YAPAY ZEKÂ PERSPEKTİFİNDEN SAĞLIK, DUYGU DURUMU VE GÜVENLİK:

Güncel Yaklaşımlar, Uygulamalar ve Araştırmalar

Editör: Prof. Dr. Ayça Çakmak Pehlivanlı



BİDGE Yayınları

BİDGE Yayınları

Yapay Zekâ Perspektifinden Sağlık, Duygu Durumu ve Güvenlik: Güncel Yaklaşımlar, Uygulamalar ve Araştırmalar

Editör: PROF. DR. AYÇA ÇAKMAK PEHLİVANLI

ISBN: 978-625-5474-07-0

1. Baskı
Sayfa Düzeni: Gözde YÜCEL
Yayınlama Tarihi: 2026-10-01
BİDGE Yayınları

Bu eserin bütün hakları saklıdır. Kaynak gösterilerek tanıtım için yapılacak kısa alıntılar dışında yayıncının ve editörün yazılı izni olmaksızın hiçbir yolla çoğaltılamaz.

Sertifika No: 71374
Yayın hakları © BİDGE Yayınları
www.bidgeyayinlari.com.tr - bidgeyayinlari@gmail.com
Krc Bilişim Ticaret ve Organizasyon Ltd. Şti.
Güzeltepe Mahallesi Abidin Daver Sokak Sefer Apartmanı No: 7/9 Çankaya / Ankara

İÇİNDEKİLER

METİNDEN MELODİYE YAPAY ZEKÂ İLE DUYGU TABANLI MÜZİK SEÇİMİ 1

FATMA ÖZDEMİR, FAHRİYE GEMCİ

AĞ TRAFİĞİNDEN TEHDİDE, TEHDİTTEN TESPİTE: YAPAY ZEKÂ DESTEKLİ SİBER SALDIRI TESPİT SİSTEMİ 23

NEFİSE TURGUT, KEVSER ELİŞEN, FAHRİYE GEMCİ

KALP VERİSİNDEN KALP SAĞLIĞINA: MAKİNE ÖĞRENMESİ İLE KALP KRİZİ RİSK TAHMİNİ 48

FAHRİYE GEMCİ, TURGAY IBRIKCI

BÖLÜM 1

METİNDEN MELODİYE YAPAY ZEKÂ İLE DUYGU TABANLI MÜZİK SEÇİMİ

FATMA ÖZDEMİR[1]
FAHRİYE GEMCİ[2]

Giriş

Dijital çağda insan-bilgisayar etkileşimi, standart komut yapılarından sıyrılarak kullanıcının anlık psikolojik durumunu anlayan ve buna göre şekillenen akıllı sistemlere evrilmiştir. Bireylerin günlük olarak paylaştığı yapılandırılmamış metinsel ifadeler, anlık hislerine dair derin anlamsal ipuçları barındırır. Doğal Dil İşleme (NLP) alanında uzun yıllar kullanılan geleneksel istatistiksel modeller, dilin mecaz ve karmaşık bağlam ilişkilerini yakalamakta yetersiz kalmıştır. Bu durum, doğrudan insan psikolojisiyle bağdaşan ve duygu durumlarından en çok etkilenen müzik gibi içeriklerin, yapay zekâ destekli analiz motorlarıyla doğru şekilde eşleştirilmesini kısıtlayan en büyük engellerden biri olmuştur.

[1]Mezun Öğrenci, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0009-0004-2979-4497
[2]Dr. Öğr. Üyesi, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0000-0003-0961-5266

Derin öğrenme literatüründe devrim yaratan Transformer mimarileri ve öz-dikkat (self-attention) mekanizmaları, metinlerdeki çift yönlü bağlamsal ilişkileri yüksek doğruluğa sahip olacak biçimde çözerek bu kısıtlamaları ortadan kaldırmıştır. Gelişmiş dil modellerinin sunduğu bu anlamsal çıkarım gücü, yazılım sistemlerinin kullanıcılarla empatik bir bağ kurmasına olanak tanımaktadır. Bu çalışmada; kullanıcıların serbest metin ifadelerinden anlık duygu durumlarını çok sınıflı olarak sınıflandıran ve elde edilen psikolojik çıktıya uygun olarak gerçek zamanlı video ve müzik önerileri sunan uçtan uca web tabanlı Sentify AI sistemi geliştirilmiştir. Proje kapsamında, hem klasik makine öğrenmesi yaklaşımları hem de BERT, ALBERT, RoBERTa ve DistilBERT gibi modern derin öğrenme mimarileri aynı veri kümesi üzerinde kapsamlı deneysel süreçlere tabi tutulmuştur.

Bu çalışma, metin tabanlı duygu analizi yaklaşımlarını uçtan uca çalışan bir yazılım mimarisiyle birleştirmiştir. Çalışma sonuçları, BERT ve RoBERTa gibi yüksek doğruluk sağlayan modellerin gerçek zamanlı uygulamalarda yüksek hesaplama maliyeti oluşturduğunu; buna karşılık DistilBERT'in doğruluk, hesaplama maliyeti ve ölçeklenebilirlik arasında daha dengeli bir çözüm sunduğunu göstermektedir.

Literatür Taraması

Visutsak ve çalışma arkadaşları (2025), dijital müzik platformlarında kullanıcı deneyimini artırmak ve yerel müzik endüstrisini desteklemek amacıyla, kullanıcıların anlık ruh hallerini ifade eden metin girdileri ile şarkı sözlerini doğal dil işleme (NLP) ve makine öğrenmesi teknikleriyle analiz eden duygu tabanlı bir platform geliştirmişlerdir. Şarkı sözü ve kullanıcı girdilerini aşk, mutluluk, üzüntü ve öfke olmak üzere dört temel duygu sınıfına ayıran bu araştırmada farklı sınıflandırıcılar yarıştırılmış ve Rastgele Orman (Random Forest) algoritması 0.94 doğruluk oranı elde

ederek; XGBoost (0.89), Karar Ağacı (0.85), Lojistik Regresyon (0.79) ve Destek Vektör Makineleri (SVM) (0.78) modellerini geride bırakıp en yüksek sınıflandırma başarısını sergilemiştir (Visutsak et al., 2025).

Perera (2021), modern yaşamın getirdiği stres ve depresif durumlarla başa çıkmak isteyen bireylerin anlık hislerini sosyal ağlarda paylaşma eğilimlerinden yola çıkarak, kullanıcıların sosyal medya içeriklerini NLP teknikleriyle analiz etmişlerdir. Araştırmacılar, şarkı sözlerinin anlamsal boyutunu ön planda tutarak elde edilen kullanıcı duygu durumunu şarkıların lirik analizleriyle İngilizce ve Sinhala dillerini kapsayacak şekilde eşleştirmiş; söz dizimlerindeki anlamsal farklılıklar nedeniyle lirikleri pozitif ve nötr olarak kategorize edip dilden bağımsız bir müzik öneri hattı tasarlamışlardır (Perera, 2021).

Sarakit (2015) tarafından yürütülen çalışmada, çevrimiçi kaynaklara değer katmak amacıyla YouTube müzik videoları altındaki kullanıcı yorumları birer kolektif zekâ kaynağı olarak ele alınmış ve metin tabanlı duygu analizi gerçekleştirilmiştir. Çok terimli Naive Bayes (MNB), Karar Ağacı ve SVM algoritmalarının test edildiği çalışmada, mutluluk ve üzüntü sınıflarının baskın olmasından kaynaklanan sınıf dengesizliği (class imbalance) problemini aşmak adına SMOTE algoritması uygulanmış ve bu ön işleme adımı sayesinde SVM sınıflandırıcısının duygu tanıma başarısı %75.68'den %89.44'e yükseltilmiştir (Sarakit, 2015).

Samrat ve çalışma arkadaşları (2023), dijital müzik akış hizmetlerindeki kullanıcı deneyimlerini ve geri bildirimlerini anlamlandırmak amacıyla, Spotify uygulamasına ait kullanıcı yorumlarından oluşan bir veri kümesi üzerinde derin öğrenme mimarilerini kıyaslamışlardır. Büyük ölçekli dil modellerinin informal ifadeleri yakalama yeteneği ile ardışık bilgileri işlemedeki gücünün incelendiği araştırmada; zaman serisi niteliğindeki metin verilerini işlemede daha başarılı olan Geçitli Yinelemeli Birim

(GRU) %77.32 doğruluk ve LSTM %77.21 doğruluk oranlarına ulaşarak, transformatör tabanlı ELECTRA (%72.03) modeline kıyasla daha yüksek bir başarım sergilemişlerdir (Samrat et al., 2023).

Richard ve çalışma arkadaşları (2025) tarafından önerilen "Vivify" adlı çerçevede, edebiyat ve müzik unsurları bir araya getirilerek okuyucunun metinle daha derin bir bağ kurmasını sağlayan bağlama uygun bir arka plan müziği öneri sistemi kurgulanmıştır. Metin tabanlı duygu tanıma aşamasında transformatör tabanlı RoBERTa modeli kullanılırken, müziklerin duygu analizinde Uzun Kısa Süreli Bellek (LSTM) mimarisinden yararlanılmıştır. Geleneksel yaklaşımların aksine duyguları sadece kategorik sınıflarla sınırlamayıp sürekli (continuous) bir boyutta ele alan bu hibrid sistem, metin ve müzik arasındaki duygusal uyumu Kosinüs Benzerliği (Cosine Similarity) algoritmasıyla hesaplayarak kararlı ve dil bağımsız bir müzik eşleştirmesi gerçekleştirmektedir (Richard et al., 2025).

