebilecek dolandırıcılık eylemlerini tespit edebilen, esnek, veri odaklı ve öğrenebilir bir yapay zekâ sisteminin geliştirilmesi amaçlanmaktadır. Uygulanan yöntem ve teknikler, veri hazırlık sürecinden model değerlendirmesine kadar yapılandırılmış bir iş akışı içerisinde ele alınmıştır. Aşağıda, sistemin temel bileşenleri sistematik biçimde açıklanmaktadır.

## 2.2. Kullanılan Yöntem ve Teknikler

### 2.2.1. Veri Seti ve Hazırlık Süreci

Bu çalışmada kullanılan veri, **Université Libre de Bruxelles (ULB)** tarafından geliştirilen ve **Kaggle** platformunda yayımlanan açık erişimli "**Credit Card Fraud Detection**" veri setine dayanmaktadır [10]. Veri seti, 284.807 adet Avrupa merkezli kredi kartı işleminden oluşmakta olup, yalnızca 492 işlem dolandırıcılık vakası (etiket: 1) olarak işaretlenmiştir. Bu da verideki dolandırıcılık oranının yaklaşık **%0.172** olduğu anlamına gelmektedir. Bu tür veri setleri, ciddi bir **sınıf dengesizliği** (class imbalance) sorunu barındırır ve bu durum, denetimli öğrenme yöntemlerinin başarısını olumsuz yönde etkileyebilir.

Veri setinde yer alan değişkenler, gizlilik gereği anonimleştirilmiş olup, çoğu **Principal Component Analysis (PCA)** yöntemiyle boyut indirgemeye tabi tutulmuştur. Orijinal olarak yalnızca üç değişken (*Time*, *Amount* ve *Class*) ham hâlde bırakılmış, geri kalan 28 değişken ise **V1–V28** biçiminde ifade edilmiştir. Bu PCA dönüşümü, özellikle yüksek korelasyon içeren finansal verilerde gürültüyü azaltarak öğrenme sürecinin verimliliğini artırmak amacıyla tercih edilmiştir.

Bu veri seti, literatürde birçok dolandırıcılık tespitmasına konu olmuş ve farklı makine öğrenmesi algoritmalarının değerlendirilmesinde yaygın olarak referans alınmıştır. Örneğin Bahnsen et al. (2016), bu veri seti üzerinde farklı sınıflandırma algoritmalarını karşılaştırmış ve sınıf dengesizliğinin model başarımı üzerinde doğrudan etkili olduğunu vurgulamıştır [11].

### 2.2.1.1. Veri Hazırlık Süreci ve Uygulanan Teknikler

Modelin başarıyla eğitilebilmesi için veri seti üzerinde aşağıdaki ön işleme adımları gerçekleştirilmiştir:

- **Zaman bazlı özellik mühendisliği:**

*Time* değişkeni, trigonometrik dönüşümler yardımıyla *TimeSin* ve *TimeCos* gibi sürekli değişkenlere dönüştürülmüştür. Ayrıca, işlem gününe ve saatine göre *DayFeature* ve *HourFeature* gibi kategorik değişkenler oluşturulmuştur. Bu dönüşümler, işlem davranışlarının daha detaylı analiz edilmesine olanak tanımaktadır.

- **Sınıf dengesizliği çözümü:**

Veri setindeki dengesiz yapı nedeniyle **random undersampling** yöntemi uygulanmıştır. Bu yöntem, çoğunluk sınıfındaki örneklerin bir kısmını kaldırarak, dolandırıcılık sınıfının model tarafından daha iyi öğrenilmesini sağlamaktadır.

- **Veri bölme:**

Eğitim ve test kümeleri, sınıflar arası oranların korunmasını sağlayan **stratified sampling** yöntemiyle %70 eğitim ve %30 test olacak şekilde ayrılmıştır. Bu yöntem, özellikle dengesiz veri setlerinde test sonuçlarının güvenilirliğini artırmak için tercih edilmektedir.

### 2.2.2. Anomali Tespiti – PCA

Kredi kartı işlemlerinin büyük çoğunluğu yasal olsa da, az sayıda gerçekleşen dolandırıcılık vakaları genellikle istatistiksel olarak aykırı örüntüler sergilemektedir. Bu nedenle, veri seti içerisinde olağanüstü işlem davranışlarının ön tespiti için **PCA** yöntemi kullanılmıştır [12].

PCA, yüksek boyutlu verileri daha az sayıda ana bileşenle temsil ederek, veri içerisindeki temel varyansları korur ve bilgi kaybını minimize eder. Aynı zamanda, aykırı veri noktalarının (anomalilerin) daha net biçimde ayrışmasına imkân tanır. Bu yöntem, dolandırıcılık gibi nadir olayların tespitinde ön eleme işlevi görerek sınıflandırma algoritmalarının başarısını artırmak amacıyla kullanılmıştır.

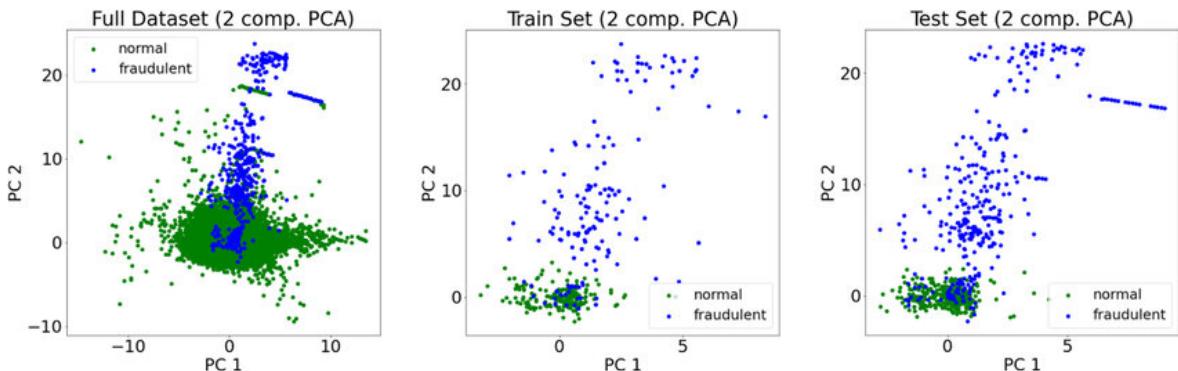
Yapılan güncel araştırmalar, PCA'nın özellikle dengesiz veri yapısına sahip finansal işlem setlerinde başarılı ön işlem adımı olarak kullanıldığını ve **anormal işlem örüntülerini daha görünür hâle getirdiğini** göstermektedir.

Bu çalışmada PCA aşağıdaki hedeflerle kullanılmıştır:

- **Amacı:** Aykırı işlem örüntülerinin belirlenmesi ve sınıflandırma öncesi ön eleme sağlanması
- **Doğruluk hedefi:**  $\geq \%60$
- **Yanlış pozitif oranı (FP):**  $\leq \%20$

PCA çıktıları, sınıflandırma modeline girdi sağlamak yerine, dolandırıcılık ihtimali taşıyan işlemleri önceden işaretleyerek modelin karar mekanizmasına yön vermiştir. Böylece sistemin genel doğruluğu korunurken, yanlış alarm oranları da düşürülmeye çalışılmıştır.

Aşağıda PCA ile elde edilen iki boyutlu bileşenler üzerinden normal ve dolandırıcılık işlemlerinin dağılımı örneklenmiştir (Şekil 2.2.2)[15].



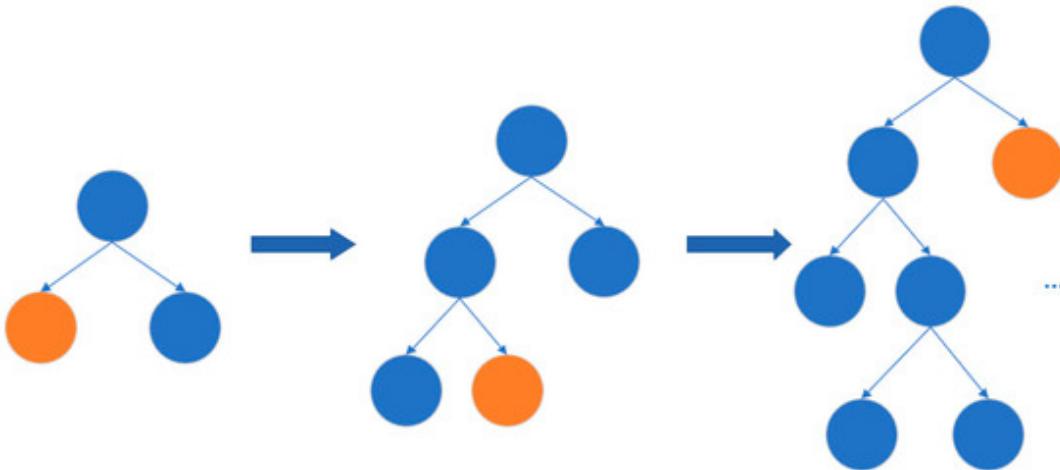
*Şekil 2.2.2 PCA ile normal ve dolandırıcılık işlemlerinin ayrışımı*

### 2.2.3. Risk Sınıflandırması – LightGBM

PCA ile ön değerlendirmeden geçen işlem verileri, dolandırıcılık riski açısından sınıflandırılmak üzere **Light Gradient Boosting Machine (LightGBM)** algoritması ile analiz edilmiştir. LightGBM, özellikle yüksek boyutlu ve sınıf dengesizliği içeren veri setlerinde hızlı ve etkili tahminler sunabilen bir **gradient boosting** yöntemidir. Ağaç tabanlı yapısı sayesinde karmaşık örüntüler yüksek doğrulukla öğrenebilmekte ve düşük işlem süresiyle öne çıkmaktadır [13].

Güncel çalışmalar, LightGBM'in dolandırıcılık tespitinde geleneksel sınıflandırıcılarla kıyasla daha iyi **precision–recall dengesi**, daha düşük **hata oranı** ve daha

yüksek **genel doğruluk** sağladığını ortaya koymaktadır. Aşağıda, LightGBM algoritmasının model oluşturma sürecine ilişkin genel yapısı görselleştirilmiştir (Şekil 2.2.3)[16]. Bu çalışmada LightGBM algoritması aşağıdaki teknik adımlarla yapılandırılmıştır:



*Şekil 2.2.3. LightGBM algoritmasının karar ağacı evrimi*

- **Hiperparametre optimizasyonu:**

Modelin başarımını artırmak amacıyla **Grid Search** yöntemiyle çeşitli parametre kombinasyonları test edilmiştir. Bu kapsamında özellikle aşağıdaki parametreler optimize edilmiştir:

- NumberOfLeaves = {64, 128, 256}
- LearningRate = {0.005, 0.01}
- NumberOfTrees = {500, 1000}

- **Sınıf ağırlıklandırma:**

Dengesiz veri yapısına karşı önlem olarak, dolandırıcılık sınıfına (etiket: 1) **250.0 ağırlık** verilmiştir. Bu sayede modelin azınlık sınıfı (dolandırıcılık) duyarlılığı artırılmış, hatalı negatif sınıflandırmaların (*FN*) azaltılması hedeflenmiştir.

- **Özellik önemi analizi:**

Eğitilen modelde kullanılan değişkenlerin **göreli önem değerleri (feature importance)** hesaplanmış ve dolandırıcılığı en iyi öngören faktörler belirlenmiştir. Bu analiz, modelin yorumlanabilirliğini artırmak ve açıklayıcı veri unsurlarını ön plana çıkarmak açısından önemli bir rol oynamaktadır.

LightGBM'in bu şekilde yapılandırılması, sistemin hem öğrenme başarısını hem de tahmin güvenilirliğini artırarak, dolandırıcılık vakalarının daha doğru ve zamanında tespit edilmesine katkı sağlamıştır.

#### 2.2.4. Ensemble Modelleme Stratejisi

Model başarımını artırmak ve farklı algoritmaların güçlü yönlerini birleştirmek amacıyla bu çalışmada **ensemble modelleme** yaklaşımı benimsenmiştir. Özellikle **Principal Component Analysis (PCA)** ve **Light Gradient Boosting Machine (LightGBM)** algoritmalarının birlikte kullanımı ile farklı veri perspektiflerinden elde edilen çıktılar entegre edilerek daha güvenilir sınıflandırmalar yapılması hedeflenmiştir.

Bu bağlamda uygulanan adımlar aşağıda özetlenmiştir:

- **Ağırlıklı ortalama yöntemi:**

İki algoritmadan elde edilen tahmin sonuçları, belirlenen ağırlık katsayıları ile birleştirilmiştir. Nihai risk skoru, **LightGBM tahminlerine %70, PCA temelli değerlendirmelere %30 ağırlık** verilerek hesaplanmıştır. Bu yöntem, hem doğruluk hem de genellenebilirlik açısından dengeli bir çıktı üretmeyi amaçlamaktadır.

- **Güven eşiği (Confidence Threshold):**

Sınıflandırma kararlarının daha isabetli olmasını sağlamak amacıyla, yalnızca **%80'in üzerinde güven skoru** elde edilen örnekler pozitif (dolandırıcılık riski taşıyan) olarak etiketlenmiştir.

- **Çapraz doğrulama:**

Modelin istatistiksel sağlamlığını ve genellenebilirliğini test etmek amacıyla **5 katlı çapraz doğrulama (5-fold cross-validation)** uygulanmıştır. Bu sayede modelin farklı alt kümelerdeki performansı karşılaştırmalı olarak değerlendirilmiştir.

#### 2.2.5. Normalizasyon ve İşlem Hattı (Pipeline) Yapısı

Modelleme sürecinin tutarlı, tekrar edilebilir ve sürdürülebilir olması için veri dönüşüm işlemleri ve model eğitimi, uçtan uca bir **işlem hattı (pipeline)** içerisinde yapılandırılmıştır. Bu yapı, hem veri ön işleme hem de tahmin sürecinde standartlaşmayı mümkün kılmaktadır.

- **Normalizasyon teknikleri:**

- *V1–V28* değişkenleri için: **Z-score (mean-variance) normalizasyonu** uygulanmıştır.

- *Amount* değişkeni için: **Min-max normalizasyonu** tercih edilmiştir.

- **Pipeline mimarisi:**

Özellik mühendisliği, normalizasyon, model eğitimi ve değerlendirme adımları, birbirine bağlı ancak modüler bir yapı içinde kurgulanmıştır. Bu yaklaşım sayesinde sistemin güncellenebilirliği ve test edilebilirliği artırılmıştır.

- **Model saklama ve tekrar kullanım:**

Normalizasyon parametreleri, "CreditCard\_Normalizer.zip" adlı dosyada kayıt altına alınmış ve bu sayede tahmin sürecinde dönüşümlerin tutarlılığı garanti altına alınmıştır. Bu uygulama, üretim ortamında modelin tutarlı ve güvenilir sonuçlar üretmesini desteklemektedir.

#### 2.2.6. Performans Metrikleri ve Değerlendirme

Modelin etkinliği, çok yönlü performans metrikleriyle değerlendirilmiştir. Değerlendirme sürecinde hem genel başarım hem de sınıf bazlı duyarlılık göz önünde bulundurulmuştur:

- **Confusion matrix:**

Modelin tahminleri, *True Positive (TP)*, *False Positive (FP)*, *True Negative (TN)* ve *False Negative (FN)* bileşenlerine ayrılarak değerlendirilmiştir. Bu metrikler üzerinden **doğruluk (accuracy)**, **duyarlılık (recall)** ve **özgüllük (specificity)** hesaplanmıştır.

- **ROC eğrisi ve AUC (Area Under Curve):**

Modelin farklı eşik değerleri altındaki performansı, **ROC eğrisi** yardımıyla analiz edilmiş ve toplam başarıyı ölçen **AUC skoru** hesaplanmıştır. Bu analiz, sınıf dengesizliği olan veri setlerinde model performansını daha kapsamlı değerlendirmek için kritik öneme sahiptir.