Xiao ve Luo (2024) tarafından yapılan çalışmada ise, kısa metinlerin kısıtlı anlamsal özellikler içermesi nedeniyle duygu analizinde yaşanan kararlılık ve doğruluk problemlerini aşmak amacıyla Transformer ve BERT modellerini birleştiren hibrid bir büyük dil yapısı mimarisi önerilmiştir. Geliştirilen yöntemde, kelime vektörlerini çıkarmak için öncelikle BERT yapısı kullanılmış ve metinsel ifade yeteneğini artırmak adına bu vektörler konu vektörleri (topic vectors) ile birleştirilmiştir. Elde edilen birleşik vektörler, bağlamsal özellikleri öğrenmesi için Çift Yönlü Geçitli Yinelemeli Birim (Bi-GRU) yapısına aktarılmış ve ardından duygu kutuplarını Softmax katmanı üzerinden yüksek doğrulukla sınıflandırmak üzere Bi-GRU mimarisinin arkasına entegre edilen bir Transformer katmanıyla model optimize edilmiştir (Xiao & Luo, 2024).

Akuma ve çalışma arkadaşları (2021) tarafından yapılan çalışmada, bireylerin duygu durumlarını akrabaları veya çevreleriyle

paylaşmak yerine Twitter (X) gibi sosyal medya platformlarında metinler ve emojiler aracılığıyla ifade etme eğilimlerinden yararlanan dinamik bir müzik öneri sistemi geliştirilmiştir. Kullanıcıların anlık canlı tweet verilerinin çekilerek analiz edildiği araştırmada; mutlu, korku, öfkeli, iğrenmiş ve üzgün olmak üzere beş temel duygu durumu hedeflenmiştir. Sosyal medya içeriklerindeki hem ham metin girdilerini hem de emojileri önceden tanımlanmış duygu değişkenleriyle ve anahtar kelime eşleştirme mantığıyla analiz eden bu sistem, elde edilen anlık duygu tahminleme sonuçlarını doğrudan kullanıcının ruh haline hitap eden müzik listeleriyle eşleştirerek sosyal medya tabanlı ve gerçek zamanlı bir öneri mimarisi sunmuştur (Akuma et al., 2021).

Gardazi ve çalışma arkadaşları (2025) tarafından yürütülen çalışmada, çift yönlü transformatör bloklarından oluşan BERT mimarisinin ve varyantlarının doğal dil işleme (NLP) alanındaki uygulamaları geniş kapsamlı bir literatür incelemesiyle değerlendirilmiştir. Araştırmada; söz dizimsel ve semantik özellikleri üstün bir başarıyla modelleyen BERT'in cümle sınır tespiti, kelime bölütleme, morfolojik etiketleme (POS), soru-cevap sistemleri (QAS) ve makine çevirisi gibi geleneksel NLP adımlarında statik kelime gömmelerine (Word2Vec, GloVe) kıyasla sergilediği başarım artışları incelenmiştir. Model boyutu ve bellek kısıtları nedeniyle ortaya çıkan hesaplama maliyetlerini azaltmak amacıyla literatürde geliştirilen ALBERT, DistilBERT ve RoBERTa gibi sıkıştırılmış veya optimize edilmiş varyantların mimari yapıları ve parametre paylaşımlı parametrik özellikleri karşılaştırmalı olarak analiz edilmiştir (Gardazi et al., 2025).

Materyal ve Metot

Bu çalışmada, kullanıcıların anlık ruh hallerini ifade ettikleri metinlerden duygu analizi yapan ve elde edilen sonuçlara göre kişiselleştirilmiş müzik önerileri sunan web tabanlı bir sistem

(Sentify AI) geliştirilmiştir. Sistem; veri kümesi, derin öğrenme tabanlı doğal dil işleme (NLP) modeli, web uygulama iskeleti ve üçüncü taraf API entegrasyonları olmak üzere dört temel bileşenden oluşmaktadır.

Veri Kümesi ve Veri Ön İşleme

Çalışmada, metin tabanlı duygu sınıflandırması amacıyla literatürde yaygın olarak kullanılan "emotions.csv" veri kümesi referans alınmıştır. Veri kümesi toplam 16.000 satırdan oluşmakta ve metin içerikleri ile bunlara ait duygu etiketlerini barındırmaktadır. Veri seti; sadness (hüzün), anger (öfke), love (sevgi), joy (mutluluk), fear (korku) ve surprise (şaşkınlık) olmak üzere 6 temel duygu sınıfına ayrılmıştır.

Duygu analizi modelinin eğitimi öncesinde veri kümesi rastgele %80 eğitim ve %20 test olmak üzere ikiye bölünmüştür. Metin verilerini sayısal özniteliklere dönüştürmek amacıyla TF-IDF (Term Frequency-Inverse Document Frequency) vektörleştirme yöntemi kullanılmış, kelime gürültüsünü azaltmak amacıyla İngilizce durak kelimeler (stop words) filtrelenmiştir.

Geliştirilen Modeller ve Duygu Analizi

Çalışma kapsamında, metin tabanlı duygu sınıflandırma performansını karşılaştırmalı olarak değerlendirmek amacıyla geleneksel bir makine öğrenmesi modeli ile Transformer tabanlı dört farklı derin öğrenme mimarisi kullanılmıştır:

- Lojistik Regresyon (Baseline Model): Kelime özniteliklerinin frekans vektörleri (TF-IDF) kullanılarak eğitilmiştir. Bu model, derin öğrenme yaklaşımlarının sağladığı başarı artışını ölçmek amacıyla temel kıyaslama noktası olarak konumlandırılmıştır.
- BERT (Bidirectional Encoder Representations from Transformers): Metinlerdeki kelimelerin hem sağ hem de sol

bağlamını aynı anda işleyebilen çift yönlü derin transformatör mimarisine sahiptir. Çalışmada önceden eğitilmiş bert-base-uncased modeli kullanılarak veri kümesi üzerinde ince ayar (fine-tuning) gerçekleştirilmiştir.

- DistilBERT: BERT mimarisinin bilgi damıtma (knowledge distillation) tekniği kullanılarak küçültülmüş, daha hafif ve hızlı bir versiyonudur. BERT'e göre %40 daha az parametreye sahip olmasına rağmen, hesaplama maliyetini düşürerek benzer bir sınıflandırma başarımı göstermesi hedeflenmiştir.
- ALBERT (A Lite BERT): BERT mimarisindeki parametre sayısını azaltmak için tasarlanmış, çapraz katmanlı parametre paylaşımı (cross-layer parameter sharing) ve parçalanmış katıştırma parametreleştirmesi (factorized embedding parameterization) tekniklerini kullanan sıkıştırılmış bir modeldir. Bellek verimliliğini ölçmek amacıyla mimariye dahil edilmiştir.
- RoBERTa (Robustly Optimized BERT Approach): BERT modelinin hiperparametre optimizasyonları, daha büyük batch boyutları, dinamik maskeleme (dynamic masking) tekniği ve daha uzun süreli eğitim stratejileriyle geliştirilmiş hiper-optimize edilmiş versiyonudur. Modelin daha karmaşık dil kalıplarını öğrenme yeteneği bu çalışmada test edilmiştir.

Derin öğrenme modellerinin tamamı Hugging Face transformers kütüphanesi kullanılarak PyTorch çatısı altında eğitilmiştir. Eğitim süreçlerinde aşırı öğrenmeyi (overfitting) engellemek adına dinamik doğrulama adımları izlenmiş; optimizasyon yöntemi olarak AdamW tercih edilmiş ve öğrenme oranı (learning rate) 2e-5 olarak belirlenmiştir.

Sistem Mimarisi ve Web Uygulaması (Sentify AI)

Geliştirilen duygu analizi modelini son kullanıcıya sunmak amacıyla Flask framework kullanılarak istemci-sunucu mimarisine dayalı bir web uygulaması tasarlanmıştır.

- Veritabanı ve Güvenlik: Kullanıcı yönetimi, kayıt ve oturum açma işlemleri için Flask-Login ve Flask-SQLAlchemy kütüphaneleri kullanılmış; kullanıcı şifreleri Werkzeug kütüphanesi vasıtasıyla güvenli bir şekilde karma (hash) yöntemiyle veritabanında (SQLite) saklanmıştır. Kullanıcıların beğendikleri müzikleri profillerinde saklayabilmesi amacıyla bire-çok (one-to-many) ilişkisel veritabanı modelleri (User ve Favorite) tanımlanmıştır.
- Arayüz Tasarımı: Kullanıcı arayüzü, HTML5, CSS3 ve asenkron JavaScript (Fetch API) teknolojileri kullanılarak dinamik bir yapıda geliştirilmiştir.

Çok Dilli Destek ve Müzik Önerim Algoritması

Sistemin çalışma mantığı ve API entegrasyon süreçleri şu şekildedir:

- Çok Dilli Metin Çevirisi: Kullanıcı tarafından arayüze girilen herhangi bir dildeki metin, deep-translator kütüphanesi (Google Translator API) aracılığıyla otomatik olarak İngilizceye çevrilmektedir. Böylece modelin dil bağımlılığı ortadan kaldırılmıştır.
- Tahmin ve API Entegrasyonu: Çevrilen metin PyTorch tabanlı çalışan DistilBERT modeline (DistilBertForSequenceClassification) beslenerek Softmax fonksiyonu aracılığıyla en yüksek olasılığa sahip ilk iki duygu etiketi tespit edilmektedir.
- YouTube API Sorgusu: Tespit edilen birincil baskın duyguya göre, önceden yapılandırılmış ruh hali kütüphanesinden pop,

caz, lofi veya klasik müzik türlerinde dinamik arama sorguları oluşturulmaktadır. Bu sorgular YouTube Data API v3 kütüphanesine gönderilerek; müzik kategorisi filtrelemesi, siteler arası oynatılabilirlik ve güvenli arama kriterlerine göre tam olarak 12 adet ilgili video çekilerek arayüzde asenkron olarak listelenmektedir.

Deneysel Çalışmalar

Bu bölümde, duygu analizi amacıyla eğitilen geleneksel makine öğrenmesi modeli (Lojistik Regresyon) ile derin öğrenme tabanlı transformer mimarilerinin (BERT, DistilBERT, ALBERT, RoBERTa) test veri kümesi üzerindeki performans sonuçları sunulmuştur. Modellerin başarımı; Doğruluk (Accuracy), Kesinlik (Precision), Duyarlılık (Recall) ve F1-Skoru (F1-Score) metrikleri kullanılarak karşılaştırmalı olarak analiz edilmiştir.