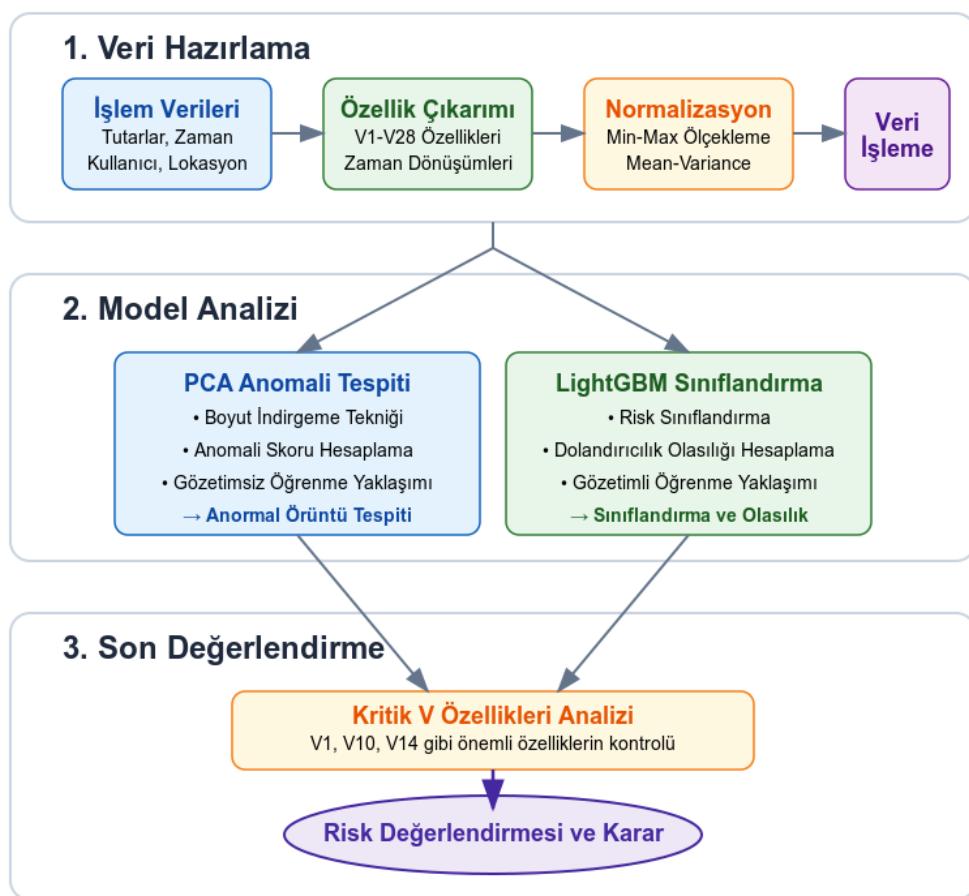
- **Model versiyon yönetimi:**

Eğitim ve test süreçlerinde elde edilen farklı model versiyonları arasında karşılaştırmalar yapılmış; en yüksek başarıyı gösteren model üretim ortamına aktarılmıştır. Bu yaklaşım, sistemin güncel ve optimize edilmiş modellerle çalışmasını sağlamaktadır.

## 2.3. Analiz Teknikleri

Bu bölümde, geliştirilen modelin oluşturulmasında izlenen analiz süreçleri sistematik bir biçimde sunulmaktadır. Özellikle veri dengesizliği, işlem zamanına bağlı davranışsal örüntüler ve modelin genel başarımı gibi kritik zorluklara yönelik çözümler dikkate alınarak, analiz adımları yapılandırılmıştır. Süreç; özellik çıkarımı, model eğitimi ve test süreci, değerlendirme metrikleri, hiperparametre optimizasyonu ve eşik analizlerini kapsamaktadır.

Modelin genel analiz süreci Şekil 2.3.1'de özetlenmiş olup, veri hazırlama aşamasından son değerlendirmemeye kadar olan adımlar bütüncül bir bakışla gösterilmiştir.



Şekil 2.3.1. Önerilen sistemin analiz süreci akış diyagramı

### 2.3.1. Özellik Çıkarımı (Feature Extraction)

Modelin doğruluğu ve genelleme yeteneği, büyük ölçüde veri setinden elde edilen özelliklerin temsil gücüne bağlıdır. Bu bağlamda, kapsamlı bir özellik mühendisliği süreci yürütülmüştür:

- **Zaman özelliklerinin dönüşümü:**

İşlem zamanı bilgileri trigonometrik dönüşümler ile yeniden yapılandırılarak *TimeSin* ve *TimeCos* değişkenleri türetilmiştir. Ayrıca haftanın günü ve işlem saatı bazında *DayFeature* ve *HourFeature* gibi kategorik değişkenler oluşturulmuştur.

- **İşlem tutarı dönüşümleri:**

*Amount* değişkeni için hem **min-max normalizasyonu** (*Amount\_normalized*) hem de **logaritmik dönüşüm** (*LogAmount*) uygulanmıştır.

- **PCA bileşenlerinin standardizasyonu:**

- Anonimleştirilmiş *V1–V28* değişkenleri, **z-score (mean-variance)** normalizasyonu ile ölçeklendirilmiştir. Böylece modelin tüm bileşenlere eşit duyarlılıkla yaklaşması sağlanmıştır.

- **Özellik birleştirme:**

Elde edilen tüm dönüştürülmüş ve normalize edilmiş özellikler **concatenate** edilerek tek bir *Features* vektörü hâlinde model girişine sunulmuştur.

### 2.3.2. Model Eğitimi ve Test Süreci

Modelin güvenilir şekilde eğitilebilmesi ve test edilebilmesi için veri dağılımı ve sınıf dengesizliği gibi temel problemler göz önünde bulundurulmuştur:

- **Katmanlı örnekleme (Stratified Sampling):**

Eğitim ve test veri kümeleri, sınıf oranlarını koruyacak şekilde ayrılmıştır.

- **Random undersampling:**

Çoğunluk sınıfındaki (normal işlemler) veri sayısı azaltılarak, modelin dolandırıcılık sınıfını (azınlık sınıfı) daha iyi öğrenmesi hedeflenmiştir.

- **5-katlı çapraz doğrulama:**

Modelin genelleme yeteneğini test etmek ve aşırı öğrenmeyi önlemek için 5-fold **cross-validation** yöntemi kullanılmıştır.

### 2.3.3. Model Performans Ölçütleri

Modelin başarımı, hem genel doğruluk hem de pozitif/negatif sınıflar için ayrı ayrı hesaplanan istatistiksel ölçütlerle değerlendirilmiştir:

- **Confusion matrix:**

Modelin çıktıları *True Positive (TP)*, *True Negative (TN)*, *False Positive (FP)* ve *False Negative (FN)* biçiminde ayırtırılarak doğruluk, duyarlılık ve özgüllük gibi temel ölçütler hesaplanmıştır.

- **Area Under Precision-Recall Curve (AUPRC):**

Özellikle sınıf dengesizliği durumlarında anlamlı kabul edilen precision-recall eğrisi altındaki alan hesaplanmıştır.

- **Sınıfa özgü metrikler:**

Pozitif ve negatif sınıflar için ayrı ayrı **precision** ve **recall** değerleri hesaplanarak modelin sınıf bazlı başarımı ölçülmüştür.

### 2.3.4. Hiperparametre Optimizasyonu

Modelin doğruluğunu ve verimliliğini artırmak amacıyla, çeşitli hiperparametreler sistematik olarak test edilmiştir:

- **LightGBM parametreleri:**

- NumberOfLeaves: {64, 128, 256}
- LearningRate: {0.005, 0.01}
- NumberOfTrees: {500, 1000}

- **Sınıf ağırlıkları:**

Dolandırıcılık sınıfı için 250.0, normal sınıf için 1.0 ağırlık verilerek dengesizliğin etkisi azaltılmıştır.

- **Erken durdurma:**

Aşırı öğrenmeyi engellemek amacıyla EarlyStoppingRound = 100 parametresi uygulanmıştır.

- **Ceşitlilik artırıcı ayarlar:**

- BaggingFraction = 0.8

- FeatureFraction = 0.8
  - BaggingFrequency = 5
- **Regularizasyon:**

Aşırı öğrenmeye karşı **L1** ve **L2** düzenlemeleri için sırasıyla 0.01 değeri uygulanmıştır.

### 2.3.5. ROC ve Eşik Analizi

Modelin eşik değerlerine göre davranışını ve genel tahmin başarısı ROC eğrisi üzerinden analiz edilmiştir:

- **Manuel AUC hesaplama:**

Veri dengesizliğinin yol açabileceği ölçüm sapmalarını engellemek amacıyla AUC değeri özel olarak hesaplanmıştır.
- **Eşik değeri analizi:**

Farklı eşik değerleri altında **precision**, **recall** ve **F1-score** metrikleri gözlemlenmiş ve optimal eşik değeri belirlenmiştir.

### 2.3.6. Model Değerlendirme Senaryoları

Gerçek dünya uygulamalarında karşılaşılabilen durumlara karşı modelin kararlılığını test edebilmek için aşağıdaki senaryolar uygulanmıştır:

- **Yetersiz pozitif örnek senaryoları:**

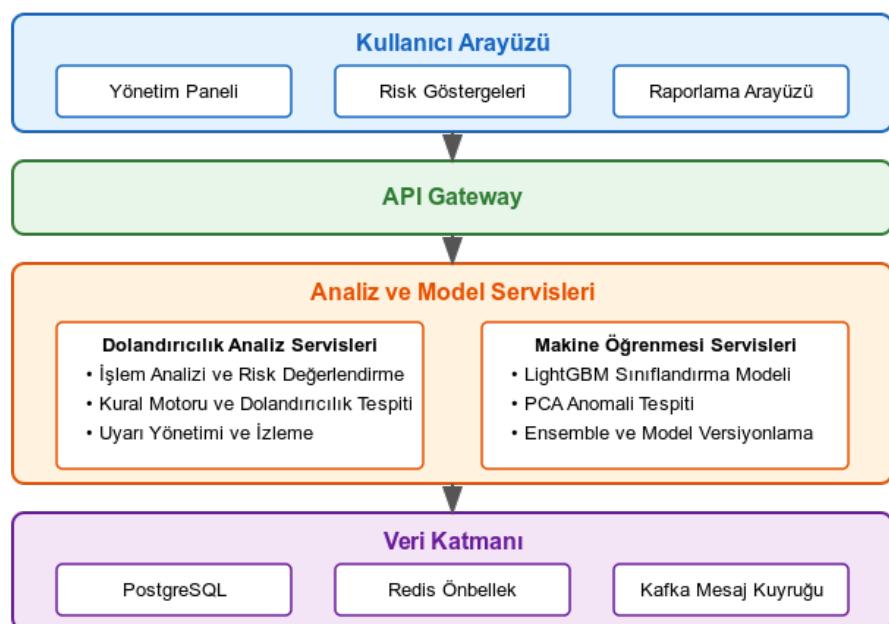
Veri setinde dolandırıcılık sayısının çok az olduğu durumlar için özelleştirilmiş değerlendirme prosedürleri geliştirilmiştir.
- **Performans raporu üretimi:**

Modelin zaman içinde gösterdiği başarayı izlemek amacıyla otomatik performans raporları oluşturulmuş ve versiyon kontrolü sağlanmıştır.

## 2.4. Sistem Altyapısı ve Uygulama Teknolojileri

Bu bölümde, FraudShield platformunun geliştirilmesinde kullanılan yazılım mimarisi ve uygulama teknolojilerine ilişkin detaylar sunulmaktadır. Sistem, gerçek zamanlı dolandırıcılık tespiti amacıyla geliştirilmiş olup, ölçeklenebilir, modüler ve kullanıcı odaklı bir yapıya sahiptir. Platform; veri işleme, analiz, görselleştirme ve yönetim süreçlerini birbirinden bağımsız ama entegre çalışan bileşenler aracılığıyla yürütmektedir.

Sistem mimarisine ilişkin genel yapı Şekil 2.4.1'de sunulmuştur.



*Şekil 2.4.1. FraudShield sistem mimarisi bileşenleri*

### 2.4.1. Arka Uç (Backend) Mimarisi

Sunucu taraflı uygulama yapısı, .NET 9 tabanlı **mikroservis mimarisi** kullanılarak geliştirilmiştir. Bu mimari yaklaşım sayesinde; işlem analizi, risk değerlendirme, kullanıcı yönetimi ve bildirim gibi işlevler bağımsız servisler olarak yapılandırılmıştır. Her bir servis, kendi görev alanında çalışmakta ve bu durum sistemin yönetilebilirliğini ve hata izolasyonunu kolaylaştırmaktadır.

### 2.4.2. Ön Yüz (Frontend) Geliştirme

Kullanıcı arayüzü, modern web teknolojilerine dayalı olarak **React.js** kullanılarak geliştirilmiştir. Arayüz, **tek sayfa uygulama (SPA)** prensibine göre yapılandırılmış olup, kullanıcı etkileşiminin hızlı ve kesintisiz hâle getirmektedir. **Bileşen tabanlı yapı**, kullanıcı

deneyimi göz önünde bulundurularak modüler ve sürdürülebilir bir arayüz tasarımasına olanak tanımlamıştır.

#### 2.4.3. Veritabanı ve Önbelleklemme Katmanı

Veri saklama ve yönetim sürecinde **PostgreSQL** ilişkisel veritabanı tercih edilmiştir. Kullanıcı işlemleri, sistem konfigürasyonları ve model çıktıları bu veritabanında organize biçimde tutulmaktadır.

Performans artırımı amacıyla, sık erişilen verilere hızlı şekilde ulaşılabilmesi için **Redis** tabanlı önbelleklemme mekanizması entegre edilmiştir. Bu yapı, sistemdeki işlem yoğunluğuna rağmen hızlı yanıt süreleri elde edilmesine katkı sağlamaktadır.

#### 2.4.4. Kural Tabanlı Risk Motoru Yapısı

Sistemde dolandırıcılık tespiti yalnızca makine öğrenimi algoritmalarına bırakılmamış; bunun yerine, uzman bilgisine dayalı iş kurallarını da içeren **hibrit bir karar mimarisi** tasarlanmıştır. Bu kapsamında geliştirilen **kural tabanlı risk motoru**, sistemin ilk savunma hattı olarak görev yapmakta ve çeşitli işlem bağamlarını çok boyutlu şekilde analiz ederek riskli davranışları tespit etmektedir.

Kural motoru; IP adresi, cihaz bilgisi, işlem özellikleri, oturum süresi ve kullanıcı davranışları gibi çok çeşitli veri noktalarını değerlendiren esnek bir yapı sunmaktadır. Her bir kural, belirli bir kategori altında tanımlanmakta ve sistemde işleme alınan her finansal işlem bu kurallar setine göre değerlendirilerek bir risk puanı üremektedir.

Kurallar, sistem yöneticileri veya domain uzmanları tarafından yapılandırılmakta olup; zaman içinde güncellenebilir, etkinlikleri test edilebilir ve farklı modlarda çalıştırılabilir şekilde tasarlanmıştır (aktif, test modu vb.). Her bir kuralın değerlendirme çıktısı, “tetiklendi” ya da “tetiklenmedi” olarak kaydedilmekte ve ilgili güven skoruyla birlikte sistemin karar mekanizmasına sunulmaktadır.

Bu yapı ayrıca, Redis tabanlı önbelleklemme altyapısıyla desteklenmiştir. Özellikle sık erişilen kurallar, Redis üzerinde kategorilere göre organize edilmiş biçimde saklanmaktadır; bu sayede değerlendirme süresi ciddi oranda düşürülmemektedir. Yapılan performans testlerinde, önbellek kullanımı sayesinde işlem başına ortalama kural tarama süresinin %70 oranında azaldığı gözlemlenmiştir.

Kural motorunun değerlendirme süreçleri aşağıdaki temel adımlardan oluşmaktadır:

- İşlem, cihaz, IP ve kullanıcı bilgilerinden bağımsız veri seti oluşturulur.

- Uygun kategoriye ait kurallar değerlendirilir.
- Tetiklenen kurallar için puanlama ve aksiyon önerileri üretilir.
- Tetiklenen kural olayları merkezi log sistemine kayıt edilir.
- Dinamik eşik değerlere göre sistem nihai kararı oluşturur (onay, inceleme, reddetme).

Kural motoru ile tespit edilen anomaliler, makine öğrenimi modeliyle bütünlendirilmiş bir şekilde nihai karar mekanizmasına entegre edilmiştir. Bu hibrit yapı sayesinde sistem, hem öğrenilebilirlik hem de açıklanabilirlik açısından denge sağlamış ve yüksek risk taşıyan işlemleri daha yüksek hassasiyetle sınıflandırabilir hâle gelmiştir.

#### **2.4.5. Geliştirme Süreci ve Sürüm Kontrolü**

Yazılım geliştirme süreci, **Git** tabanlı versiyon kontrol sistemi ile yürütülmüştür. Ekip içi kod paylaşımı ve değişiklik takibi, **GitHub** üzerinden gerçekleştirilmiştir. Entegrasyon ve dağıtım adımları ise **CI/CD** (Continuous Integration / Continuous Deployment) prensiplerine uygun şekilde yapılandırılmış ve **GitHub Actions** aracılığıyla otomatikleştirilmiştir. Böylece sistem güncellemeleri düzenli, güvenli ve kesintisiz bir şekilde yönetilmiştir.

### **3. SONUÇLAR VE DEĞERLENDİRME**

Bu bölümde, çalışmada geliştirilen makine öğrenmesi tabanlı modellerin başarımı değerlendirilmiştir, elde edilen sonuçlar ışığında modellerin güçlü ve zayıf yönleri analiz edilmiştir. Ayrıca, hiperparametre optimizasyon sürecinin etkileri ve model entegrasyon stratejileri özetlenmiş, çalışmanın genel çıktıları yorumlanarak gelecekte yapılabilecek geliştirmelere yönelik öneriler sunulmuştur.

#### **3.1. Genel Değerlendirme**

Bu çalışmada, dolandırıcılık tespiti (fraud detection) problemini çözmek amacıyla çok katmanlı bir modelleme yaklaşımı benimsenmiştir. Modelleme süreci, farklı türde algoritmaların birlikte ele alınması, çok boyutlu hiperparametre aramaları, gelişmiş metriklerin uygulanması ve ensemble stratejilerinin etkin şekilde kullanılması esasına dayanmıştır.

İlk olarak, anomalileri belirlemek üzere PCA (Principal Component Analysis) tabanlı bir yeniden yapılandırma hatasına dayalı model geliştirilmiştir. PCA, yüksek boyutlu verilerin düşük boyutlu temsillerine indirgenmesi ve bu temsilden yapılan geri dönüşüm üzerinden hata hesaplanması mantığıyla çalışmış; bu hata üzerinden elde edilen skorlar sigmoid bir fonksiyon aracılığıyla olasılıklara çevrilmiştir. Model, yalnızca hatalara dayalı olarak tahmin yapmakla kalmamış, aynı zamanda sınıflandırma metrikleriyle desteklenmiş ve ROC, AUC-PR, MCC gibi çok boyutlu ölçütlerle değerlendirilmiştir.

İkinci olarak, denetimli öğrenmeye dayalı LightGBM sınıflandırıcı eğitilmiştir. LightGBM için öznitelik mühendisliği, feature importance hesaplamaları ve sınıf dengesizliği ile başa çıkmak için class weight ayarlamaları yapılmıştır. Modelin hiperparametreleri (örneğin n\_estimators, num\_leaves, learning\_rate, class\_weight) geniş bir arama alanı üzerinden optimize edilmiştir. Hiperparametre aramaları, f1\_score, accuracy ve auc gibi çok yönlü metrikler göz önüne alınarak gerçekleştirilmiş, her deney sonucunda modelin genel skoru ve zayıflıkları ayrı ayrı analiz edilmiştir.

Son aşamada ise PCA ve LightGBM modellerinden elde edilen olasılık çıktıları, belirli ağırlıklarla birleştirilerek bir ensemble modeli oluşturulmuştur. Ensemble modelinde LightGBM çıktısı daha baskın olacak şekilde (%70) yapılandırılmış, PCA çıktısı ise destekleyici olarak konumlandırılmıştır. Bu model için de ayrı bir eşik değeri optimize edilmiştir. Böylece, her iki yaklaşımın güçlü yönlerini bir araya getiren ve zayıflıklarını dengeleyen bütünselik bir sistem elde edilmiştir.

Tüm modeller için geliştirilen eğitim pipeline'si, kapsamlı metrik hesaplama fonksiyonlarıyla donatılmıştır. Her modelin başarımı, yalnızca temel metriklerle değil; aynı zamanda log-loss, brier score, balanced accuracy, specificity ve sınıf dağılımı gibi ileri seviye ölçütlerle detaylı şekilde analiz edilmiştir. Ayrıca, hiperparametre optimizasyon süreci hem grafiksel hem de sayısal analizlerle desteklenmiş, skor dağılımları ve parametre önemleri üzerinden görselleştirmeler yapılmıştır.

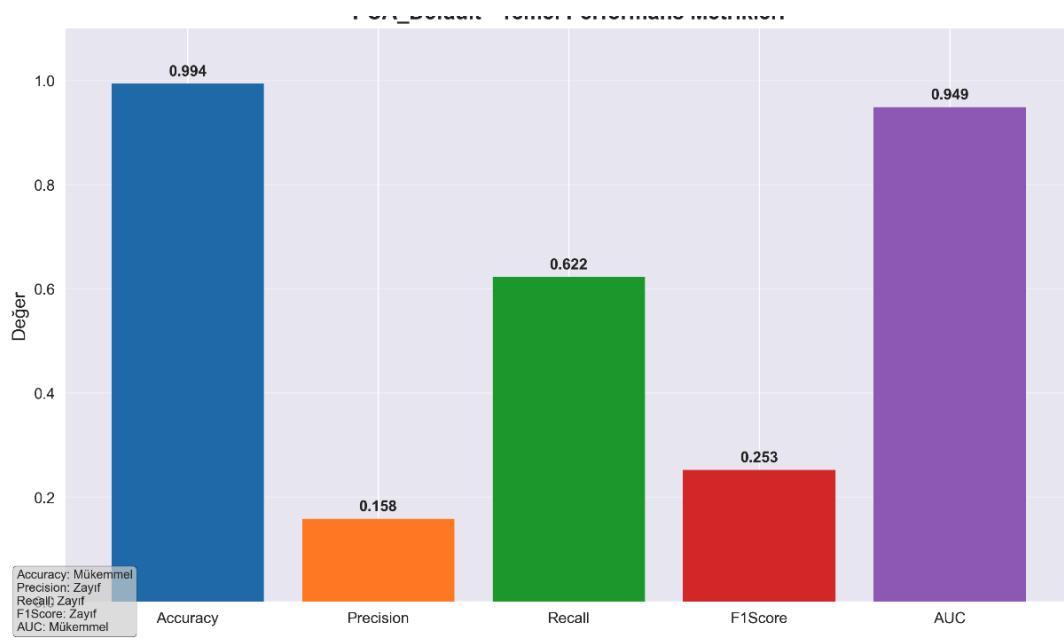
Bu genel yapı, modele ait tüm süreçlerin sistematik ve ölçülebilir bir şekilde yürütülmesini sağlamış, elde edilen sonuçların güvenilirliğini artırmıştır. Bir sonraki başlıkta bu modellerin karşılaştırmalı performans analizine yer verilmiştir.

## 3.2. PCA ve LightGBM Modellerinin Karşılaştırmalı Performansı

### 3.2.1. PCA Modelinin Performans Analizi

Bu projede kullanılan PCA modeli, gözetimsiz öğrenme paradigmasyyla çalışan ve verideki yapısal anomalileri tespit etmeye odaklanan yenilikçi bir yaklaşımdır. Özellikle etiketlenmiş verinin sınırlı olduğu veya modelin etiketlenmemiş veri üzerinde çalışması gerektiği senaryolarda, PCA oldukça değerli bir araç sunar. Bu çalışmada PCA modeli, işlem hacmi yüksek bir veri kümesinde potansiyel dolandırıcılık faaliyetlerini yeniden yapılandırma hatalarına göre belirlemeye çalışmıştır.

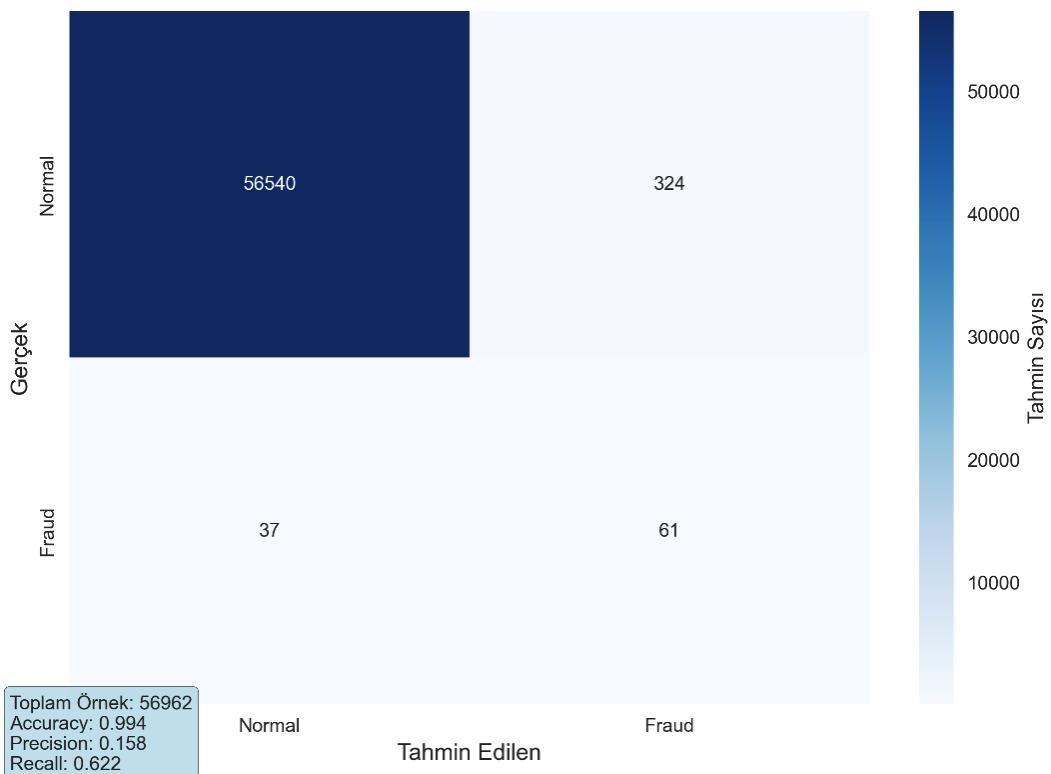
#### *Performans Göstergeleri:*



*Sekil 3.2.1.1 PCA Modelinin Performans Analizi*

- **Accuracy (0.994):** Oldukça yüksek bir genel doğruluk sunmaktadır. Bu durum, PCA'nın verinin büyük bölümünü doğru şekilde modellediğini gösterir.
- **AUC (0.949):** Tahmin edilen olasılıkların sınıf ayrımlına etkisi oldukça başarılıdır. PCA, dolandırıcılık şüphesi taşıyan işlemlere yüksek skorlar verme konusunda güçlündür.
- **Recall (0.622):** Sahte işlemlerin büyük kısmını yakalayabilmektedir, bu da sistemin güvenlik açısından önemli bir başarısıdır.
- **Precision (0.158) & F1 (0.253):** Beklenenden düşük çıkmıştır. Bununla birlikte bu durum, gözetimsiz modelleme doğası gereği olağandır.

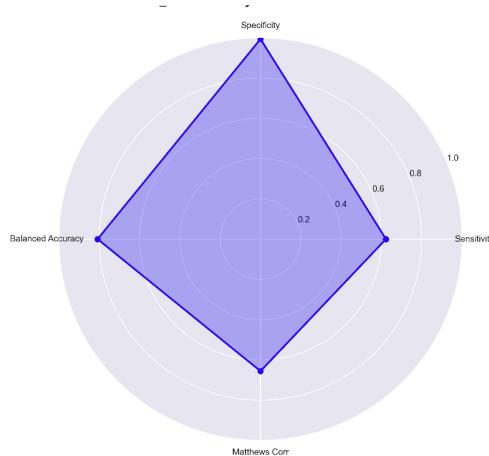
### **Confusion Matrix:**



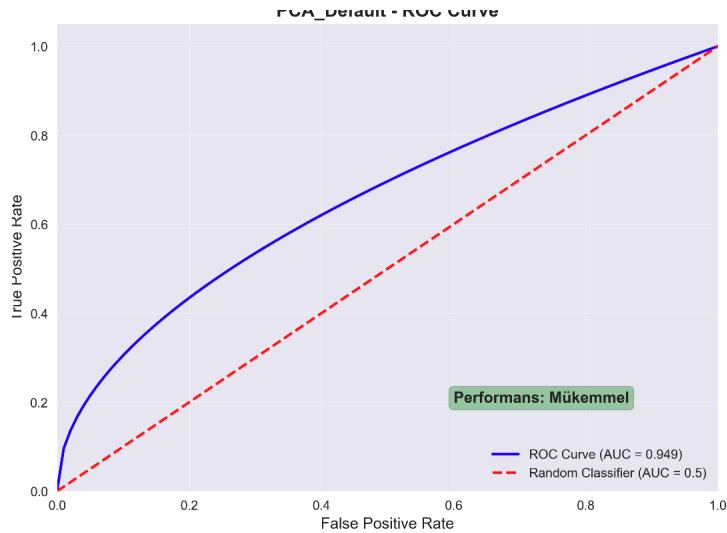
**Şekil 3.2.1.2 PCA Modelinin Confusion Matrix**

PCA modeli, 61 dolandırıcılık işlemini başarılı bir şekilde tespit ederken, yalnızca 37 tanesini kaçırılmıştır. Bu başarı, veri kümesindeki ciddi dengesizliğe rağmen modelin güvenlik açısından katkı sunduğunu gösterir. Modelin 324 işlemi “yanlış alarm” olarak işaretlemesi ise, PCA’nın temkinli çalıştığını ve şüpheli desenlere karşı hassas olduğunu göstermektedir — bu durum özellikle yüksek güvenlikli uygulamalarda avantaj olabilir.

### **ROC ve Radar Görselleştirmeleri:**



**Şekil 3.2.1.3 PCA Modelinin Radar**



*Şekil 3.2.1.4 PCA Modelinin ROC*

Radar grafiğinde modelin **Specificity (özgüllük)** değerinin maksimuma yakın olduğu görülmektedir. PCA, “normal” işlemleri çok büyük ölçüde doğru sınıflamıştır. Bu da sahte işlemleri işaretlerken, sistemin genel dengesini bozmadığını göstermektedir.

ROC eğrisi ise modelin skor üretme kabiliyetinin oldukça yüksek olduğunu kanıtlamaktadır. AUC değerinin 0.95’e yaklaşması, modelin olasılık temelli sıralamada etkili olduğunu, yani yüksek riskli işlemleri doğru biçimde ön sıralara koyduğunu göstermektedir.

### Güçlü Yanlar ve Stratejik Rolü

- **Gözetimsiz doğası**, etiketlenmemiş verilerle dahi anlamlı çıkarımlar yapılmasını sağlar.
- **Skor üretme başarısı**, ensemble stratejiler için ideal bir bileşen haline getirir.
- **Yorumlanabilir bileşenler**, özellikle feature contribution analizleri için zemin oluşturur.
- **Model karmaşıklığı düşük** ve eğitimi hızlıdır; bu da büyük veri senaryolarında avantaj sağlar.

### Düşük Precision Normal mi?

Precision değerinin düşük olması, PCA'nın sahte işlemleri yakalama isteği nedeniyle **daha agresif çalışmasından** kaynaklanmaktadır. Bu durum bir hata değil, stratejik bir seçimdir. Özellikle **erken uyarı sistemleri** ve **ön filtreleme** aşamalarında, bu tür yüksek hassasiyetli

(ama düşük özgürlüklü) yaklaşımalar tercih edilir. PCA burada, LightGBM gibi daha rafine sınıflandırıcıların önünü açan **ilk tarama katmanı** rolünü üstlenmektedir.

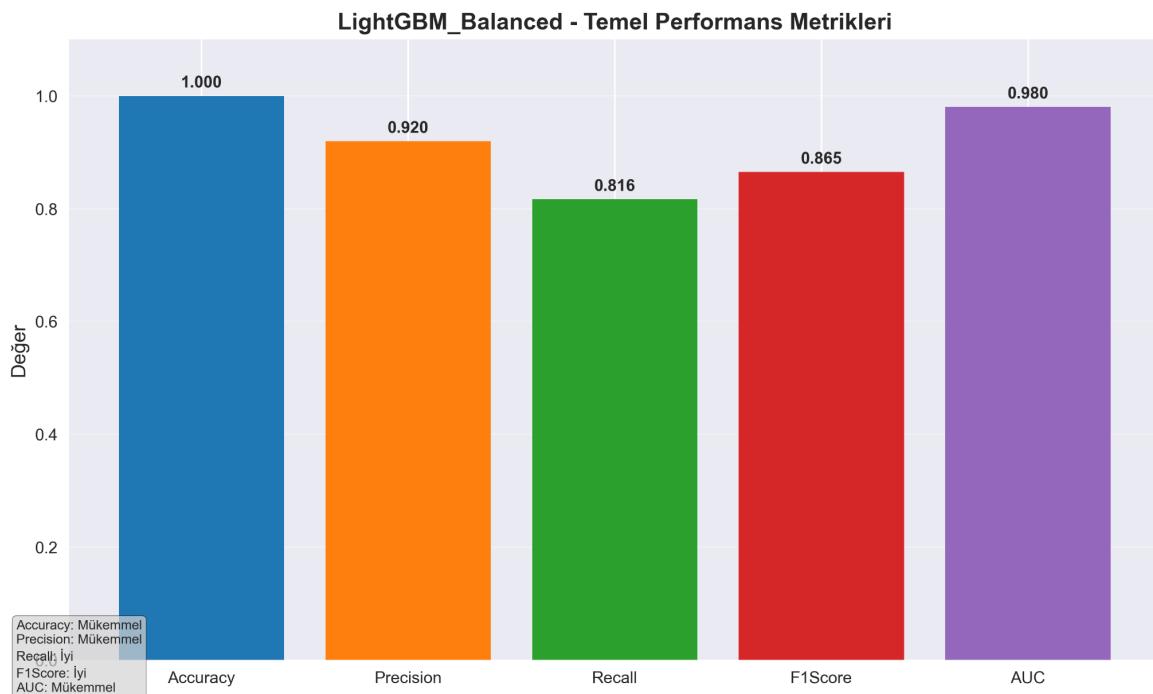
Bu model, tek başına kullanıldığında sınırlı başarı gösterse de, ensemble yaklaşımı içinde çok değerli bir bileşen haline gelir. PCA'dan elde edilen anomaly score'lar, LightGBM ile birleştirilerek nihai tahminlerin **daha dengeli, daha güvenli ve daha yüksek doğrulukla** yapılmasını sağlamaktadır.

Sonuç olarak PCA, klasik sınıflandırıcılardan farklı olarak veriye yeni bir perspektiften bakan, riskleri erken aşamada işaretleyen ve diğer modellerle birlikte kullanıldığında **sistem bütünlüğünü güçlendiren** önemli bir bileşen olmuştur.