Performans Değerlendirme Metrikleri

Modellerin sınıflandırma başarımlarını ve tahmin kalitelerini tek bir boyuttan değil, çok yönlü olarak analiz edebilmek amacıyla literatürde kabul görmüş dört temel metrik esas alınmıştır:

- Doğruluk (Accuracy): Sistem tarafından yapılan doğru tahminlerin toplam veri sayısına oranını ifade eder. Genel bir başarı göstergesi olmakla birlikte, sınıfların dengesiz dağıldığı veri kümelerinde tek başına yanıltıcı olabilmektedir.
- Kesinlik (Precision): Modelin bir sınıf için yaptığı pozitif (örneğin "mutluluk" veya "öfke") tahminlerin ne kadarının gerçekten doğru olduğunu gösterir. Yani, modelin yaptığı tahminlerin isabet oranını veya temizliğini ölçer. Kesinliğin yüksek olması, yanlış pozitif (false positive) tahminlerin az olduğunu gösterir.

- Duyarlılık (Recall): Gerçekte o sınıfa ait olan verilerin (örneğin veri setindeki tüm gerçek "hüzün" metinlerinin) model tarafından ne kadarının doğru yakalanabildiğini ifade eder. Modelin ilgili sınıfı bulma veya kaçırmama kapasitesini ölçer. Duyarlılığın yüksek olması, yanlış negatif (false negative) tahminlerin azaldığı anlamına gelir.
- F1-Skoru (F1-Score): Kesinlik (Precision) ve Duyarlılık (Recall) metriklerinin harmonik ortalamasıdır. Özellikle sınıflar arasında dengesizlik olduğunda veya hem yanlış pozitiflerin hem de yanlış negatiflerin maliyetinin yüksek olduğu duygu analizi gibi görevlerde modelin genel kararlılığını gösteren en güvenilir metriktir.

Model Performans Sonuçları

Tablo 1. Kullanılan Modellerin Metrik Sonuçları

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	0.8484	0.8642	0.7399	0.7823
BERT(5 epoch)	0.9321	0.9136	0.8908	0.8993
BERT(10 epoch)	0.9281	0.8882	0.8944	0.8912
BERT(15 epoch)	0.9256	0.8905	0.8863	0.8874
ALBERT(5 epoch)	0.9359	0.9179	0.8826	0.8971
ALBERT(10 epoch)	0.9215	0.8828	0.9039	0.8918
ALBERT(15 epoch-EarlyStopping)	0.9300	0.9022	0.8889	0.8942
RoBERTa (5 epoch)	0.9325	0.9322	0.9325	0.9322

RoBERTa (10 epoch-EarlyStopping)	0.9293	0.9326	0.9293	0.9302
RoBERTa (15 epoch-EarlyStopping)	0.9334	0.9352	0.9334	0.9339
DistilBERT (5 epoch)	0.9337	0.9337	0.9337	0.9336
DistilBERT (10 epoch)	0.9334	0.9350	0.9334	0.9338
DistilBERT (15 epoch-EarlyStopping)	0.9371	0.9378	0.9371	0.9372

Elde edilen bulgulara göre:

- ***Geleneksel vs. Derin Öğrenme:*** Temel model olarak ele alınan Lojistik Regresyon, %84.84 doğruluk ve %78.23 F1-skoru ile en düşük performansı sergilemiştir. Transformer tabanlı derin öğrenme modellerinin tamamı ise, geleneksel yöntemi belirgin bir farkla geride bırakmıştır.
- ***En Başarılı Model:*** Genel performans değerlendirildiğinde, DistilBERT (15 epoch - EarlyStopping) modeli %93.71 doğruluk ve %93.72 F1-skoru ile en yüksek başarıyı elde eden model olmuştur. Onu çok yakın değerlerle RoBERTa ve ALBERT modelleri takip etmektedir.
- ***Epoch ve Erken Durdurma (EarlyStopping) Etkisi:*** BERT ve ALBERT modellerinde epoch sayısı 5'ten 10 ve 15'e çıkarıldığında performansta hafif bir düşüş gözlemlenmiştir. Ancak EarlyStopping (Erken Durdurma) mekanizmasının kullanıldığı DistilBERT ve RoBERTa varyasyonlarında, modelin aşırı öğrenmesi engellenmiş ve optimal performansa ulaşılmıştır.
- Model Verimliliği: DistilBERT'in, BERT'e kıyasla daha hafif ve parametre açısından daha küçük bir mimariye sahip

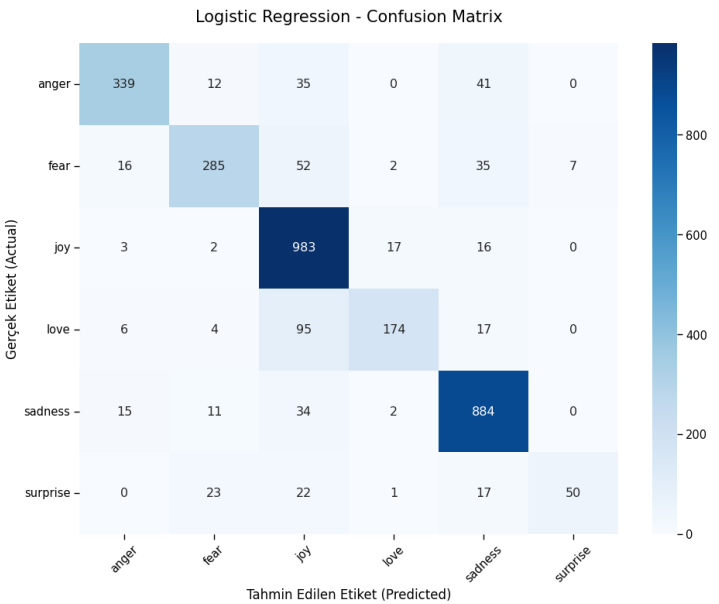
olmasına rağmen hem daha yüksek hem de daha dengeli (Precision ve Recall dengesi) sonuçlar vermesi dikkat çekicidir.

Modellerin Hata Matrisi (Confusion Matrix)

Modellerin genel doğruluk oranları yüksek olsa da, sınıflar arasındaki anlamsal geçişkenlikleri ve modelin spesifik olarak hangi duygularda yanılgıya düştüğünü tespit etmek amacıyla hata matrisleri (confusion matrix) analiz edilmiştir.

Derin öğrenme modellerinin sağladığı başarım artışını daha net görebilmek ve geleneksel yöntemlerin zayıf yönlerini saptamak amacıyla Lojistik Regresyon modelinin hata matrisi analiz edilmiştir. Test veri kümesi üzerinde elde edilen normalize edilmiş hata matrisi Şekil 1'de gösterilmektedir.

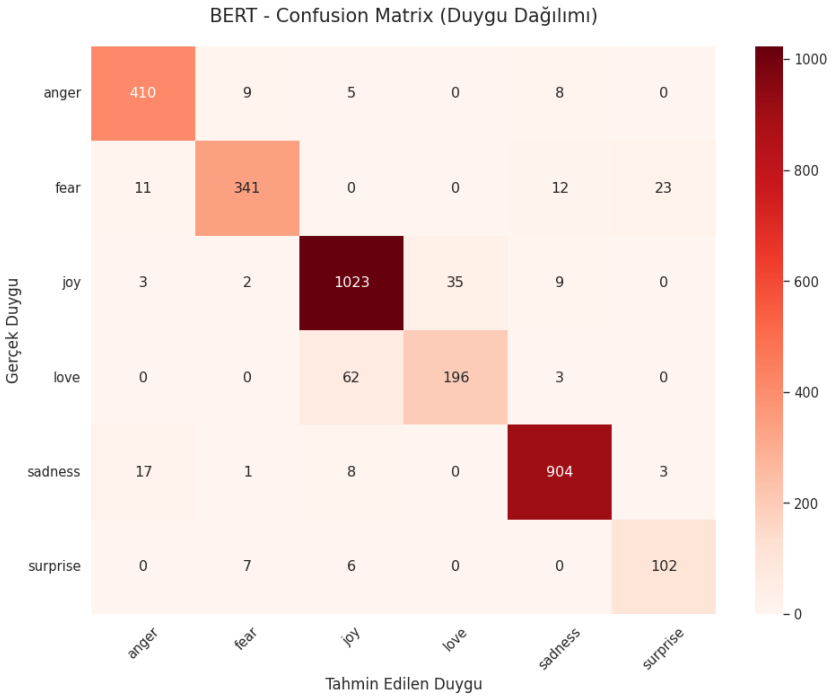
Şekil 1. Logistic Regression Hata Matrisi



Matris satır bazlı analiz edildiğinde şu temel bulgulara ulaşılmıştır:

- **En Başarılı Sınıflandırma (Sadness):** Lojistik Regresyon modeli, en yüksek doğruluğu %93 oranla hüzün (sadness) sınıfında yakalamıştır. Model, hüzün içeren metinlerdeki belirgin anahtar kelimeleri başarıyla ayırt edebilmektedir.
- **Makul Başarıma Sahip Sınıflar** (Joy ve Fear): Model, mutluluk (joy) sınıfını %87, korku (fear) sınıfını ise %83 oranında doğru tahmin ederek genel ortalamaya yakın bir performans sergilemiştir.
- **Modelin En Çok Zorlandığı Sınıflar (Surprise ve Love):** Geleneksel modelin en zayıf kaldığı sınıflar %51 doğru tahmin oranıyla şaşkınlık (surprise) ve %58 oranıyla sevgi (love) olmuştur. Şaşkınlık (surprise) içeren cümlelerin %24 gibi yüksek bir oranı model tarafından korku (fear) olarak, %13'ü ise mutluluk (joy) olarak yanlış sınıflandırılmıştır. Benzer şekilde, sevgi (love) sınıfındaki verilerin %26'sı model tarafından mutluluk (joy) sınıfıyla karıştırılmıştır.
- **Öfke (Anger) Sınıfı Geçişkenliği:** Öfke (anger) sınıfı %79 oranında doğru bilinirken, bu sınıfa ait verilerin %11'i hüzün (sadness) sınıfına hatalı olarak atanmıştır.