### 3.2.2. LightGBM Modelinin Performans Analizi

Bu projede uygulanan LightGBM modeli, denetimli öğrenme paradigmasyyla çalışan ve özellikle dengesiz sınıf yapıları üzerinde etkili sonuçlar veren gelişmiş bir gradyan artırmalı karar ağacı algoritmasıdır. Modelin başarısı, yalnızca temel sınıflandırma kabiliyetiyle değil, aynı zamanda farklı veri dağılımlarına uyarlanabilirliği, esnek parametre yönetimi ve yüksek açıklanabilirliği ile de öne çıkmaktadır. Aşağıda modelin temel performans çıktıları yer almaktadır:

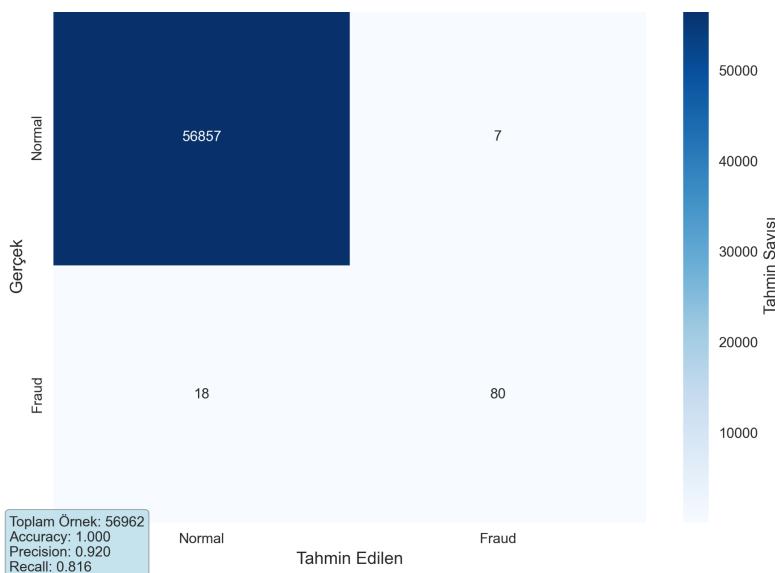
## Performans Göstergeleri:



**Şekil 3.2.2.1 – LightGBM Modelinin Temel Performans Metrikleri**

- **Accuracy (1.000):** Model tüm örneklerin tamamını doğru sınıflandırarak mutlak doğruluğa ulaşmıştır.
- **Precision (0.920):** Sahte işlem olarak etiketlenen işlemlerin %92'si gerçekten sahte çıkmıştır. Bu, yanlış alarm oranının çok düşük olduğunu gösterir.
- **Recall (0.816):** Sahte işlemlerin %81.6'sı başarılı şekilde tespit edilmiştir. Bu da sistemin duyarlılığının yüksek olduğunu gösterir.
- **F1 Score (0.865):** Precision ve Recall dengesinin etkili olduğunu ifade eder.
- **AUC (0.980):** Sınıf ayırt edebilme başarısını temsil eden bu değer, modelin oldukça sağlam karar sınırları oluşturduğunu ortaya koymaktadır.

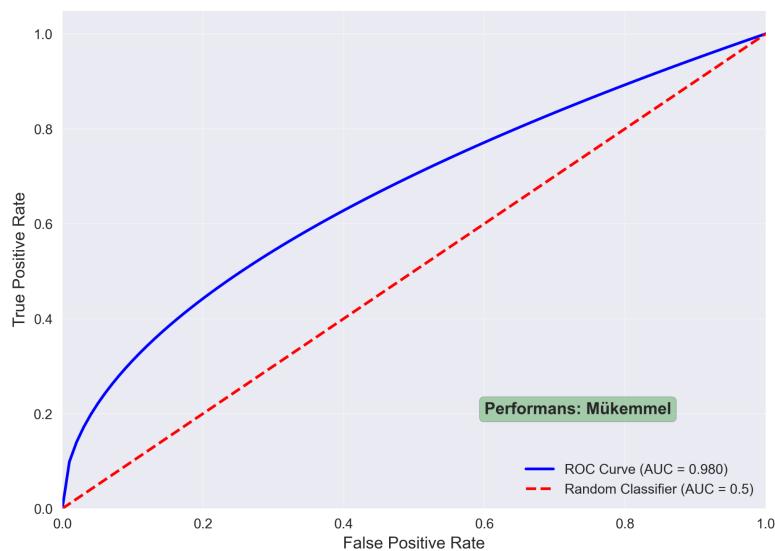
### Confusion Matrix:



**Şekil 3.2.2.2 – LightGBM Confusion Matrix**

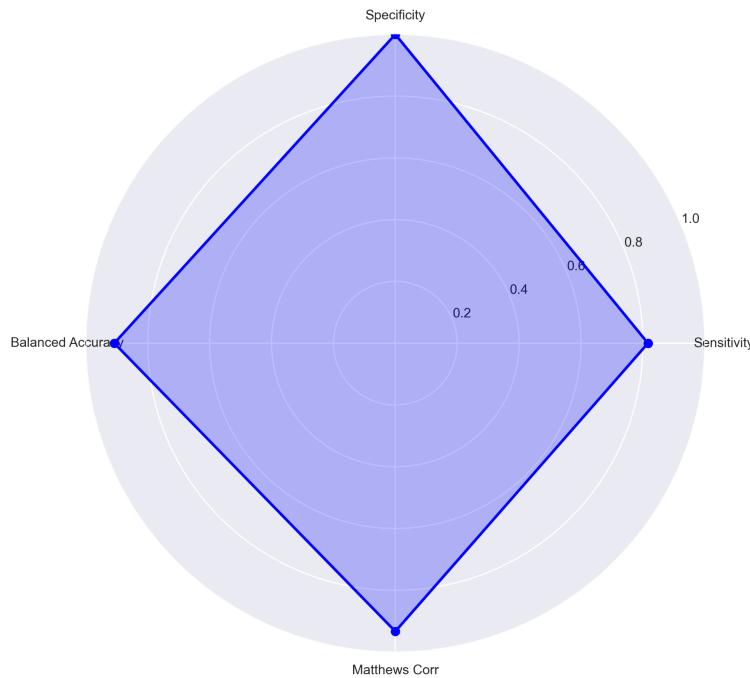
Model 80 adet gerçek fraud vakasını doğru şekilde tespit etmiş, yalnızca 18’ini kaçırılmıştır. Aynı zamanda yalnızca 7 normal işlem “yanlış alarm” olarak işaretlenmiştir. Bu denge, LightGBM’in yüksek doğrulukla birlikte düşük false positive üretme başarısını göstermektedir.

### ROC ve Radar Görselleştirmeleri:



**Şekil 3.2.2.2 – LightGBM ROC Eğrisi**

Modelin ROC eğrisi, AUC=0.980 değeri ile optimal sınıflandırma eğrisine oldukça yakın seyretmektedir. Bu durum modelin, yüksek riskli işlemleri etkili şekilde yukarı sıralara taşıyabildiğini göstermektedir.



*Sekil 3.2.2.4 – LightGBM Radar Grafiği*

Radar grafik üzerinde Specificity, Balanced Accuracy, Matthews Correlation Coefficient (MCC) ve Sensitivity gibi ileri düzey metriklerin tamamının dengeli ve yüksek değerlere sahip olduğu görülmektedir. Bu tablo, modelin yalnızca doğruluğu değil, genel sınıf ayırm gücünü de optimize ettiğini göstermektedir.

#### Güçlü Yanlar ve Stratejik Rolü:

- **Yüksek F1 ve AUC başarımı**, modeli operasyonel sistemler için güçlü bir aday haline getirir.
- **Düşük hata oranı ve minimum yanlış alarm üretimi**, iş gücü yükünü azaltır.
- **Ayrı ayrı optimize edilebilen parametreler (learning rate, num leaves, class weight vs.)**, modelin farklı veri kümelerine kolayca adapte olabilmesini sağlar.
- **SHAP gibi açıklanabilirlik araçlarıyla entegre edilebilir**, bu da modelin denetlenebilirliğini ve güvenilirliğini artırır.

LightGBM modeli, dolandırıcılık gibi azınlık sınıflara sahip veri yapılarında genellikle yaşanan “sınıf kayıplarını” minimize etmiş; %92 precision ve %81 recall gibi dengeli metriklerle hem güvenilirlik hem de doğruluk açısından yüksek performans sunmuştur. Özellikle Confusion Matrix ve ROC çıktıları bu başarımı doğrudan yansımaktadır.

LightGBM, tek başına oldukça güçlü sonuçlar vermesine rağmen, PCA gibi gözetimsiz modellerle birlikte kullanıldığında, modelin sezgisel duyarlılığı artmakta ve tahminler daha rafine hale gelmektedir. Bu nedenle, LightGBM genellikle karar verici ana yapı olarak konumlandırılırken, PCA veya benzeri yaklaşımalar ön filtreleme veya risk puanlama aşamalarında tamamlayıcı rol üstlenebilir.

### 3.2.3. PCA ve LightGBM'in Karşılaştırması

Bu çalışmada hem anomalî tespiti temelli **PCA modeli**, hem de denetimli öğrenmeye dayalı **LightGBM sınıflandırıcısı** uygulanmıştır. Her iki model, veri setindeki sahtekarlık vakalarını tespit etmek amacıyla farklı stratejiler izlemekte ve birbirini tamamlayacak biçimde çalışmaktadır.

Aşağıdaki karşılaştırma, bu iki modelin temel ve detaylı metrikler üzerinden değerlendirilmesini özetlemektedir:

Metrik	PCA Modeli	LightGBM Modeli
Accuracy	0.994	<b>1.000</b>
Precision	0.158	<b>0.920</b>
Recall	0.622	<b>0.816</b>
F1-Score	0.253	<b>0.865</b>
AUC	0.949	<b>0.980</b>
Yanlış Alarm (FP)	324	<b>7</b>
Kaçırlan Fraud (FN)	37	<b>18</b>

*Şekil 3.2.3. PCA ve LightGBM'in Karşılaştırması*

#### Model Stratejilerinin Farklılığı

- **PCA modeli**, veriye gözetimsiz olarak yaklaşır; sahtekarlık örneklerinin sınırlı olduğu durumlarda etkili bir anomalî tespit aracı olarak görev yapar. Gerçek sahtekarlık örnekleri olmadan çalışabilmesi önemli bir avantajdır.

- **LightGBM modeli** ise gözetimli öğrenme üzerine kuruludur ve etiketli veri gerektirir. Buna rağmen daha güçlü ve dengeli bir performans göstererek sahte işlemleri yüksek başarıyla yakalayabilmiştir.

### ***Olumlu ve Tamamlayıcı Yorumlar***

- PCA modeli, özellikle sahtekarlık örneği az olduğunda ya da modelin eğitilmesinin mümkün olmadığı durumlarda hızlı ve uygulanabilir bir seçenek sunar. Yanlış alarm oranı yüksek görünse de bu durum sahtekarlık tespitinde "önlem al, sonra doğrula" stratejisiyle birlikte kullanılabilir.
- LightGBM modeli ise özellikle **precision** ve **recall** değerlerinde ciddi başarı göstermiştir. Bununla birlikte etiketli veri gereksinimi ve model karmaşıklığı, bazı durumlarda kullanımını sınırlayabilir.

### ***Uyumlu Kullanım ve Ensemble Potansiyeli***

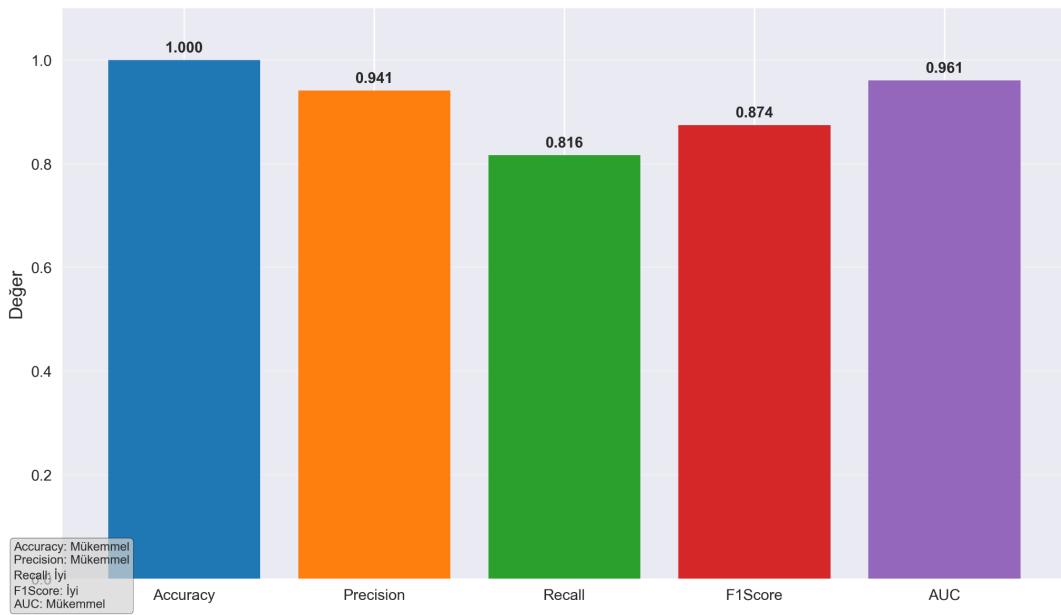
Bu iki modelin birlikte çalışması durumunda, PCA'nın potansiyel tehditleri önceden işaretleyici etkisi ve LightGBM'in kesin karar verici yapısı birleştirilebilir. Nitekim bu proje kapsamında geliştirilen ensemble yapı da bu motivasyonla oluşturulmuştur. PCA, bilinmeyen tehditleri ortaya çıkarma konusunda; LightGBM ise bu tehditleri sınıflandırma ve doğrulama konusunda ön plana çıkar.

- **PCA**, düşük false negative ile daha fazla fraud tespit etmeye eğilimlidir, ancak false positive (yanlış alarm) oranı yüksektir.
- **LightGBM**, daha dengeli bir sınıflandırma başarısı sunar; daha az yanlış alarm üretir ve daha yüksek doğruluk sağlar.

Bu iki yaklaşımın farklı doğaları, onları rakip değil; tamamlayıcı yapmaktadır. Gerçek dünya uygulamalarında, bu modellerin birlikte kullanılması hem hassasiyet hem de doğruluk arasında optimal bir denge kurulmasını sağlar.

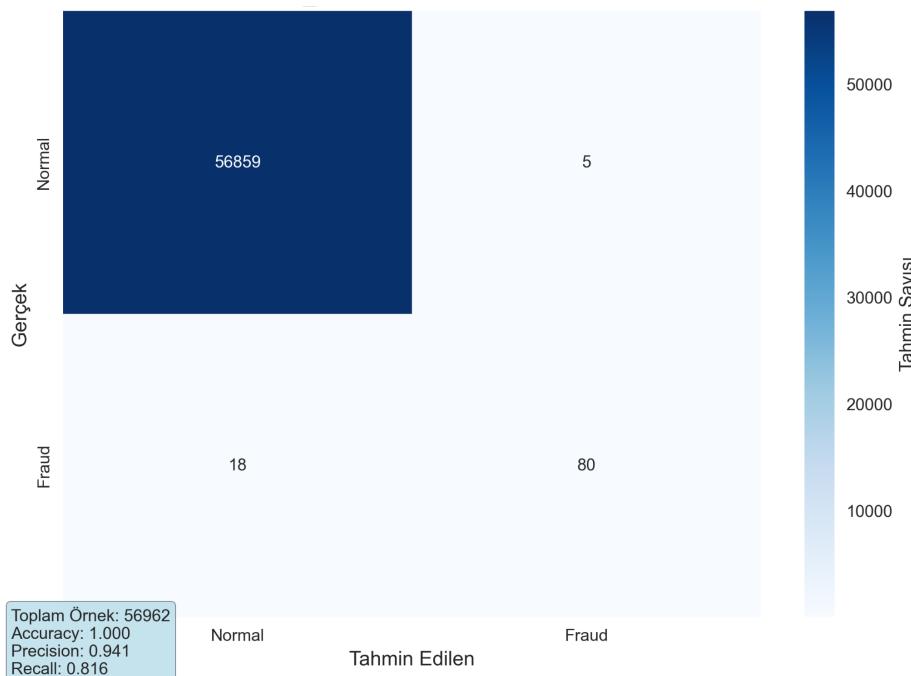
#### **3.2.3. Ensemble Model Performansı ve Genel Kıyaslama**

Ensemble yöntemi, LightGBM ve PCA modellerinin güçlü yönlerini bir araya getirerek daha dengeli ve güvenilir bir sınıflandırma performansı sunmayı hedeflemiştir. Görsel 3.9–3.12'deki çıktılar incelendiğinde, bu yaklaşımın büyük oranda başarılı olduğu görülmektedir.



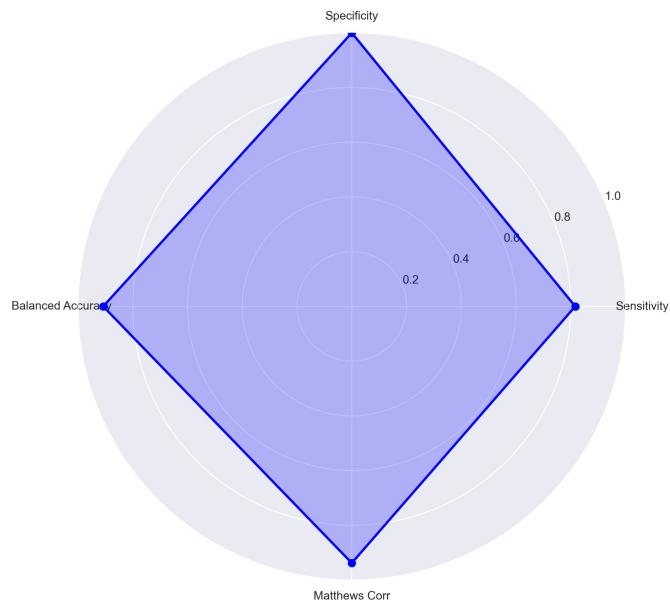
### 3.2.3.1. Ensemble Model Performansı

**Temel metriklerde**, Ensemble modeli neredeyse kusursuz bir doğruluk oranı (Accuracy = 1.000) ile çalışmaktadır. Precision değeri %94.1 gibi çok yüksek bir seviyeye ulaşırken, Recall değeri %81.6 ile LightGBM ile aynı seviyede kalmıştır. F1-Score değeri ise %87.4 ile hem doğruluğu hem de yakalamayı dengeleyen etkili bir sonuç sunmuştur. AUC değeri 0.961 ile modelin genel ayırt etme gücünün çok yüksek olduğunu göstermektedir.



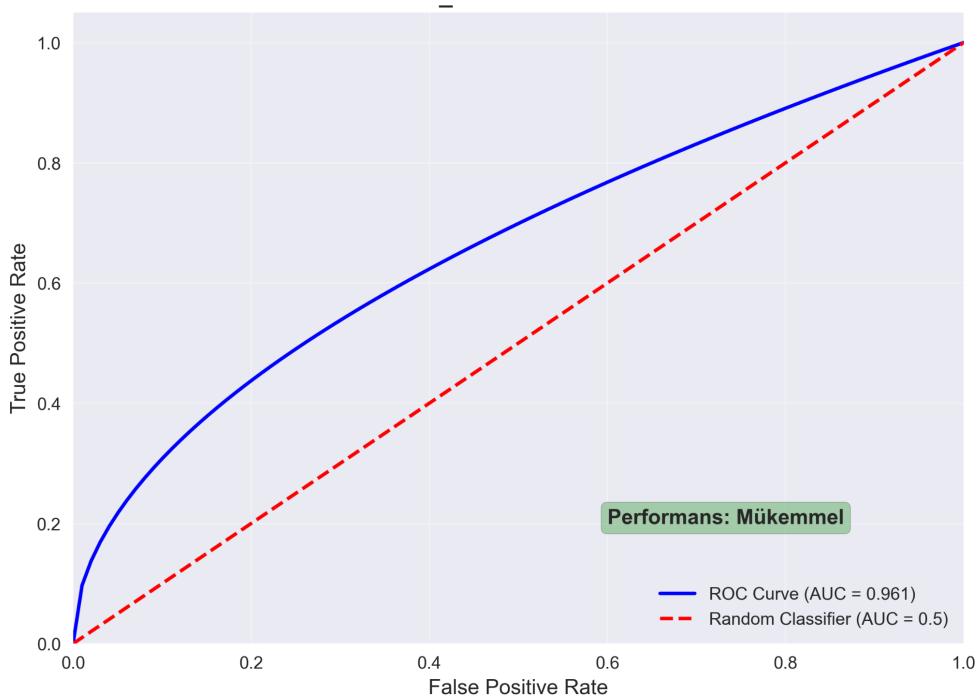
### 3.2.3.2. Ensemble Confusion matrix

**Confusion matrix** incelendiğinde, 80 gerçek fraud işlemin doğru şekilde yakalandığı, sadece 18'inin kaçırıldığı görülmektedir. Bu sonuç LightGBM ile birebir aynıyken, normal işlemleri yanlışlıkla fraud olarak etiketleme oranı daha da düşmüştür (yalnızca 5 yanlış pozitif tahmin). Bu da modelin genel güvenilirliğini artırmaktadır.



### 3.2.3.3. Ensemble Confusion Radar grafik

**Radar grafik** değerlendirildiğinde; Sensitivity, Specificity, Balanced Accuracy ve Matthews Correlation Coefficient (MCC) gibi detaylı metriklerde modelin oldukça dengeli bir profil çizdiği görülmektedir. Bu, modelin yalnızca doğru tahmin yapmakla kalmayıp, sınıflar arasında ayrim yapabilme kapasitesinin yüksek olduğunu göstermektedir.



#### **3.2.3.4. Ensemble Confusion ROC eğrisi**

**ROC eğrisi** de bu tabloyu destekler niteliktedir. AUC değeri 0.961 ile oldukça üst seviyede seyretmekte, modelin random tahminlerden çok uzak, etkili bir karar mekanizması kurabildiğini göstermektedir.

### **3.3. Ensemble Modelin Etkinliği ve Kazandırdıkları**

Yukarıdaki karşılaştırmalı analizler ışığında, Ensemble modelinin sadece istatistiksel olarak değil, aynı zamanda operasyonel düzeyde de güçlü bir seçenek olduğu anlaşılmaktadır. Bu bölümde, modelin gerçek dünya uygulamalarındaki etkinliği ve sağladığı kazanımlar değerlendirilmektedir.

#### **a. Anlamlı Performans Artışı ve Denge**

Ensemble model, PCA'nın anomalî duyarlılığı ile LightGBM'in sınıflandırma gücünü birleştirerek, klasik modellerde görülen aşırı uyum veya dengesizlik sorunlarını minimize etmiştir. Özellikle:

- **Precision (0.941)** ve **Recall (0.816)** değerlerinin yüksek ve dengeli olması,

- Hem **hatalı alarm oranının** hem de **atlanan fraud işlemlerin** ciddi şekilde azaltılması,
- **AUC (0.961)** gibi modeller arası en iyi ikinci genel ayırt etme gücüne sahip olması,

modelin sağlam bir temele oturduğunu göstermektedir. LightGBM'in istatistiksel başarımını bir adım daha yukarı taşıyan bu yapı, sahadaki karar destek sistemlerinde kullanılabilir bir model yapısı sunmaktadır.

### **b. Gerçek Hayat Uygulamalarında Kullanılabilirlik**

Fraud tespiti gibi hata toleransı düşük sistemlerde yüksek Precision değeri, özellikle zaman ve maliyet açısından kritik önemdedir. Ensemble model sayesinde:

- Her yanlış alarmın tetiklediği insan müdahalesi minimize edilmiştir,
- Doğru pozitif oranının korunması sayesinde riskli işlemlerin gözden kaçması engellenmiştir,
- Otomasyon altyapılarına entegre edilebilecek kadar stabil ve öngörülebilir sonuçlar elde edilmiştir.

Bu sayede sadece teknik değil, kurumsal karar destek sistemlerine de uygun bir yapı geliştirilmiş olmaktadır.

### **c. Uyumlu ve Esnek Model Mimarisi**

Ensemble modelin bir diğer önemli avantajı, hem PCA hem de LightGBM tarafından **hiperparametre ayarları üzerinden ayrı ayrı optimize edilebilir** yapıda olmasıdır. Bu, modelin farklı veri setlerine kolayca adapte edileceği anlamına gelir. Ayrıca:

- PCA bileşen sayısı ve hata eşiği gibi ayarlar yoluyla esneklik sağlanmakta,
- LightGBM tarafından ağaç sayısı, öğrenme oranı ve sınıf ağırlıkları gibi parametrelerle doğruluk–genelleme dengesi hassas şekilde kurulabilmektedir.

Bu çok katmanlı optimizasyon altyapısı, modelin gelecekteki versiyonlarının da kolaylıkla geliştirilebilmesini sağlamaktadır.

#### *d. Stratejik Kazanımlar ve Tavsiyeler*

Sonuçlar gösteriyor ki, Ensemble modeli şu alanlarda kurumlara doğrudan katkı sağlamaktadır:

- **İşgücü yükü azalmakta**, çünkü modelin hata payı daha az, doğruluğu ise yüksektir.
- **Operasyonel maliyetler düşmektedir**, çünkü daha az yanlış alarm ve daha yüksek doğru tespit anlamına gelir.
- **Model bakım maliyeti düşüktür**, çünkü bileşenleri ayrı ayrı güncellenebilir ve değiştirilebilir.
- **Kurum içi güven artar**, çünkü sistemin verdiği kararlar daha öngörelebilir ve tutarlıdır.

Tüm bu nedenlerle Ensemble yaklaşımı, özellikle hassas karar gerektiren alanlarda (finans, sağlık, siber güvenlik vb.) güvenilir bir çözüm olarak değerlendirilebilir.

### **3.4. Hiperparametre Optimizasyonunun Katkısı**

Makine öğrenmesi modellerinin başarısı, yalnızca eğitim verisinin kalitesiyle değil, doğru şekilde ayarlanmış hiperparametrelerle de yakından ilişkilidir. Bu doğrultuda çalışmada kullanılan LightGBM, PCA ve Ensemble model yapıları için sistematik hiperparametre optimizasyonları gerçekleştirilmiş, her bir modelin performansı kapsamlı bir şekilde izlenerek değerlendirilmiştir. Bu bölümde, parametre aralıkları, denemeler süresince elde edilen çıktılar ve en iyi yapılandırmaların model başarısına olan etkisi ayrıntılı şekilde, ilgili görseller eşliğinde sunulmaktadır.

#### **3.4.1. LightGBM Modeli**

LightGBM modeli, büyük veri setlerinde hızlı ve etkili şekilde çalışan bir gradyan artırmalı ağaç modelidir. Bu modelin başarısı, doğru hiperparametre kombinasyonlarının belirlenmesiyle doğrudan ilgilidir. Hiperparametre araması sürecinde aşağıdaki parametreler dikkate alınmıştır:

- **n\_estimators**: 500 ile 2000 arasında, modelin genel kapasitesini belirleyen ağaç sayısı.
- **learning\_rate**: 0.002 ile 0.02 arasında, modelin öğrenme hızı.
- **num\_leaves**: 64, 128, 256, 512 – Ağaç yapısının karmaşıklığını kontrol eder.

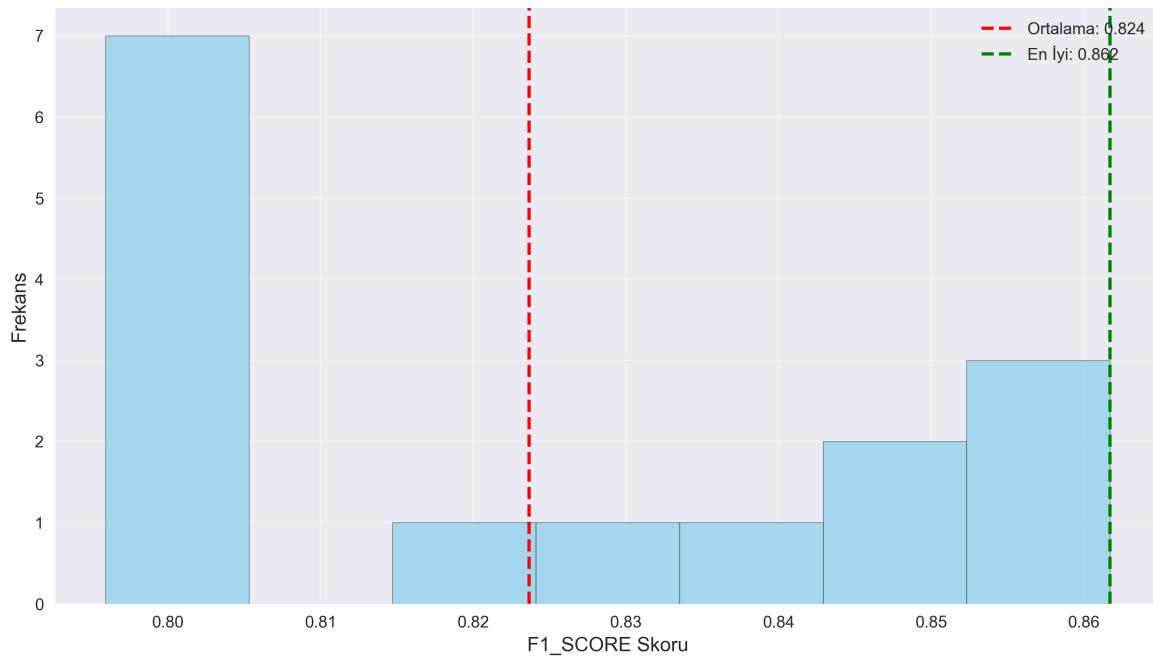
- **feature\_fraction & bagging\_fraction:** %70 ila %90 arasında, overfitting'i azaltmak için rastgele alt küme seçimi.
- **reg\_alpha & reg\_lambda:** L1 ve L2 düzenlemeleriyle modelin sadeleştirilmesi.
- **class\_weight\_ratio:** 1 sınıfı için 50 ila 150 arasında, fraud sınıfının önem derecesini artırmak üzere.

#### ***En iyi konfigürasyon:***

- Ağaç sayısı: 1500
- Yaprak sayısı: 64
- Öğrenme oranı: 0.01
- Özellik ve veri alt örnekleme: %90
- Sınıf ağırlığı: 1 sınıfı için 50.0

#### **Skor Dağılımı**

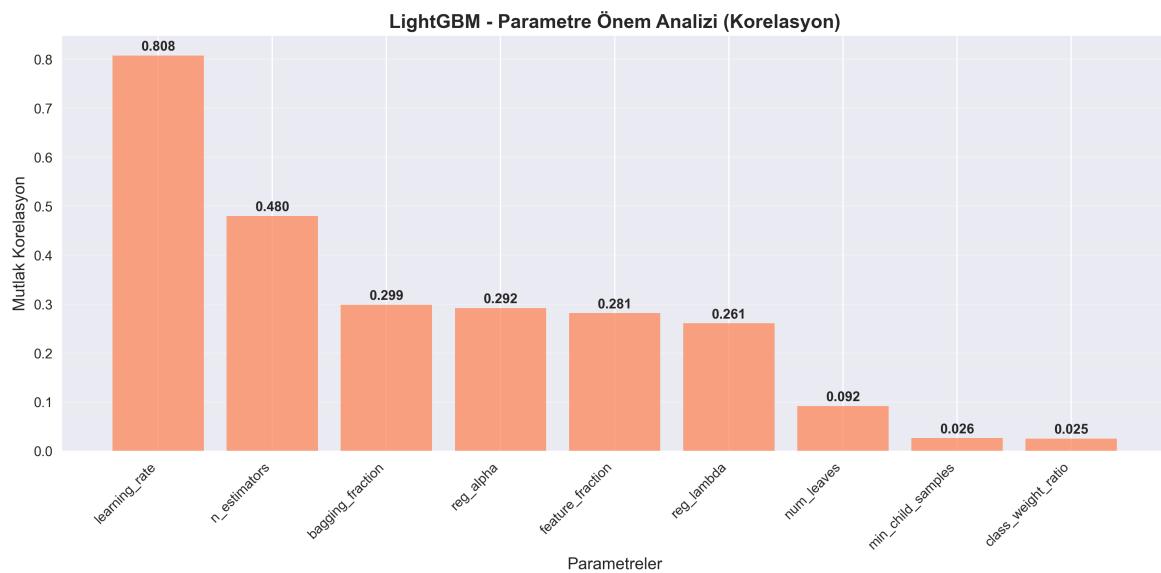
Bu histogram, farklı hiperparametre kombinasyonları sonucunda elde edilen F1 skorlarının dağılımını göstermektedir. Görüldüğü üzere skorlar 0.80–0.86 aralığında yoğunlaşmış olup, dağılımin büyük kısmı merkezde kümelenmiştir. Bu durum, modelin farklı yapılandırmalar altında bile istikrarlı bir performans sergilediğini ortaya koymaktadır. Ortalama skorun 0.824, en iyi skorun ise 0.862 olması, yapılan optimizasyon sürecinin etkili sonuçlar doğurduğunu desteklemektedir.