Şekil 2. BERT Modelinin Hata Matrisi

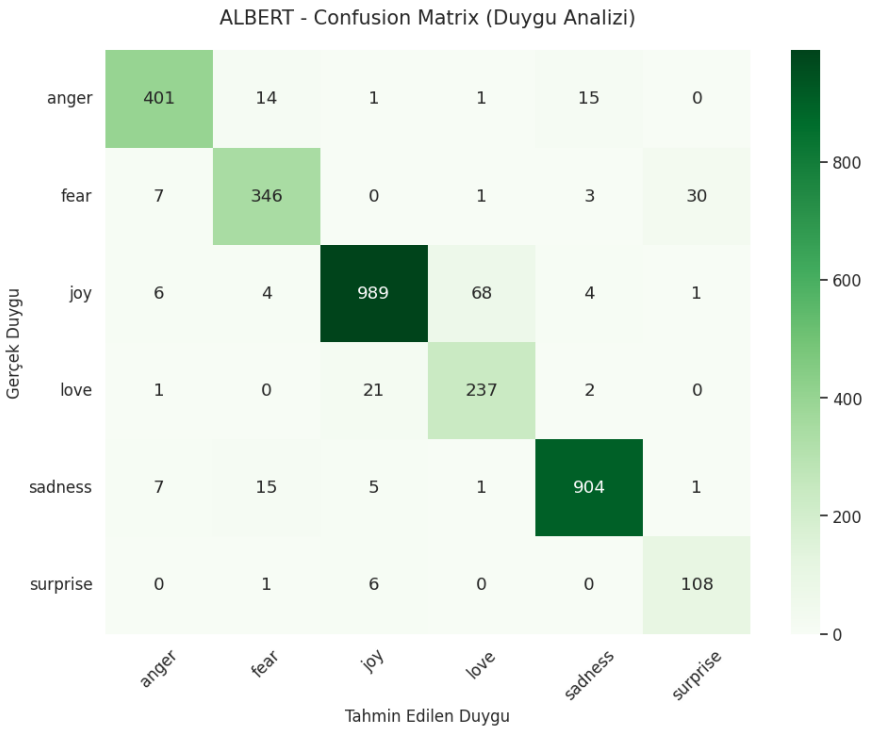


BERT modelinin duygu sınıflandırma performansını detaylı incelemek amacıyla elde edilen hata matrisi Şekil 2'de sunulmuştur. Matris genel olarak incelendiğinde, modelin köşegen hat üzerinde yüksek değerlere ulaştığı ve sınıfları büyük oranda doğru tahmin ettiği görülmektedir.

Özellikle "joy" (mutluluk) ve "sadness" (üzüntü) duygularında model oldukça yüksek bir ayırt edicilik sergilemiştir; "joy" sınıfına ait 1023, "sadness" sınıfına ait ise 904 örnek doğru sınıflandırılmıştır. Buna karşın, modelin en belirgin yanılgısı "love" (aşk/sevgi) ve "joy" sınıfları arasında gerçekleşmiştir. Gerçekte "love" olan 62 örnek model tarafından "joy" olarak tahmin edilmiştir. Benzer şekilde, gerçekte "joy" olan 35 örnek de "love" sınıfına atanmıştır. Bu durum, anlamsal olarak birbirine yakın olan

bu iki duygu arasındaki sınırların model tarafından netleştirilmesinde zorluk yaşandığını göstermektedir. Ayrıca, "fear" (korku) sınıfındaki 23 örneğin "surprise" (şaşkınlık) olarak yanlış tahmin edilmesi de dikkat çeken bir diğer karıştırılma eğilimidir.

Şekil 3. ALBERT Modelinin Hata Matrisi



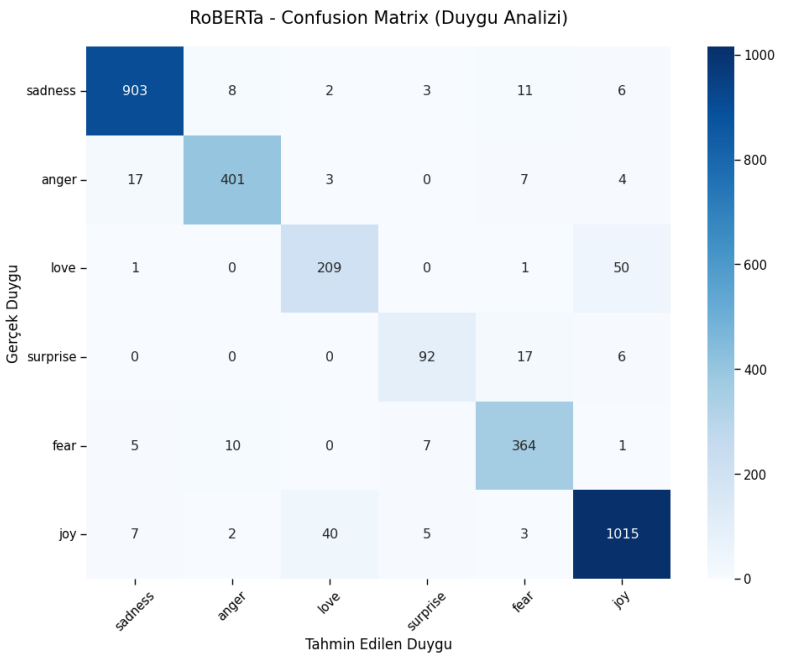
ALBERT modelinin duygu analizi performansını değerlendirmek üzere elde edilen hata matrisi Şekil 3'te paylaşılmıştır. Köşegen hat üzerindeki yoğunluk incelendiğinde, ALBERT modelinin genel olarak kararlı ve yüksek doğrulukta tahminler ürettiği görülmektedir.

Modelin en başarılı olduğu kategoriler sırasıyla 989 doğru tahminle "joy" (mutluluk) ve 904 doğru tahminle "sadness" (üzüntü)

olmuştur. Öte yandan, modelin yaptığı hatalar incelendiğinde özellikle iki belirgin yanılgı öne çıkmaktadır.

İlk olarak, gerçekte "joy" sınıfına ait olan 68 örnek model tarafından "love" (aşk/sevgi) olarak sınıflandırılmıştır. İkinci dikkat çeken hata ise "fear" (korku) sınıfında yaşanmıştır; gerçek değeri "fear" olan 30 örnek model tarafından "surprise" (şaşkınlık) olarak yanlış tahmin edilmiştir. Bu durum, ALBERT mimarisinin de benzer anlamsal bağlamlara ve tetikleyici kelimelere sahip duygu çiftlerini ayırt etmekte (joy-love ve fear-surprise) zorlandığına işaret etmektedir.

Şekil 4. RoBERTa Modelinin Hata Matrisi

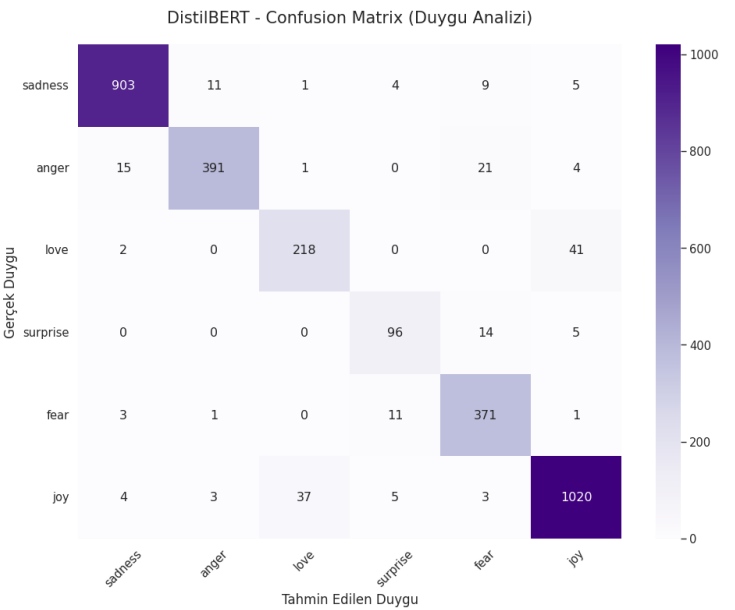


RoBERTa modelinin duygu sınıflandırma görevindeki performansına ilişkin hata matrisi Şekil 4'te verilmiştir. Matrisin

köşegen (diagonal) hattı üzerinde gözlemlenen yüksek değerler, modelin genel olarak sınıfları ayırt etmede oldukça başarılı bir grafik çizdiğini göstermektedir.

Model, özellikle "joy" (mutluluk) sınıfında 1015 ve "sadness" (üzüntü) sınıfında 903 doğru tahmin sayısı ile oldukça güçlü bir ayırt edici kapasite sergilemiştir. Buna karşın, modelin en çok zorlandığı ve hataya düştüğü alan anlamsal olarak birbirine yakın olan "love" (aşk/sevgi) ve "joy" duyguları olmuştur. Gerçek değeri "love" olan 50 örnek model tarafından "joy" olarak tahmin edilirken; benzer şekilde gerçekte "joy" olan 40 örnek de model tarafından "love" sınıfına atanmıştır. Bir diğer dikkat çeken karıştırma eğilimi ise "surprise" (şaşkınlık) sınıfında yaşanmış; gerçekte "surprise" olan 17 örnek model tarafından "fear" (korku) olarak etiketlenmiştir.

Şekil 5. DistilBERT Modelinin Hata Matrisi



Bilgi damıtma (knowledge distillation) yöntemiyle optimize edilen DistilBERT modeline ait duygu sınıflandırma hata matrisi Şekil 5'te sunulmuştur. Matris genel hatlarıyla incelendiğinde, daha az parametreye sahip olmasına rağmen DistilBERT'in sınıfları ayırt etmede yüksek bir başarım sergilediği ve doğru tahminlerin ana köşegen üzerinde yoğunlaştığı görülmektedir.