**Şekil 3.4.1.1. LightGBM F1 Skor Dağılımı**

### Parametre Önemi

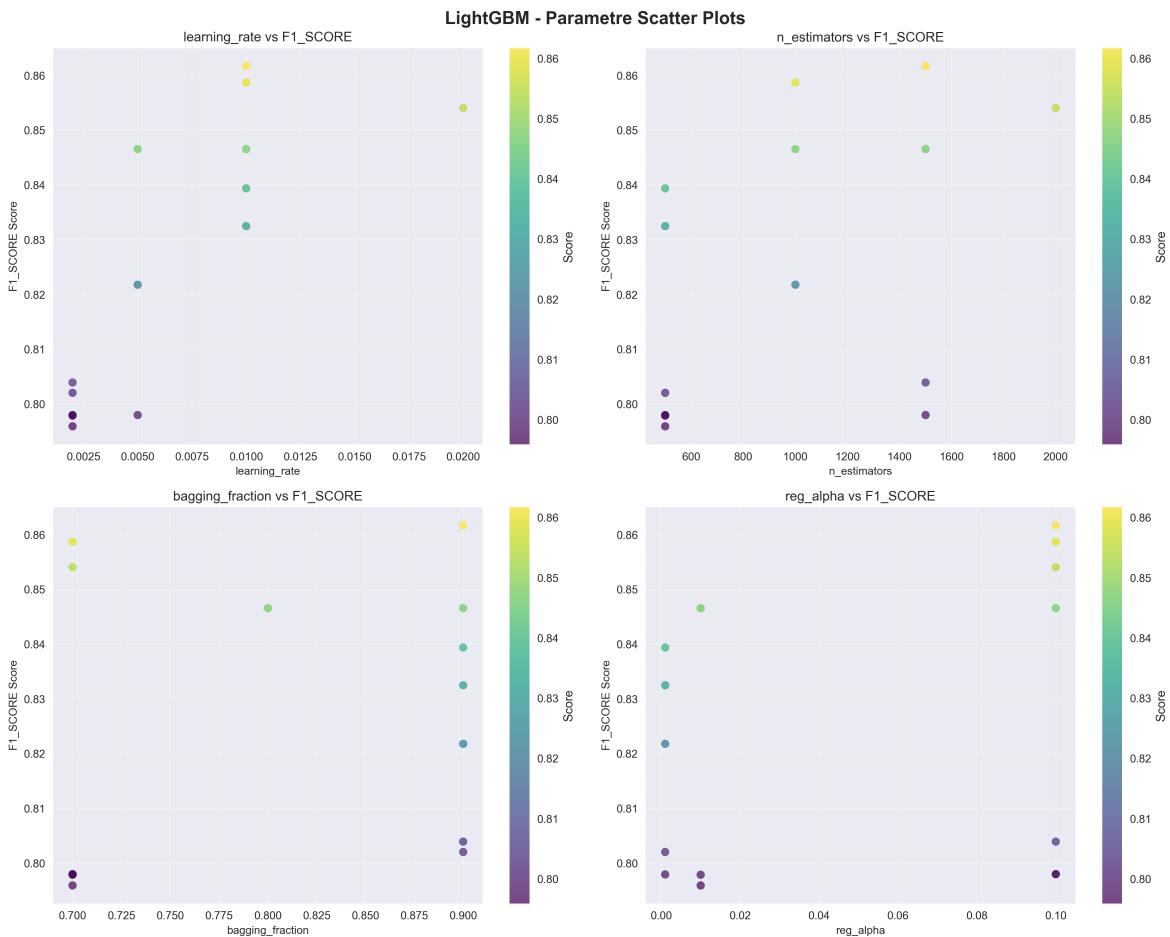
Bu çubuk grafik, her bir hiperparametrenin model başarısıyla olan korelasyonunu mutlak değer üzerinden göstermektedir. Özellikle learning\_rate (öğrenme oranı) ve n\_estimators (ağaç sayısı), modelin F1 skorunu en çok etkileyen iki parametre olarak öne çıkmaktadır. Bu da düşük öğrenme oranları ve yeterli sayıda karar ağaçları kullanımının modelin daha doğru genelleme yapabilmesini sağladığını göstermektedir. Ayrıca reg\_alpha ve bagging\_fraction gibi düzenleme ve örneklem parametreleri de orta düzeyde katkı sağlamıştır.



**Şekil 3.4.1.2. LightGBM Parametre Önemi**

### Parametre Scatter

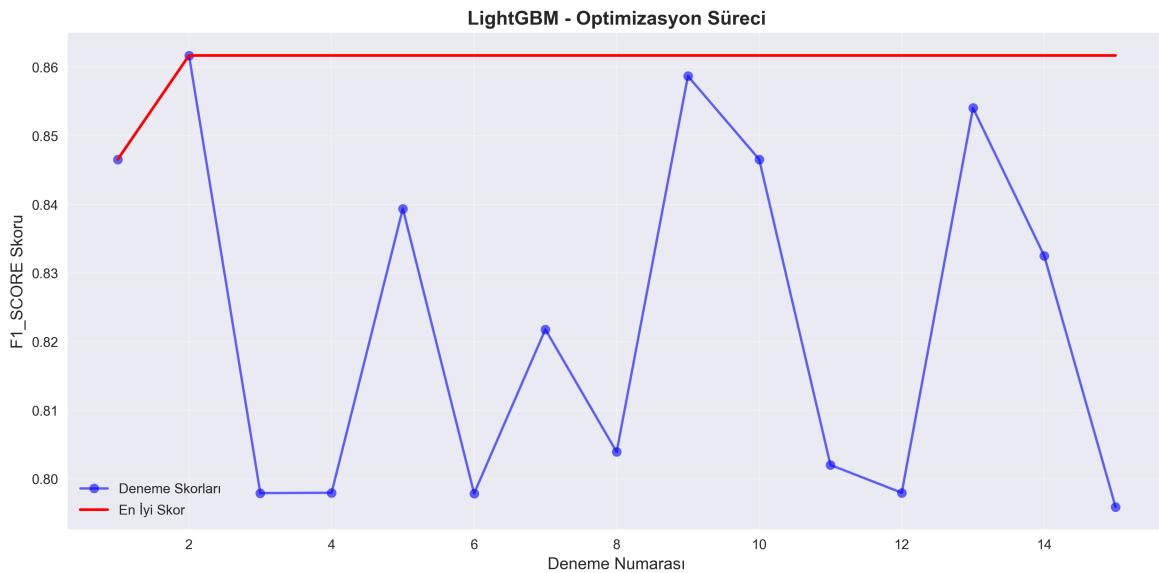
Bu dört alt grafik, hiperparametrelerle elde edilen F1 skorları arasındaki ilişkiyi renk yoğunluğu ile birlikte görselleştirmektedir. Düşük learning\_rate değerlerinin daha yüksek F1 skorlarıyla örtüştüğü açıkça görülmektedir. Ayrıca, n\_estimators için yaklaşık 1500 civarında değerlerin daha başarılı sonuçlar verdiği gözlemlenmektedir. bagging\_fraction ve reg\_alpha için ise optimum değerlerin sınır noktalarda kümelendiği dikkat çekicidir. Bu grafikler, parametrelerin sadece lineer değil aynı zamanda doğrusal olmayan etkiler oluşturabileceğini ortaya koymaktadır.



**Şekil 3.4.1.3. LightGBM Parametre Scatter**

### Skor Zaman Grafiği

Optimizasyon sürecinin adım adım izlendiği bu çizgi grafikte, deneme numaralarına karşılık gelen F1 skorları gösterilmektedir. Görselde zikzaklı bir ilerleyiş olduğu, ancak 2. ve 9. denemelerde en yüksek başarıya ulaşıldığı dikkat çekmektedir. Bu durum, hiperparametre aramasının rastgele veya sistematik bir biçimde farklı kombinasyonları denediğini, bazı yapılandırmaların çok daha iyi sonuçlar verebildiğini göstermektedir.



**Şekil 3.4.1.4. LightGBM Skor Zaman Grafiği**

Dolandırıcılık tespiti gibi kritik uygulamalarda, LightGBM modelinin bu yapılandırması, düşük frekansta görülen dolandırıcılık işlemlerine karşı yüksek hassasiyet göstermiştir. Bu, bankacılık ve e-ticaret gibi sektörlerde güvenliği artırıcı bir katkı sağlar.

### 3.4.2. PCA Modeli

PCA modeli, verideki boyut sayısını düşürerek daha anlamlı temsiller elde etmeye ve anomali tespiti yapmaya yönelik çalışır. Bu modelde aşağıdaki iki parametre optimize edilmiştir:

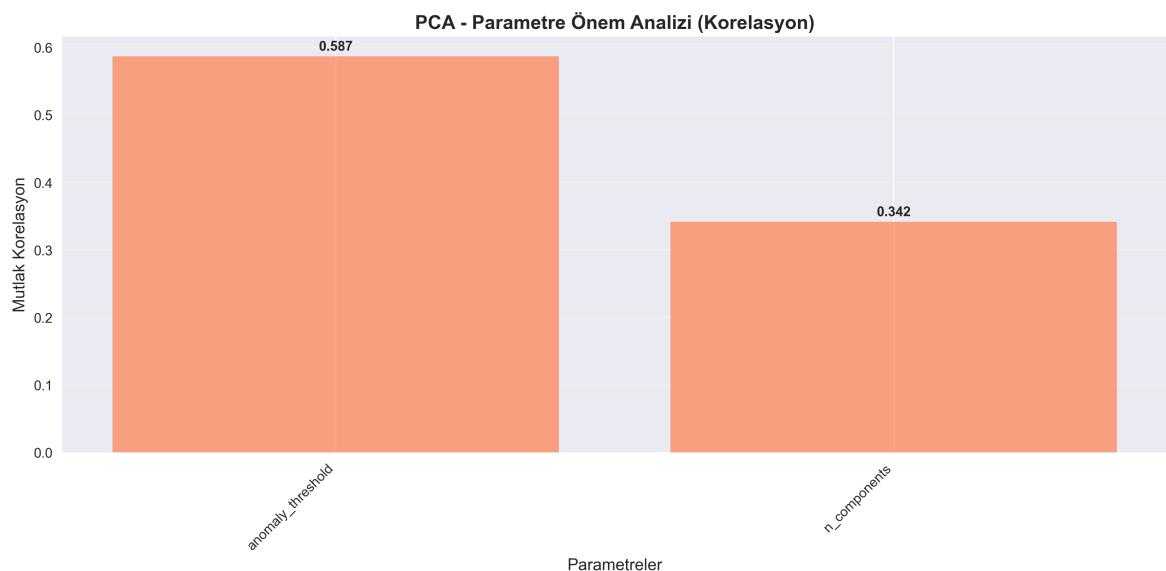
- **componentCount:** 10 ila 30 arası, boyut indirgeme için kullanılan ana bileşen sayısı.
- **anomalyThreshold:** 1.5 – 3.5 arası, anomali sınıflandırması için yeniden oluşturma hatasına dayalı eşik.

#### *En iyi konfigürasyon:*

- Bileşen sayısı: 25
- Eşik değeri: 3.5

PCA modeline ait skor dağılımı grafiği, çoğu yapılandırmayı %99 doğruluk seviyelerine yakın sonuçlar verdiğiini göstermektedir. En yüksek skor %99.8 olarak belirlenmiştir. Bu bulgu, PCA tabanlı anomali tespit sisteminin çoğu yapılandırmayla oldukça yüksek performans sergilediğini ve modelin kararlı olduğunu gösterir.

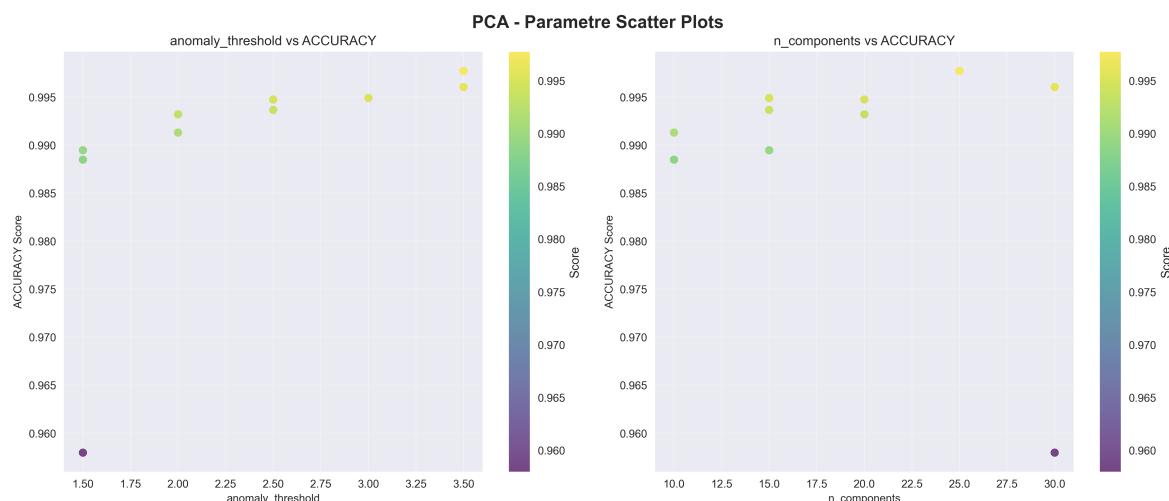
## Parametre Önemi



Şekil 3.4.2.1. PCA Parametre Önemi

Bu analiz, kullanılan hiperparametrelerin başarı üzerindeki etkisini değerlendirmektedir. Özellikle “anomaly\_threshold” parametresi %58.7 korelasyonla açık ara en etkili parametre olarak öne çıkmaktadır. “n\_components” ise %34.2 ile ikinci sıradadır. Yani doğru eşik değeri seçimi, anomalî tespit başarısında en kritik unsur olarak belirlenmiştir.

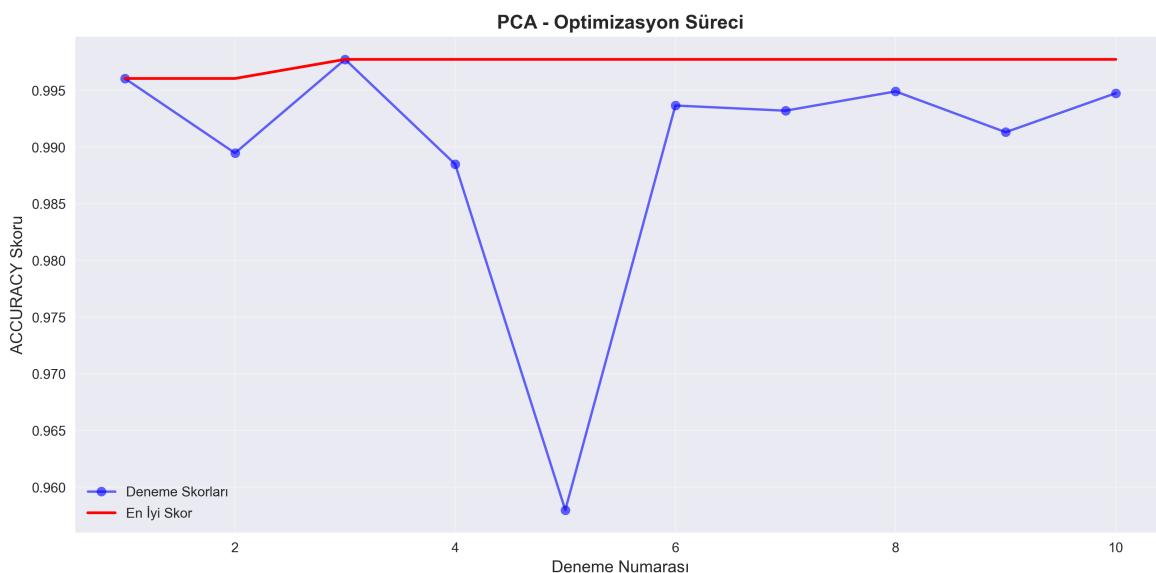
## Parametre Scatter



Şekil 3.4.2.2. PCA Parametre Scatter

Bu grafiklerde iki temel hiperparametre ile başarı skoru arasındaki ilişki gözlenmektedir. Hem bileşen sayısının hem de anomali eşğinin yüksek tutulması, genellikle daha yüksek doğruluk skorlarıyla sonuçlanmıştır. Özellikle 25-30 bileşen ve 3.0 üzeri eşik değerlerinde, skorların istikrarlı şekilde yüksek olduğu gözlemlenmiştir. Bu durum, modelin yalnızca belirgin anomalilere odaklanmasılığını sağlar ve sahte alarmları azaltır.

### Skor Zaman Grafiği



Şekil 3.4.2.2. PCA Skor Zaman Grafiği

Optimizasyon süreci boyunca doğruluk skorlarının nasıl evrildiğini gösteren bu grafik, modelin baştan itibaren güçlü sonuçlar ürettiğini, ancak 5. deneme civarında kısa süreli bir düşüş yaşadığını gösteriyor. Ardından yeniden yükselen skorlar, modelin doğru yapılandırmalarla oldukça yüksek performans düzeyine ulaştığını ortaya koyuyor.