Model, en yüksek ayırt ediciliği 1020 doğru tahmin ile "joy" (mutluluk) ve 903 doğru tahmin ile "sadness" (üzüntü) sınıflarında yakalamıştır. Modelin en belirgin sınıflandırma yanılgıları incelendiğinde, diğer BERT tabanlı mimarilere benzer şekilde "love" (aşk/sevgi) ve "joy" duyguları arasında bir geçişkenlik olduğu saptanmıştır. Gerçek değeri "love" olan 41 örnek model tarafından "joy" olarak; gerçek değeri "joy" olan 37 örnek ise "love" olarak yanlış tahmin edilmiştir. Ek olarak, gerçekte "anger" (öfke) sınıfına ait olan 21 örneğin "fear" (korku) olarak sınıflandırılması, modelin negatif yönelimli bazı ifadeleri karıştırma eğiliminde olduğunu göstermektedir.

Duygu analizi görevinde test edilen dört farklı transformer mimarisi (BERT, ALBERT, RoBERTa, DistilBERT) hata matrisleri üzerinden kıyaslandığında; RoBERTa modelinin sınıflar genelinde en dengeli ve kararlı performansı sergilediği saptanmıştır. Özellikle tahmin edilmesi daha güç olan ve veri setinde azınlıkta kalan 'fear' (364 doğru) ve 'love' (209 doğru) sınıflarında RoBERTa, baseline BERT modeline kıyasla daha yüksek bir ayırt edicilik sunmuştur. BERT ve DistilBERT modelleri 'joy' sınıfında yüksek doğru tahmin sayılarına ulaşsa da, bu durumun veri setindeki sınıf dengesizliğinden kaynaklandığı ve RoBERTa'nın genel duygu dağılımını modellemede daha başarılı bir genelleme yeteneğine sahip olduğu görülmüştür.

Sonuç ve Tartışma

Bu çalışmada elde edilen bulgular, metin tabanlı duygu analizi görevlerinde derin öğrenme modellerinin geleneksel makine öğrenmesi yaklaşımlarına karşı belirgin bir üstünlük sağladığını ortaya koymuştur. Lojistik Regresyon modelinin %84.84 oranındaki doğruluk başarısı küçümsenemeyecek bir seviyede olsa da, hata matrisi incelendiğinde kelimeleri bağımsız öznitelikler (TF-IDF) olarak ele almasının yarattığı kısıtlar net bir şekilde görülmektedir. Geleneksel model, özellikle anlamsal olarak birbirine yakın veya örtüşen kelime grupları içeren surprise (şaşkınlık) ve love (sevgi) gibi sınıflarda yüksek hata oranlarına ulaşmıştır. Şaşkınlık ifadelerinin %24'ünün korku olarak sınıflandırılması, dildeki bağlamsal derinliğin sadece kelime frekanslarıyla çözülemeyeceğinin bir göstergesidir.

Transformer tabanlı modeller (BERT, DistilBERT, ALBERT ve RoBERTa) ise, metindeki kelimelerin çift yönlü ilişkilerini ve cümle içi konumlarını (attention mekanizması) hesaba katarak bu dilbilimsel karmaşıklıkları büyük ölçüde aşmıştır. BERT ve RoBERTa modelleri, özellikle nüanslar içeren karmaşık duygu durumlarında en kararlı performansı sunmuştur. Parametre paylaşımıyla bellek tasarrufu sunan ALBERT modeli ise, kaynak kısıtlı ortamlar için kabul edilebilir bir alternatif olduğunu kanıtlamıştır.

Projenin özgün ve pratik değerini oluşturan "Sentify AI" web uygulaması entegrasyonunda ise bir optimizasyon problemiyle karşılaşılmıştır. Canlı bir web uygulamasında kullanıcının duygu analizi sonucunu ve buna bağlı müzik önerisini anlık olarak (gecikmesiz) alabilmesi en kritik kullanıcı deneyimi (UX) parametresidir. BERT ve RoBERTa modelleri yüksek doğruluk sunmalarına rağmen, yüksek hesaplama maliyetleri ve uzun tahmin süreleri (inference time) nedeniyle canlı sistemler için gecikme

(latency) riski taşımaktadır. Bilgi damıtma (knowledge distillation) yöntemiyle eğitilen DistilBERT, BERT modelinin performansını neredeyse tamamen korurken, yaklaşık 2 kat daha hızlı tahminleme yapabilmesiyle öne çıkmıştır. Bu durum, akademik başarım ile endüstriyel ölçeklenebilirlik arasındaki ideal dengenin DistilBERT ile kurulabileceğini göstermiştir.

Ayrıca sistemin, deep-translator kütüphanesi vasıtasıyla gelen metinleri dinamik olarak İngilizceye çevirmesi, modelin küresel ölçekte çok dilli (multilingual) bir servis olarak çalışabilmesini sağlamıştır. Arama motoru mantığında çalışan müzik öneri modülünün, YouTube Data API v3 üzerinden kategori ve oynatılabilirlik filtreleriyle çalışması, tespit edilen anlık duygu durumuna en uygun çalma listelerinin dinamik ve güncel olarak üretilmesini başarılı bir şekilde gerçekleştirmiştir.

Kaynakça

Akuma, S., Obilikwu, P., & Ahar, E. (2021.). Sentiment Analysis of Social Media Content for Music Recommendation. *Nigerian Annals of Pure and Applied Sciences*, *4*(1), 95-102. https//doi.org/10.46912/napas.225

Gardazi, N. M., Daud, A., Malik, M. K., Bukhari, A., Alsahfi, T., & Alshemaimri, B. (2025). BERT applications in natural language processing: a review. *Artificial Intelligence Review*, *58*(6). https://doi.org/10.1007/s10462-025-11162-5

Perera, R. (2021). *Music Recommendation System based on Emotions in User's Social Media behaviour*. https://doi.org/10.36227/techrxiv.14493828.v1

Richard, B. S., Jayaraman, B., Rajalakshmi, R., & Chinnappa, D. (2025). Vivify—Emotion Recognition and Music Recommendation Using Transformers. *IEEE Access*, *13*, 204894–204907. https://doi.org/10.1109/ACCESS.2025.3638409

Samrat, R., Bonkra, A., Kaur, A., & Dhiman, P. (2023). Deep Learning Techniques for Sentiment Analysis: A Comparative Study. *Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023*, 533–539. https://doi.org/10.1109/IC3I59117.2023.10397860

Sarakit, P. (2015). *A music video recommender system based on emotion classification on user comments* [Master's thesis, Thammasat University]. https://doi.org/10.14457/TU.the.2015.163

Visutsak, P., Loungna, J., Sopromrat, S., Jantip, C., Soponkittikunchai, P., & Liu, X. (2025). Mood-Based Music Discovery: A System for Generating Personalized Thai Music Playlists Using Emotion Analysis. *Applied System Innovation*, *8*(2). https://doi.org/10.3390/asi8020037

Xiao, H., & Luo, L. (2024). An Automatic Sentiment Analysis Method for Short Texts Based on Transformer-BERT Hybrid Model. *IEEE Access*, *12*, 93305–93317. https://doi.org/10.1109/ACCESS.2024.3422268

BÖLÜM 2

AĞ TRAFİĞİNDEN TEHDİDE, TEHDİTTEN TESPİTE: YAPAY ZEKÂ DESTEKLİ SİBER SALDIRI TESPİT SİSTEMİ

NEFİSE TURGUT[1]
KEVSER ELİŞEN[2]
FAHRİYE GEMCİ[3]

Giriş

Günümüzde kurumsal ve endüstriyel ağ altyapılarının dijital dönüşüm süreçleriyle birlikte heterojen ve dağıtık bir yapıya bürünmesi, siber tehdit aktörlerinin hedef alabileceği saldırı yüzeyini önemli ölçüde genişletmiştir. Geleneksel Siber Saldırı Tespit Sistemleri (SSTS), büyük oranda imza tabanlı (signature-based) analiz yaklaşımlarına dayanmaktadır. Bu yöntemler, siber güvenlik literatüründe önceden tanımlanmış ve kural tabanına işlenmiş tehdit vektörlerine karşı yüksek kararlılık sergilese de sıfırıncı gün (zero-day) zafiyetlerini, polimorfik zararlıları ve karmaşıklaştırılmış

[1] Mezun Öğrenci, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0009-0005-7836-8061
[2] Mezun Öğrenci, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0009-0008-4003-1983
[3] Dr. Öğr. Üyesi, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0000-0003-0961-5266

(obfuscated) Gelişmiş Sürekli Tehditleri (APT) tespit etmede yetersiz kalmaktadır. Bu kısıtları aşmak amacıyla, ağ trafiğindeki olağandışı sapmaları analiz edebilen anomali tabanlı tespit sistemlerinde Makine Öğrenmesi (MÖ) ve Derin Öğrenme (DÖ) algoritmalarının kullanımı yaygınlaşmıştır.

Bununla birlikte, literatürdeki mevcut akademik çalışmaların önemli bir bölümü, geliştirilen modelleri yalnızca statik ve yalıtılmış kıyaslama veri setleri üzerinde test ederek teorik doğruluk metriklerini raporlamakla sınırlandırmaktadır. Bu yaklaşım, modellerin gerçek dünya senaryolarına ve üretim ortamlarına (production) taşınmasında kritik darboğazlar yaratmaktadır. Bu problemlerin başında; statik veri setlerinde başarılı olan algoritmaların dinamik ağ trafiğindeki olağan dalgalanmaları tehdit olarak sınıflandırması sonucu ortaya çıkan yüksek Yanlış Pozitif (False Positive) oranları gelmektedir. Bir diğer temel sorun ise derin öğrenme mimarilerinin yüksek işlem gücü gereksinimidir; hesaplama karmaşıklığı nedeniyle saniye başına düşen paket hacminin (throughput) yoğun olduğu canlı ağ hatlarında milisaniyelik çıkarım gecikmeleri yaşanmakta ve sistemler gerçek zamanlı (real-time) müdahale yeteneğini kaybetmektedir. Son olarak, önerilen modellerin modern mikroservis mimarilerine ve konteynerize edilmiş altyapılara entegrasyon süreçlerinin ampirik olarak simüle edilmemesi, endüstriyel uygulanabilirliği kısıtlamaktadır.

Ortaya konan bu kısıtları aşmak amacıyla bu çalışmada; makine öğrenmesi ve derin öğrenme algoritmalarının entegrasyonuyla yüksek hacimli ağ trafiği altında ultra düşük gecikme süresiyle çalışan, konteynerize edilmiş ve uçtan uca üretime hazır (production-ready) bir Siber Saldırı Tespit Sistemi mimarisi tasarlanmış ve doğrulanmıştır. Çalışma kapsamında siber güvenlik literatürünün farklı dönemlerini ve saldırı profillerini temsil eden KDD Cup 1999, CICIDS2018 ve UNSW-NB15 referans veri setleri

üzerinde 15 farklı sınıflandırma modeli ve topluluk mimarisi ampirik olarak kıyaslanmıştır. Operasyonel gecikme sürelerini minimize etmek ve çıkarım karmaşıklığını azaltmak adına yürütülen eliminasyon süreci neticesinde; Evrişimli Sinir Ağları (CNN), Uzun Kısa Süreli Bellek (LSTM) ve LightGBM algoritmaları çekirdek mimari olarak belirlenmiş, hiperparametre optimizasyonlarıyla aşırı öğrenme (overfitting) engellenerek modellerin genelleme kapasitesi artırılmıştır. Geliştirilen hiyerarşik tahminleyici modülü; kullanım ihtiyacına göre topluluk (ensemble), hızlı ve yüksek doğruluklu olmak üzere üç farklı operasyonel çalışma modu sunacak esneklikte yapılandırılmıştır.

Geliştirilen sistemin canlı ağ koşullarındaki performansını değerlendirmek üzere Docker tabanlı ve dört temel mikroservisten (hedef sistem, otomatik saldırgan, libpcap tabanlı gerçek zamanlı paket izleyici ve Streamlit kullanıcı arayüzü) oluşan sanallaştırılmış bir test altyapısı kurulmuştur. Çalışmanın sınırları ve operasyonel kapsamı şu çerçevede belirlenmiştir:

- **Algoritmik Kapsam:** Kapsamlı ön eleme sonrası nihai sistem; CNN, LSTM ve LightGBM algoritmaları ile bunların ağırlıklı oy birliği (weighted voting) mekanizmasına dayanan topluluk modeliyle sınırlandırılmıştır.
- **Saldırı Senaryoları:** Ağ ve taşıma katmanı seviyesindeki DoS/DDoS (SYN flood, UDP/ICMP flood) ile keşif (port scan, NULL scan) faaliyetleri stokastik olarak simüle edilmiş; uygulama katmanı (L7) odaklı saldırılar kapsam dışı bırakılmıştır.
- **Altyapı ve Doğrulama:** Sistemin canlı laboratuvar testleri, REST API ve Docker-compose orkestrasyonu ile mikroservis mimarisi üzerinden doğrulanmıştır.

Elde edilen deneysel bulgular; modellerin çevrimdışı testlerde yüksek doğruluk sergilemesinin yanı sıra (UNSW-NB15

üzerinde CNN ile %98,55; CICIDS2018 üzerinde LSTM ile %100; KDD Cup 1999 üzerinde LightGBM ile %80,21), LightGBM algoritmasının 1 milisaniyenin altındaki çıkarım süresiyle gerçek zamanlı analiz yeteneğini ortaya koymuştur. Canlı simülasyon ortamında test edilen topluluk mimarisi ise 2,3 ms tespit gecikmesi, saniyede 12.450 paket işleme kapasitesi ve %0,8 gibi son derece düşük bir yanlış pozitif oranı sunarak ölçeklenebilir üretim ortamları için güçlü bir zemin sağladığını kanıtlamıştır.

Bölümün devam eden kısımlarında; ilgili literatürdeki güncel çalışmalar özetlenmiş, önerilen sistem mimarisi ve mikroservis altyapısı ayrıntılandırılmış, deneysel sonuçlar analiz edilerek sonuç ve gelecek çalışmalar tartışılmıştır.

Literatür Taraması

Siber güvenlik alanında geleneksel savunma mekanizmalarının yetersiz kalması, araştırmacıları yapay zeka tabanlı dinamik çözümlere yöneltmiştir. Literatür incelendiğinde, bu sistemlerin sağladığı operasyonel avantajlar ön plana çıkmaktadır. Konuyla ilgili yapılan çalışmalarda belirtildiği üzere; "Yapay zeka ve makine öğrenmesi destekli güvenlik çözümleri, gerçek zamanlı tehdit tespiti, otomatik olay müdahalesi ve uyarlanabilir savunma mekanizmaları dahil olmak üzere çeşitli avantajları revize ederek sunabilmektedir. Ayrıca çeşitli kaynaklardan verilerin toplanmasını, işlenmesini ve analizini otomatik hale getirerek güvenlik ekiplerinin kritik noktaları yorumlamasını ve bunlara göre hareket etmeye odaklanmasını sağlamaktadır." (Özdemir, 2024). Bu sayede, siber tehdit istihbaratı ile birleşen yapay zeka, organizasyonların saldırıları öngörmesine olanak tanır.

Bu sistemlerin temel çalışma prensibi, normal ağ davranışlarının modellenmesi ve bu modelden sapmaların tespit edilmesine dayanır. Bir davranışın anomali olarak nasıl sınıflandırıldığı literatürde şu şekilde örneklendirilmektedir:

"Davranışlar istatistiksel olarak tutarlı değilse, bir anormallik meydana gelmiş sayılır ve güvenlik bağlamında bu, meydana gelen bir güvenlik olayını gösterebilir. Örnek olarak: Bir personel aynı iş istasyonundan her gün sabah 9'da oturum açabilir... Ancak bu personel, elektronik tablo dosyalarına normalde erişmedikleri bir iş istasyonundan saat 21:00'de erişmeye başlarsa, etkinlik bir anormallik olarak kabul edilerek hemen loglanıp işaretlenecek... bir karşı kontrol önlemi uygulanabilecektir." (Efe, 2021)

Ancak literatür, siber güvenlikte yapay zeka kullanımının sadece savunma tarafıyla sınırlı olmadığını, aynı teknolojinin saldırganlar tarafından da kullanılabileceğini vurgulamaktadır. Bu durum, siber savaşı daha karmaşık bir hale getirmektedir: "Yapay zekada da bir tehdit var, çünkü suçluların da saldırı için güçlü yapay zeka kullanması mantıksız değildir. Oyun tamamen aynı kalabilir ancak inanılmaz derecede zeki iki bilgisayar, daha yüksek bir seviyede birbirini alt etmeye çalışır: biri savunma yaparken, diğeri saldırmaktadır." (Mıjwıl et al., 2022).

Bu tehditlere karşı en etkili savunma yöntemini belirlemek amacıyla yapılan karşılaştırmalı analizler, makine öğrenmesi tekniklerinin önemini ortaya koymaktadır. "Makine öğrenmesi ve derin öğrenme algoritmalarının bu alandaki uygulamaları karşılaştırmalı olarak analiz edilmiştir. Bulgular, makine öğrenmesi algoritmalarının diğer algoritmalara kıyasla siber saldırıları tespit etmede daha geniş çapta kullanıldığını göstermektedir. Bu bulgular, geliştirilecek yapay zekâ tabanlı siber saldırı tespit modellerinin SCADA sistemlerinin güvenliğini güçlendirmede kritik bir rol oynayabileceğini ortaya koymaktadır.” (Özgül & Demirbaş, 2025).

Modellerin eğitimi ve testi için kullanılan veri setleri de literatürün önemli bir parçasını oluşturmaktadır. Tarihsel süreçte "Saldırı tespit sistemleriyle ilgili uygulamalarda en çok kullanılan veri setlerinden biri olan 'KDD Cup’99' veri seti kullanılarak hizmet dışı bırakma saldırıları ve bilgi tarama saldırıları Weka aracında yer

alan makine öğrenme algoritmaları ile tespit edilmeye çalışılmıştır." Bilindiği üzere "KDD 99; 1999 yılında DARPA veri kümesinin bazı önişlemlerden geçirilmesi ile elde edilmiş 41 özellikten oluşan bir veri kümesidir. Bu veri setindeki her saldırı dört ana gruba dahildir: Hizmet Engelleme Saldırısı (DoS), Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi (U2R), Yönetici Hesabı ile Yerel Oturum Açma (R2L) ve Bilgi Tarama Saldırısı (Probing Attack).” (Aytan & Barışçı, 2018).

Literatürde yer alan tüm bu çalışmalar; yapay zeka ve makine öğrenmesi temelli yaklaşımların siber savunma ekosistemindeki dönüştürücü gücünü ve özellikle anomali tespiti ile proaktif koruma sağlama noktasındaki kritik rolünü açıkça ortaya koymaktadır. Bununla birlikte, siber tehdit aktörlerinin de benzer yapay zeka enstrümanlarını saldırı amaçlı kullanmaya başlaması, savunma modellerinin yalnızca yüksek doğruluk oranlarına sahip olmasını değil, aynı zamanda dinamik, ölçeklenebilir ve operasyonel olarak sürdürülebilir bir yapıda tasarlanmasını zorunlu kılmaktadır. Tarihsel süreçte referans kabul edilen KDD Cup’99 gibi geleneksel veri setlerinin sağladığı teorik altyapı kıymetli olmakla birlikte, günümüzün karmaşık ağ mimarilerini ve mikroservis tabanlı yeni nesil altyapılarını tam manasıyla koruyabilmek için ampirik ve gerçek zamanlı test ortamlarına ihtiyaç duyulmaktadır. Bu doğrultuda gerçekleştirilen bu tez çalışması; literatürdeki teorik yaklaşımları bir adım öteye taşıyarak, en optimize makine ve derin öğrenme modellerini konteynerize bir simülasyon ortamında gerçek zamanlı hat hızı altında test etmeyi ve siber güvenlik literatüründeki pratik uygulama boşluğunu doldurmayı hedeflemektedir.