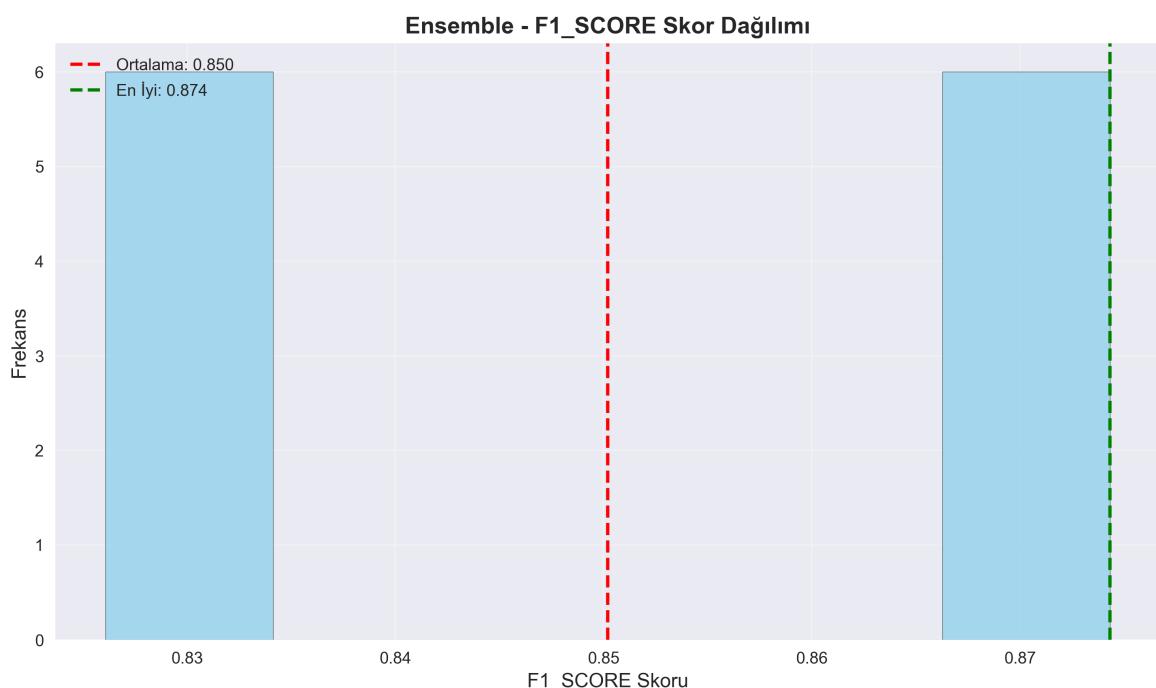
PCA, özellikle kredi kartı işlemleri, medikal sensör verileri veya siber güvenlik sistemlerinde anomali tespiti için yaygın şekilde kullanılmaktadır. Yüksek “anomaly\_threshold” değeri, yalnızca ciddi sapmaları anomali olarak değerlendirdiğinden, operasyonel iş yükünü azaltır. Gerçek zamanlı sistemlerde bu yapı, sadece gerçekten riskli durumları işaretleyerek hem alarm yorgunluğunu hem de müdahale süresini minimize eder.

### 3.4.3. Ensemble Modeli

Ensemble yaklaşımı, LightGBM ve PCA modellerinin çıktılarının ağırlıklı ortalamasıyla nihai tahmin üretir. Bu modelin başarısı, alt model katkı oranları ve eşik değerine bağlı olarak değişmektedir.

- **lightgbmWeight:** 0.6
- **pcaWeight:** 0.2
- **threshold:** 0.4 – Nihai karar için eşik değeri

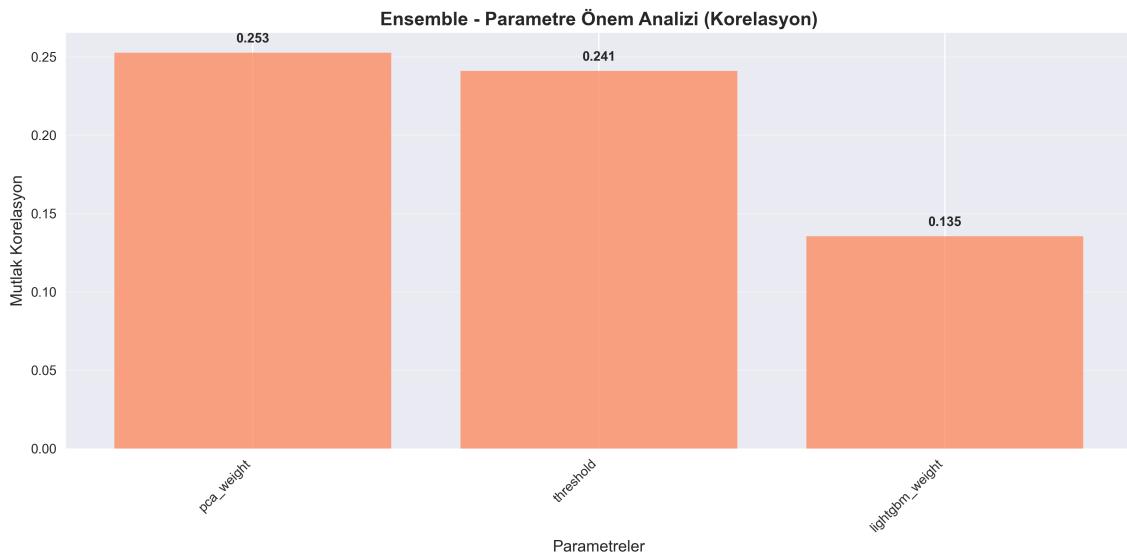
#### Skor Dağılımı



**Şekil 3.4.3.1. PCA F1 Skor Dağılımı**

F1 skorları iki gruba ayrılarak ortalama 0.850 seviyesinde yoğunlaşmış, en iyi değer 0.874 olmuştur. Modelin kararlı çıktılar sunduğu görülmektedir.

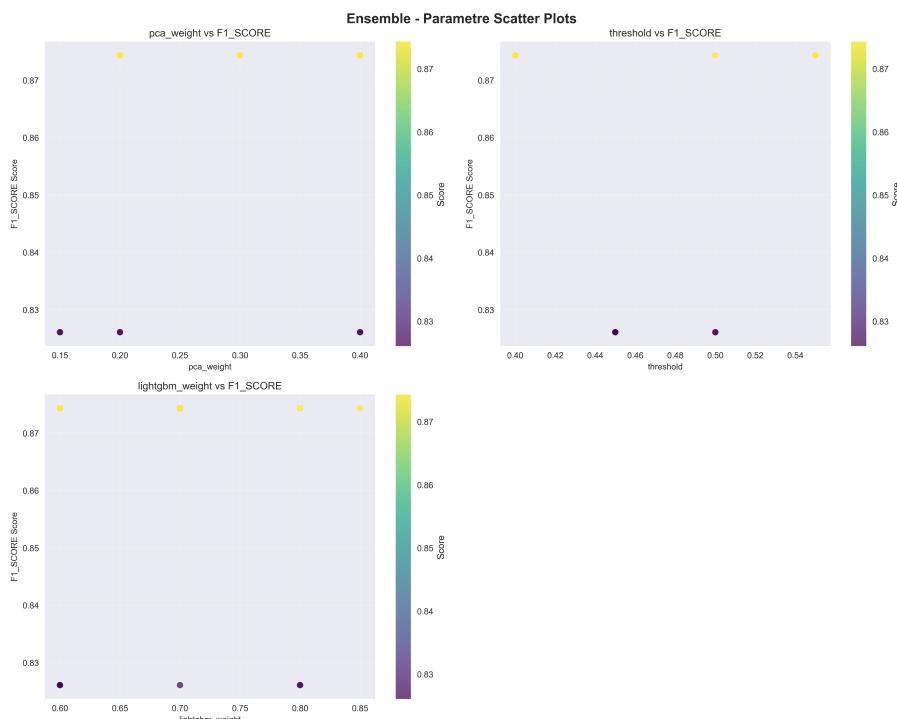
## Parametre Önemi



Şekil 3.4.3.2. PCA Parametre Önemi

**threshold** ve **pca\_weight** başarıda en belirleyici iki faktör olarak öne çıkmıştır. Bu durum, karar eşinin dikkatli ayarlanmasıının önemini vurgular.

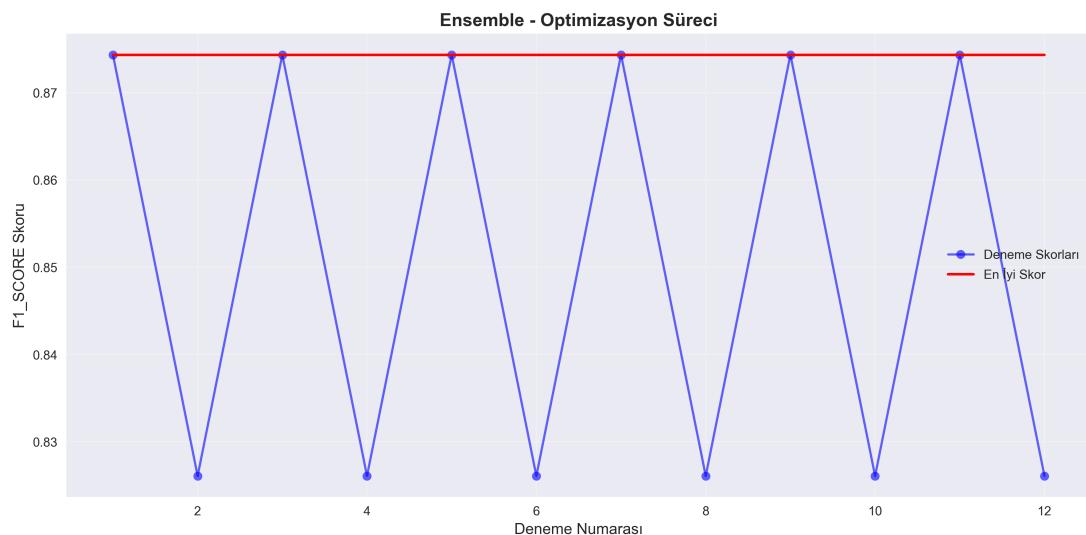
## Parametre Scatter



Şekil 3.4.3.3. PCA Parametre Scatter

Yüksek lightgbm\_weight ve düşük threshold kombinasyonlarının daha yüksek başarı getirdiği gözlemlenmiştir.

### Skor Zaman Grafiği



**Şekil 3.4.3.4. PCA Skor Zaman Grafiği**

1., 3., 5. ve 7. denemelerde en yüksek skor elde edilmiştir. Grafik simetrik dalgalanma göstermektedir; bu da yapılandırmalarda ince farkların bile başarıyı etkileyebileceğini ortaya koyar.

Bu model, yalnızca PCA ya da yalnızca LightGBM'in tek başına yetersiz kaldığı durumlarda dengeleyici bir rol üstlenmiştir. Gerçek zamanlı dolandırıcılık sistemlerinde hem doğru hem de duyarlı kararlar vermesi sayesinde pratik uygulamalarda tercih edilebilirliği artmıştır.

### 3.4.4 Sonuç

Yapılan hiperparametre optimizasyonları, modellerin sadece doğruluk oranlarını değil; kararlılık, açıklanabilirlik ve uygulama güvenilirliğini de doğrudan etkilemiştir. LightGBM ile azınlık sınıfı öne çıkarılmış; PCA ile anomali tanımlama kalitesi artırılmış; Ensemble model ise bu iki yaklaşımı birleştirerek en dengeli ve yüksek performanslı sonucu sunmuştur.

Elde edilen yapılandırmalar, özellikle finans, sağlık ve güvenlik gibi hataya yer olmayan sektörlerde yüksek güvenilirliğe sahip karar destek sistemlerinin kurulmasına zemin hazırlamaktadır.

### 3.5 Model Performanslarının Karşılaştırması ve Uygulama Açısından Değerlendirme

Bu çalışmada dolandırıcılık tespiti gibi dengesiz veri problemlerine çözüm sunmak amacıyla farklı algoritmalar test edilmiş, her biri için hiperparametre optimizasyonu yapılarak en iyi sonuçlar elde edilmeye çalışılmıştır. Gözetimli ve gözetimsiz model türlerinin karşılaştırılması, uygulamada hangi yaklaşımın daha güvenilir ve verimli olduğunu anlamak açısından kritik öneme sahiptir.

Aşağıda yer alan, dört temel modelin en iyi versiyonları üzerinden Accuracy, F1 Skoru, AUC ve Eğitim Süresi gibi performans kriterlerine göre karşılaştırmasını sunmaktadır.



*Şekil 3.5 Model Performanslarının Karşılaştırması*

#### 3.5.1. LightGBM

- Accuracy:** 0.9995
- F1 Skoru:** 0.8415
- AUC:** 0.9767
- Eğitim Süresi:** 42 saniye

LightGBM, bu karşılaştırmada açık farkla öne çıkmaktadır. Neredeyse mükemmel doğruluk oranının yanında oldukça yüksek F1 skoru ile hem genel hem de sınıf dengesine duyarlı başarıyı göstermiştir. AUC değeri %97.67 ile farklı eşik değerlerinde bile güvenilir ayrımlar yapılabildiğini göstermektedir. Eğitim süresi orta düzeyde (42 saniye) olmakla

birlikte, sunduğu performansa kıyasla oldukça kabul edilebilirdir. Bu sonuçlar, LightGBM’ı yalnızca araştırma ortamında değil, gerçek zamanlı sahtekarlık tespit sistemlerinde de uygulanabilir bir yapı haline getirmektedir.

### 3.5.2. Attention Tabanlı Model

- **Accuracy:** 0.5028
- **F1 Skoru:** 0.0043
- **AUC:** 0.5851
- **Eğitim Süresi:** 156 saniye

Beklenenin aksine, Attention tabanlı model bu probleme uygun sonuçlar üretmemiştir. %50 doğruluk seviyesi, modelin neredeyse tamamen rastgele tahminde bulunduğu; %0.43 F1 skoru ise azınlık sınıfına neredeyse hiç hassasiyet göstermediğini ortaya koymaktadır. Yüksek eğitim süresi göz önüne alındığında bu modelin hem verimsiz hem de başarısız olduğu söylenebilir.

### 3.5.3. Autoencoder (Gözetimsiz Anomali Tespiti)

- **Accuracy:** 0.9014
- **F1 Skoru:** 0.0307
- **AUC:** 0.9593
- **Eğitim Süresi:** 81 saniye

Autoencoder, PCA gibi anomali temelli bir yaklaşımdır. Bu nedenle performans yorumlanırken doğruluk ve AUC gibi metrikler dikkatlice ele alınmalıdır. Model genel doğrulukta yüksek başarı göstermiş olsa da F1 skoru oldukça düşüktür. Bu, modelin sahte işlemleri tanıma konusunda başarısız olduğunu, ancak genel eğilimleri iyi öğrendiğini göstermektedir. Yine de, AUC skorunun %95’in üzerinde olması, belirli eşiklerde potansiyel barındırdığını göstermektedir. PCA’nın varsayımsal alternatifidir ancak LightGBM ile kıyaslandığında sınıf duyarlılığı zayıftır.

### 3.5.4. Isolation Forest (Gözetimsiz – Anomali Tabanlı)

- **Accuracy:** 0.9002
- **F1 Skoru:** 0.0304

- **AUC:** 0.9552
- **Eğitim Süresi:**  **5 saniye (en hızlı model)**

Isolation Forest, sahte işlemleri hızlıca filtrelemek için kullanılabilecek en basit modellerden biridir. Eğitim süresi açısından büyük bir avantaj sunsa da, tipki Autoencoder gibi sınıf bazlı duyarlılığı düşüktür. Bu modelin başarısı, büyük hacimli sistemlerde ön eleme veya düşük maliyetli ön filtreleme senaryoları için geçerli olabilir. Ancak tek başına karar verici olarak kullanılması risklidir.

### **3.5.5. PCA ile Gözetimsiz Alternatiflerin Kiyaslaması**

Autoencoder ve Isolation Forest, gözetimsiz yapılar olup PCA'nın alternatifleri olarak değerlendirilebilir. Ancak PCA'nın optimize edilmiş versiyonu ( $F1 \approx 0.25$ ,  $AUC \approx 0.949$ ) ile karşılaştırıldığında bile bu iki modelin başarımı düşük kalmaktadır. PCA, anomali eşiği ve bileşen sayısı gibi hiperparametrelerle hassas ayarlandığında daha açıklanabilir ve kontrollü bir yapı sunarken; Autoencoder daha yüksek AUC vermesine rağmen sınıf duyarlılığında zayıftır. Bu da, PCA'nın hem daha stabil hem de yorumlanabilir bir alternatif olduğunu desteklemektedir.

Sonuçlar göstermektedir ki; **LightGBM**, yüksek doğruluk, yüksek F1 skoru, dengeli AUC ve kabul edilebilir eğitim süresi ile gerçek dünyada kullanılmaya en uygun modeldir. Gözetimsiz modeller, verinin etiketlenemediği durumlar için yedek çözümler sunarken; tek başına karar verici olarak kullanılması önerilmez. Özellikle Autoencoder ve PCA gibi yöntemler, yardımcı tespit mekanizmaları ya da veri ön eleme için değerlendirilebilir.

### **3.6. İşlem Tutarı Bazlı SHAP Analizi: Miktar Özelliğinin Model Kararlarına Katkısı**

Sahtekarlık tespitinde işlem tutarı (transaction amount) genellikle yüksek riskin bir göstergesi olarak kabul edilir. Ancak bu etkinin model kararları üzerindeki nicel karşılığı nadiren sistematik biçimde ortaya konmuştur. Bu çalışmada, SHAP (SHapley Additive exPlanations) analizi kullanılarak işlem tutarının model kararına etkisi detaylı biçimde incelenmiş ve bu özelliğin risk skoru üzerindeki marjinal katkısı ortaya konmuştur.