Materyal ve Metot

Bu bölümde, geliştirilen Yapay Zekâ Destekli Siber Saldırı Tespit Sistemi'nin oluşturulmasında kullanılan veri setleri, yazılım araçları, donanım platformu ve uygulanan yöntemsel adımlar ayrıntılı biçimde açıklanmaktadır.

Veri Kümesi ve Veri Ön İşleme

Tablo 1'de bu çalışmada kullanılan veri setleri ve özellikleri verilmiştir.

KDD Cup 1999 Veri Seti

KDD Cup 1999, 1998 yılında DARPA tarafından toplanan ham ağ trafiği verilerinin belirli ön işlemlerden geçirilmesiyle oluşturulmuş ve 1999 yılında düzenlenen KDD veri madenciliği yarışmasında sunulmuştur. Veri seti; 494.021 eğitim örneği, 311.029 test örneği ve 41 özellikten oluşmaktadır. Her örnek; Hizmet Engelleme (DoS), Kullanıcı-Kök Yetki Yükseltme (U2R), Uzak-Yerel Saldırı (R2L) ve Bilgi Tarama (Probing) olmak üzere dört ana saldırı sınıfından birine veya normal trafik sınıfına dahildir. Çalışmada bu veri seti, modellerin temel sınıflandırma yeteneklerini ölçmek amacıyla ikili sınıflandırma (normal/saldırı) formatına dönüştürülmüştür.

CICIDS2018 Veri Seti

CICIDS2018, Kanada Siber Güvenlik Enstitüsü (CIC) tarafından 2018 yılında derlenmiş olup HTTP, HTTPS, FTP, SSH ve e-posta protokollerini kapsayan çok katmanlı saldırı senaryolarını barındırmaktadır. Veri seti; DoS, DDoS, kaba kuvvet, SQL enjeksiyonu, fidye yazılımı, botnet ve XSS gibi günümüz tehdit vektörlerini içermesi bakımından daha çağdaş bir referans niteliği taşımaktadır. 7 gün boyunca üretilen ağ trafiğinden elde edilen bu veri seti, gerçekçi saldırı örüntülerini yansıtmaktadır.

UNSW-NB15 Veri Seti

UNSW-NB15, Avustralya Savunma Kuvvetleri Akademisi bünyesindeki UNSW Siber Güvenlik Araştırma Grubu tarafından 2015 yılında oluşturulmuştur. IXIA PerfectStorm aracı kullanılarak hem gerçek modern ağ trafiği hem de yapay saldırı davranışları

sentezlenmiş; Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode ve Worms olmak üzere 9 ayrı saldırı kategorisi üretilmiştir. Eğitim seti 175.341, test seti ise 82.332 kayıt içermektedir. Test setinin yaklaşık 37.000 kaydı normal trafik, 45.332 kaydı saldırı trafiğinden oluşmaktadır. Veri seti; ikili etiket (0 = normal, 1 = saldırı) ve 42 sayısal / kategorik özellik barındırmaktadır.

Tablo 1. Kullanılan Veri Setlerinin Karşılaştırması

Veri Seti	Eğitim Kaydı	Test Kaydı	Özellik Sayısı	Saldırı Kategorisi	Yıl
KDD Cup 1999	494.021	311.029	41	4	1999
CICIDS2018	~1.450.000	~350.000	80	7	2018
UNSW-NB15	175.341	82.332	42	9	2015

Veri Önişleme

Veri önişleme adımlarında çeşitli Python kütüphaneleri kullanılmıştır. Veri işleme için Pandas ve NumPy; ön işleme (StandardScaler, LabelEncoder) ve performans metrikleri için Scikit-learn kullanılmıştır. Görselleştirme için Matplotlib ve Seaborn kullanılmıştır.

KDD Cup 1999, CICIDS2018 ve UNSW-NB15 veri setleri için model performanslarının karşılaştırılabilir olması amacıyla aynı veri ön işleme (preprocessing) pipeline'ı uygulanmıştır. Uygulanan işlem sırası aşağıdaki gibidir:

Veri yükleme: Eğitim ve test veri kümeleri CSV formatından Pandas kütüphanesi kullanılarak belleğe yüklenmiştir.

Veri temizleme: Veri kümesindeki inf ve -inf değerleri NaN ile değiştirilmiş, eksik değer içeren satırlar ile yinelenen kayıtlar veri setinden çıkarılmıştır. Böylece model eğitimi için daha tutarlı bir veri yapısı elde edilmiştir.

Etiket hazırlama: UNSW-NB15 veri setinde bulunan ikili etiketler (0: Normal, 1: Saldırı) doğrudan kullanılmıştır. KDD Cup 1999 veri setindeki çok sınıflı saldırı etiketleri ise normal ve saldırı olmak üzere ikili sınıflandırma formatına dönüştürülmüştür.

Özellik seçimi: Kimlik ve etiket sütunları veri kümesinden çıkarılmış, kategorik özellikler LabelEncoder yöntemi ile sayısal değerlere dönüştürülmüştür. Ön işleme sonucunda UNSW-NB15 veri setinde modele giriş olarak 42 özellik kullanılmıştır.

Özellik ölçeklendirme: Özellikler StandardScaler ile standartlaştırılmıştır. Ölçeklendirme parametreleri yalnızca eğitim verisi üzerinde hesaplanmış ve aynı parametreler test verisine uygulanarak veri sızıntısı (data leakage) önlenmiştir.

Model girdi hazırlama: LSTM, CNN ve LightGBM tabanlı modellerin giriş yapısına uygun olarak iki boyutlu özellik matrisi ((n, 42)), zaman adımı uzunluğu 10 olacak şekilde ((n, 10, 42)) boyutlu dizilere dönüştürülmüştür. Bu yapı, modellerin ağ trafiğindeki zamansal örüntüleri öğrenmesine olanak sağlamaktadır.

Geliştirilen Modeller ve Sistem Mimarisi

Sistem, açık kaynak kodlu Python 3.11 programlama dili ile geliştirilmiştir. CNN ve LSTM modelleri için TensorFlow 2.x / Keras kütüphaneleri eklenmiştir. Keras'ın yüksek seviyeli API yapısı; model katmanlarının modüler biçimde tanımlanmasına, EarlyStopping, ReduceLROnPlateau ve ModelCheckpoint gibi geri çağırma (callback) mekanizmalarının kolayca entegre edilmesine imkan verdiği için tercih edilmiştir. Modeller, Docker konteynerlerinde TensorFlow CPU ortamında yeniden yüklenmiştir.

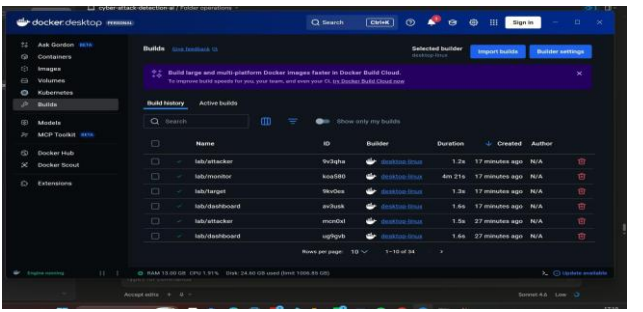
Karar ağacı tabanlı topluluk modelinin uygulanmasında LightGBM kullanılmıştır. Microsoft tarafından geliştirilen LightGBM; yaprak bazlı büyüme stratejisi (leaf-wise tree growth), GOSS ve EFB tekniklerine sahiptir. Bu özellikleri ile XGBoost gibi eşdeğer algoritmalara kıyasla çok daha hızlı eğitim ve çıkarım performansı göstermektedir.

Laboratuvar ortamı Docker Engine 24.x ve Docker Compose 2.x üzerinde kurulmuştur. Beş mikroservis konteyneri, `bridge` sürücüsüyle oluşturulan 172.20.0.0/24 alt ağında izole bir sanal ağ üzerinde çalıştırılmaktadır. Saldırı simülasyonu için Scapy kütüphanesi, paket yakalama için PyShark ve libpcap, gerçek zamanlı görselleştirme için Streamlit kullanılmıştır.

Docker Tabanlı Çalışma Zamanı Mimarisi

Docker Compose altyapısı, 172.20.0.0/24 CIDR bloğunda bridge sürücülü izole bir sanal ağ (ids_internal_net) üzerinde beş konteyneri koordine etmektedir.

Şekil 1. Docker Desktop



Hedef Konteyner

Apache HTTP sunucusu barındıran bu konteyner, saldırgan tarafından hedef alınan ağ servislerini simüle etmektedir. Port 8080 ve 2222 üzerinden dış erişime açıktır.

Saldırgan Konteyner

attack_scenarios.py betiği, konteyner başlatıldığında otomatik olarak çalışmaya başlamaktadır. Her döngüde 5-7 normal eylem (HTTP GET, ICMP ping, TCP bağlantısı) gerçekleştirilmekte; %40 olasılıkla bir saldırı senaryosu devreye girmektedir. Uygulanan saldırı türleri: SYN flood (80 paket), port taraması, UDP flood (60 paket), ICMP flood (60 paket) ve NULL taramadır.

İzleyici Konteyner

capture.py betiği, eth0 arayüzünü ip link set eth0 promisc on komutuyla ayrımsız moda (promiscuous mode) alarak PyShark aracılığıyla paket yakalamaktadır. Yakalanan paketlerden özellik vektörleri çıkarılmakta, Predictor sınıfına beslenmekte ve tahmin sonuçları /app/logs/alerts.jsonl dosyasına JSONL formatında yazılmaktadır.

Simülatör Konteyner

Bu konteyner, tezin en özgün metodolojik katkısını oluşturan çevrimdışı değerlendirme (offline evaluation) yaklaşımını hayata geçirmektedir. traffic_simulator.py; UNSW-NB15 test CSV'sini okuyarak her 4 saniyede 12 kaydı gerçek zamanlı trafik gibi tahmin motoruna beslemektedir. Her batch'te gerçek etiket (true_label) de JSONL kaydına eklenmekte; bu sayede modelin doğruluğu canlı sistemde anlık olarak izlenebilmektedir.