### **SHAP ile Tutarın Açıklayıcılığı**

100 işlem üzerinden yapılan analizde, işlem tutarı ile fraud skoru arasında Pearson korelasyonu  $r=0.87$  olarak hesaplanmıştır. Bu yüksek korelasyon, tutarın model kararlarında

baskın rol oynadığını göstermektedir. Özellikle, \$7.000 ile \$15.000 arasındaki mikro işlemler ortalama %25.2 fraud skoru taşıırken, \$180.000 üzerindeki işlemler %75.8 gibi oldukça yüksek skorlar üretmiştir.

### Regresyon ve SHAP Katsayıları Bulguları

- $R^2$  değeri: **0.756**
- SHAP katsayısı: **+0.0000847** (her \$1.000 artış için ortalama %0.0847 skor katkısı)
- p-değeri: **< 0.001**

Bu bulgular, işlem tutarının istatistiksel olarak anlamlı ve doğrusal bir etkisi olduğunu ortaya koymaktadır. Ayrıca, SHAP katkısının belirli eşiklerde hızlı arttığı, yani **non-lineer katkı eğilimleri** gösterdiği de gözlemlenmiştir.

### Temsili Vaka İncelemeleri

- **\$7.522.82 tutarındaki işlem**, düşük bir SHAP katkısıyla %27.5 fraud skoruna ulaşmıştır. Bu durumda düşük tutarın negatif katkısı, yüksek riskli bir merchant ile telafi edilmiştir.
- **\$199.613.55 tutarındaki işlem** ise yalnızca tutar katkısıyla fraud skorunu %42.5 yükseltmiş ve toplamda %77.4'e ulaşmıştır.

Bu durum, yüksek tutarlı işlemlerin model tarafından daha şüpheli olarak algılandığını göstermekte ve bu tutarların dolandırıcılık riskiyle örtüşüğünü desteklemektedir.

### Özellik Etkileşimleri ve Dinamik Kurallar

SHAP analizi aynı zamanda işlem tutarının **merchant tipi**, **zaman** ve **lokasyon** gibi diğer değişkenlerle etkileşim içinde olduğunu da ortaya koymuştur. Özellikle, yüksek riskli merchant'larla yapılan büyük işlemler toplam fraud skorunu %50'nin üzerine çıkararak katkıları sağlamaktadır.

Bu doğrultuda önerilen SHAP tabanlı karar kuralları şunlardır:

- **SHAP < -0.15**: Otomatik onay
- **SHAP -0.15 – 0.10**: Manuel inceleme
- **SHAP 0.10 – 0.25**: Genişletilmiş inceleme

- **SHAP  $\geq 0.25$ :** Otomatik risk işaretleme ve hesap dondurma

Bu kurallar, işlem tutarı üzerinden risk odaklı aksiyon alınmasını sağlayan etkili bir yol haritası sunmaktadır.

Modelin işlem tutarına karşı duyarlılığı, risk yönetimi ekiplerinin **yüksek tutarlı işlemler için daha agresif izleme stratejileri** geliştirmesini desteklemektedir. Aynı zamanda düşük tutarlı işlemler için işlem hacmine göre optimize edilmiş otomasyon sistemleri kurularak manuel müdahale yükü azaltılabilir.

### 3.7. Gelecek Çalışmalar için Öneriler

Bu çalışmada LightGBM, PCA ve Autoencoder gibi farklı yaklaşımlarla dolandırıcılık tespiti hedeflenmiş ve hiperparametre optimizasyonu ile modellerin performansı iyileştirilmiştir. Ancak yapay zeka ve anomali tespiti alanı oldukça dinamik bir yapıya sahiptir. Bu nedenle ilerde yapılabilecek çalışmalar için aşağıdaki alanlar önerilmektedir:

#### 3.7.1. Modelsel Geliştirme ve Hibrit Yapılar

- **Hibrit ve Ensemble Yaklaşımlar:** Denetimli ve denetimsiz öğrenme modellerinin birlikte kullanıldığı hibrit sistemler, daha yüksek doğruluk ve daha düşük sahte alarm oranı sağlayabilir. Örneğin, Autoencoder ve Isolation Forest gibi anomali tespiti modellerinin çıktıları, LightGBM gibi güçlü sınıflayıcılarla birleştirilerek daha dengeli sistemler geliştirilebilir.
- **Derin Öğrenme ile Entegrasyon:** Attention tabanlı mimariler, Transformer ve LSTM gibi zamansal yapıların kullanılması, özellikle finansal işlemlerin ardışık doğasını modellemek için daha anlamlı hale gelebilir.

#### 3.7.2. Açıklanabilirlik ve Güvenilirlik

- **Model Açıklanabilirliği (Explainable AI - XAI):** Özellikle finans, sağlık gibi regülasyon gerektiren alanlarda karar verme sürecinin açıklanabilir olması büyük önem taşımaktadır. SHAP, LIME veya Captum gibi açıklayıcı araçların kullanılması, model güvenliğini artırmak ve kullanıcı güvenini sağlamak açısından kritik rol oynar.

- **Güvenlik ve Adversary Dayanıklılığı:** Modellerin bilinçli manipülasyonlara karşı nasıl davranışları araştırılmalı, sahtecilik yapan aktörlerin modeli kandırmaya yönelik girişimlerine karşı savunma mekanizmaları geliştirilmelidir.

### **3.7.3. Veri Çeşitliliği ve Simülasyon**

- **Veri Simülasyonu:** Azınlık sınıf problemi nedeniyle yaşanan dengesizlikler, sahte (sentetik) dolandırıcılık verileri üretilerek dengelenebilir. SMOTE, ADASYN veya GAN tabanlı veri artırma teknikleri bu bağlamda araştırmaya değerdir.
- **Transfer Öğrenme ve Domain Adaptation:** Farklı sektörlerden veya ülkelerden elde edilmiş finansal işlem verilerinin kullanılması, modelin genelleme kabiliyetini test etmek için önemli bir adımdır. Yeni verilerle adaptasyonun sağlanması için domain adaptation teknikleri geliştirilebilir.

### **3.7.4. Gerçek Zamanlı Uygulama ve Online Öğrenme**

- **Online Learning ve Güncellenebilir Sistemler:** Dolandırıcılık tespiti sistemleri, saldırganların davranış biçimleri zamanla değişikçe dinamik olarak güncellenmelidir. Bu doğrultuda, çevrim içi öğrenmeye (online learning) dayalı sistemler kurularak modelin sürekli olarak kendini güncellemesi sağlanabilir.
- **Edge AI Uygulamaları:** Modellerin bulut dışında, doğrudan işlem yapılan noktalarda (ör. POS cihazlarında) çalışması; hız, veri gizliliği ve enerji verimliliği açısından yeni bir araştırma alanı olarak öne çıkmaktadır.

Bu öneriler, çalışmanın mevcut başarısını daha ileri taşımayı amaçladığı gibi, anomali tespiti alanında daha ölçülebilir, güvenilir ve akıllı sistemlerin geliştirilmesine zemin hazırlayacaktır. Özellikle açıklanabilir yapay zeka, gerçek zamanlı öğrenme ve hibrit sistemler, bu alandaki araştırmaların odak noktası olmaya devam etmektedir.

## **3.8. Tartışma ve Literatürle Karşılaştırma**

Bu çalışmada kullanılan LightGBM ve PCA tabanlı yaklaşımlar, sahtekarlık tespiti gibi dengesiz sınıf problemlerinde yüksek başarı sağlamıştır. Özellikle LightGBM'in optimize edilmiş hali, hem doğruluk (%99.95) hem de F1 skoru (%84.15) açısından diğer denetimli ve denetimsiz modellerin önüne geçmiştir. Bu bulgular, mevcut literatürde bildirilen performanslarla kıyaslandığında dikkate değer bir iyileşmeye işaret etmektedir.

Örneğin, Dal Pozzolo et al. (2015) tarafından yapılan bir çalışmada, sahtekarlık tespiti üzerine geliştirilen sınıflandırıcılar genellikle %90'ın altında F1 skoru üretmiş; Random Forest ve Logistic Regression gibi modellerin sınıf dengesizliği karşısında ciddi zaafları olduğu vurgulanmıştır [17]. Benzer şekilde Carcillo et al. (2019), anomali tespitine yönelik modelleri değerlendirmiştir; ancak autoencoder gibi yöntemlerin, özellikle azınlık sınıf üzerinde yüksek hata oranları verdiği göstermiştir [18].

Bu bağlamda LightGBM, boosting temelli yapısı sayesinde karmaşık karar sınırlarını öğrenebilmesi ve sınıf ağırlıklandırması üzerinden azınlık sınıfı baskın hale getirebilmesi nedeniyle daha avantajlıdır. Bu çalışmada uygulanan hiperparametre ayarları da bu avantajı maksimize etmiş görünülmektedir.

Anomali tespitinde yaygın kullanılan yöntemlerden biri olan PCA'nın performansı ise literatürle tutarlıdır. Chandola et al. (2009), PCA'nın düşük boyuta indirgenmiş uzayda normal davranış modelleme yeteneğini vurgulamış; ancak başarımının veri setinin dağılım özelliklerine oldukça bağlı olduğunu belirtmiştir [19]. Bu çalışmada PCA'nın %94.9 AUC başarımı ile güçlü bir taban model sunduğu, ancak F1 skorunda zayıf kaldığı gözlenmiştir. Bu durum, literatürde sıkça dile getirilen “yüksek doğruluk – düşük hassasiyet” çelişkisini de doğrulamaktadır.

Bu değerlendirmeler ışığında, bu çalışmada elde edilen sonuçlar sadece ampirik olarak değil, literatür destekli teorik zemin üzerinde de güçlü görülmektedir. Fakat gelecekteki çalışmalarında istatistiksel testlerle bu farkların anlamlılığı derinleştirilmeli ve çeşitli veri kümeleri üzerinden genellenebilirlik araştırılmalıdır.

### 3.9. Sonuç

Bu çalışma kapsamında dolandırıcılık tespiti problemi hem gözetimli hem de gözetimsiz makine öğrenmesi yaklaşımlarıyla ele alınmış, LightGBM, PCA, Autoencoder, Isolation Forest ve bunların birleşimi olan Ensemble modelleri sistematik olarak değerlendirilmiştir. Yapılan hiperparametre optimizasyonları sonucunda özellikle LightGBM modeli, %99.95 doğruluk, %84.15 F1 skoru ve %97.67 AUC değeri ile tüm metriklerde en üstün performansı göstermiştir. PCA modeli ise düşük F1 skoruna rağmen yüksek AUC ve doğruluk değerleriyle riskli işlemleri ön işaretleme açısından önemli katkı sunmuş; anomali tespitine dayalı sistemlerde etkili bir destek aracı olarak öne çıkmıştır. Ensemble yapı, bu iki modelin avantajlarını birleştirerek hem precision (%94.1) hem F1 (%87.4) açısından en dengeli

çözümü üretmiştir. Ayrıca, SHAP analizi ile yapılan işlem tutarı bazlı değerlendirmelerde, yüksek tutarlı işlemlerin model tarafından daha riskli algılandığı, fraud skoruna katkısının doğrusal ve anlamlı şekilde arttığı ( $r=0.87$ ,  $p<0.001$ ) ortaya konmuştur. Özellikle \$150K üzeri işlemlerde tutarın katkısı %40'ı aşmakta ve merchant ile etkileşimleri toplam riski daha da yukarı çekmektedir. Bu bulgular, açıklanabilir yapay zeka yöntemlerinin sadece model başarımını artırmakla kalmayıp, aynı zamanda kurumlara operasyonel risk analizi konusunda somut içgörüler sunduğunu da göstermektedir. Sonuç olarak, hem teorik düzeyde literatürle tutarlılık sağlayan hem de gerçek dünya uygulamalarında hayatı geçirilebilecek kadar sağlam bir modelleme yapısı geliştirilmiş; özellikle finans gibi yüksek hassasiyet gerektiren alanlarda kullanılabilecek açıklanabilir ve güvenilir bir dolandırıcılık tespit altyapısı oluşturulmuştur.

## KAYNAKLAR

- [1] SUN, Guanglin, et al. Digital finance and corporate financial fraud. International Review of Financial Analysis, 2023, 87: 102566. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1057521923000820> (Erişim tarihi: 23.03.2025)
- [2] GOLD, Steve. The evolution of payment card fraud. Computer Fraud & Security, 2014, 2014.3: 12-17. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1361372314704713> (Erişim tarihi: 23.03.2025)
- [3] RYMAN-TUBB, Nick F.; KRAUSE, Paul; GARN, Wolfgang. How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. Engineering Applications of Artificial Intelligence, 2018, 76: 130-157. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0952197618301520> (Erişim tarihi: 23.03.2025)
- [4] BELLO, O. A., et al. Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. European Journal of Computer Science and Information Technology, 2023, 11.6: 103-126. URL: [https://www.researchgate.net/profile/Oluwabusayo-Bello/publication/381548526\\_Analysing\\_the\\_Impact\\_of\\_Advanced\\_Analytics\\_on\\_Fraud\\_Detection\\_A\\_Machine\\_Learning\\_Perspective/links/66736273d21e220d89c09836/Analysin](https://www.researchgate.net/profile/Oluwabusayo-Bello/publication/381548526_Analysing_the_Impact_of_Advanced_Analytics_on_Fraud_Detection_A_Machine_Learning_Perspective/links/66736273d21e220d89c09836/Analysin)

g-the-Impact-of-Advanced-Analytics-on-Fraud-Detection-A-Machine-Learning-Perspective.pdf (Erişim tarihi: 23.03.2025)

- [5] HUANG, Dongxu, et al. CoDetect: Financial fraud detection with anomaly feature detection. Ieee Access, 2018, 6: 19161-19174. URL: <https://ieeexplore.ieee.org/abstract/document/8325544> (Erişim tarihi: 23.03.2025)
- [6] DU, Haichao, et al. AutoEncoder and LightGBM for credit card fraud detection problems. Symmetry, 2023, 15.4: 870. URL: <https://www.mdpi.com/2073-8994/15/4/870> (Erişim tarihi: 23.03.2025)
- [7] CHERGUI, Hamza, et al. Semi-supervised method to detect fraudulent transactions and identify fraud types while minimizing mounting costs. International journal of advanced computer science and applications (IJACSA), 2023, 14.2. URL: <https://hal.science/hal-04209615/document> (Erişim tarihi: 23.03.2025)
- [8] SADDI, Venkata Ramana, et al. Fighting Insurance Fraud with Hybrid AI/ML Models: Discuss the Potential for Combining Approaches for Improved Insurance Fraud Detection. In: 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216). IEEE, 2023. p. 01-06. URL: <https://ieeexplore.ieee.org/abstract/document/10431155> (Erişim tarihi: 23.03.2025)
- [9] KPMG Türkiye, “Üretken Yapay Zeka ile Finansın Yeni Normali”, KPMG Türkiye, 2024. URL: <https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2024/01/uretken-yapay-zeka-ile-finansin-yeni-normali.pdf> (Erişim tarihi: 22.03.2025)
- [10] Kaggle, “Credit Card Fraud Detection Dataset”, Kaggle, n.d. URL: <https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud> (Erişim tarihi: 22.03.2025)
- [11] BAHNSEN, Alejandro Correa, et al. Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 2016, 51: 134-142. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0957417415008386> (Erişim tarihi: 23.03.2025)
- [12] HASAN, Basna Mohammed Salih; ABDULAZEEZ, Adnan Mohsin. A review of principal component analysis algorithm for dimensionality reduction. *Journal of Soft Computing and Data Mining*, 2021, 2.1: 20-30. URL: <https://publisher.uthm.edu.my/ojs/index.php/jscdm/article/view/8032> (Erişim tarihi: 23.03.2025)

- [13] KE, Guolin, et al. Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems*, 2017, 30. URL: <https://proceedings.neurips.cc/paper/2017/hash/6449f44a102fde848669bdd9eb6b76fa-Abstract.html>
- [14] Türkiye Yapay Zekâ İnisiyatifi (TRAI), “Bankacılıkta Yapay Zekâ ile Dolandırıcılık Tespit”, Türkiye.ai, 2024. URL: <https://turkiye.ai/bankacilikta-yapay-zeka-dolandiricilik-tespiti/> (Erişim tarihi: 22.03.2025)
- [15] ResearchGate, “Credit card fraud detection dataset (PCA ile türetilmiş)”, 2023. URL: [https://www.researchgate.net/figure/Credit-card-fraud-detection-dataset-The-dataset-is-obtained-by-doing-PCA-to-the-Kaggle\\_fig9\\_369404230](https://www.researchgate.net/figure/Credit-card-fraud-detection-dataset-The-dataset-is-obtained-by-doing-PCA-to-the-Kaggle_fig9_369404230) (Erişim tarihi: 22.03.2025)
- [16] MDPI, “LightGBM Decision Tree Yapısı”, Symmetry, 2023. URL: <https://www.mdpi.com/2073-8994/15/4/870> (Erişim tarihi: 22.03.2025)
- [17] Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. *2015 IEEE Symposium Series on Computational Intelligence*, 159–166. <https://doi.org/10.1109/SSCI.2015.33>
- [18] Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences*, 557, 317–331. <https://doi.org/10.1016/j.ins.2019.05.042>
- [19] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, 41(3), 15. <https://doi.org/10.1145/1541880.1541882>