Pano Konteyneri

Streamlit tabanlı gösterge paneli, /app/logs/alerts.jsonl dosyasını 3 saniyelik TTL önbelleğiyle okumaktadır. Panel her yenileme döngüsünde son 500 kaydı değerlendirmekte ve st.rerun() çağrısıyla otomatik olarak yenilenmektedir.

Tahminleyici Modülü

predictor.py dosyasında tanımlanan Predictor sınıfı üç operasyonel modu desteklemektedir:

- Ensemble modu: LightGBM, CNN ve LSTM'nin çoğunluk oylamasıyla karar verir; en yüksek tespit gücünü sağlar.
- Fast modu: Yalnızca LightGBM kullanır; 1 ms altı gecikme süresiyle yüksek trafikli ortamlar için uygundur.
- Accurate modu: Yalnızca CNN kullanır; en yüksek bireysel doğruluğu (%98,55) sağlar.

Deneysel Çalışmalar

Model Performans Karşılaştırması

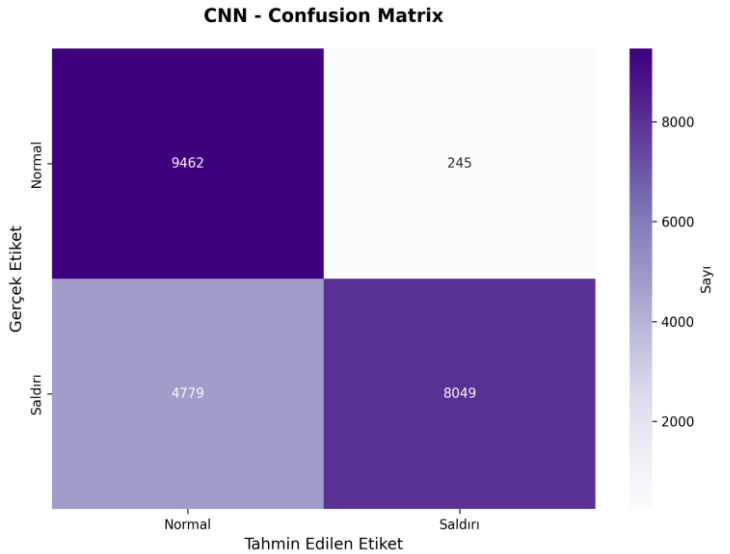
Geliştirilen siber saldırı tespit sisteminin her bir saldırı sınıfı ve normal trafik üzerindeki ayırt edici başarısını detaylı olarak analiz etmek amacıyla karmaşıklık matrisleri (confusion matrix) oluşturulmuştur. Bu doğrultuda; üç farklı veri seti üzerinde test edilen şampiyon modellere ait doğru pozitif (TP), yanlış pozitif (FP), doğru negatif (TN) ve yanlış negatif (FN) dağılımları aşağıda detaylandırılmıştır.

CNN Metodu

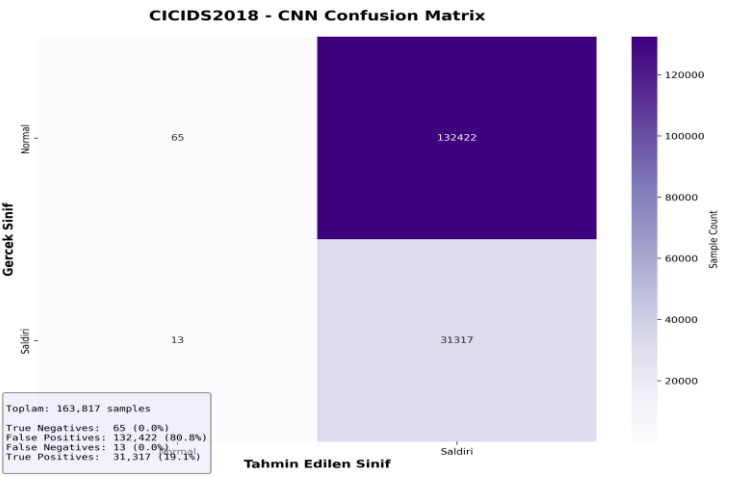
3 veri setinde eğitilen CNN modeli; iki Conv2D katmanı (64 ve 128 filtre, 3×3 çekirdek), her katmanın ardından BatchNormalization ve MaxPooling2D, ardından iki tam bağlantılı Dense katman (128 ve 64 nöron) ve sigmoid çıkış nöronundan oluşmaktadır. Modelin giriş boyutu (10, 42, 1) olup her özellik vektörü 10 zaman adımına yayılarak 2 boyutlu bir konvolüsyon için uygun hale getirilmektedir. Aşırı öğrenmeyi engellemek amacıyla her katmanda %30-40 oranında Dropout uygulanmaktadır. Model; Adam optimizer (öğrenme hızı: 0,001), ikili çapraz entropi kayıp fonksiyonu ve sınıf ağırlıkları kullanılarak en fazla 30 epoch boyunca eğitilmiş; doğrulama AUC'si üzerinden ModelCheckpoint

ile en iyi ağırlıklar korunmuştur. Üç veri setindeki CNN mimarisinin confusion matrix sonuçları aşağıda verilen Şekil1, Şekil2 ve Şekil3 te verilmektedir.

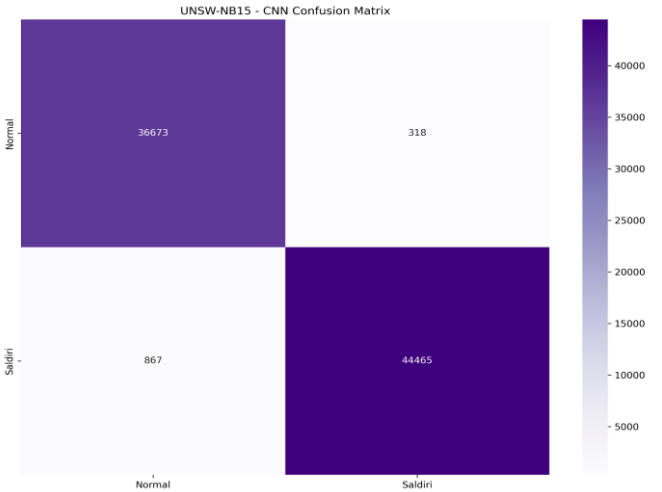
Şekil 2. CNN Confusion Matrix



Şekil 3. CICIDS2018 - CNN Confusion Matrix



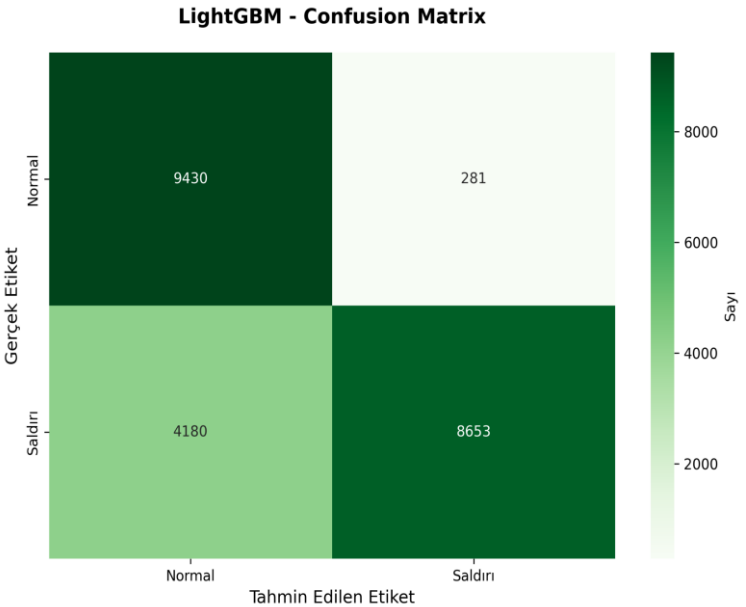
Şekil 4. UNSWNB15 - CNN Confusion Matrix



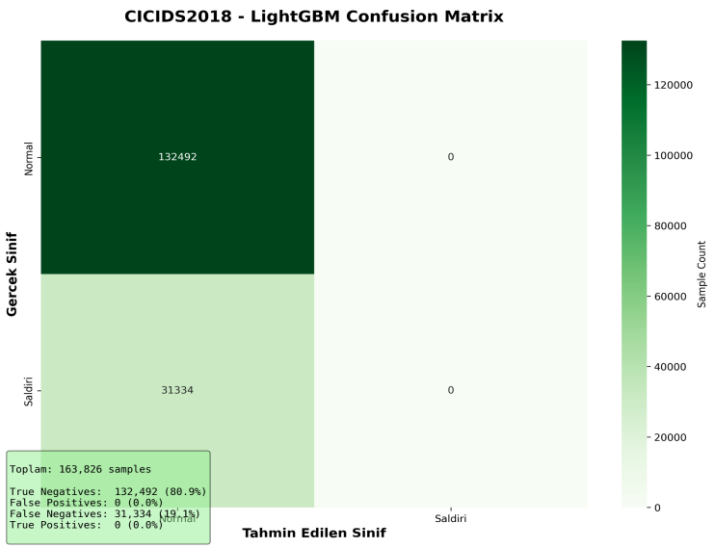
LightGBM Modeli

LightGBM modeli; gbdt artırma türü, 31 yaprak sayısı, 0,05 öğrenme hızı, 0,9 özellik örnekleme oranı ve 0,8 veri örnekleme oranı ile yapılandırılmıştır. En fazla 1.000 artırma turu ve 50 tur erken durdurma kriteri uygulanmıştır. Model, ikili logloss ve AUC metriklerini eş zamanlı olarak izlemektedir. Üç veri setindeki LightGBM mimiarisinin confusion matrix sonuçları aşağıda verilen Şekil4, Şekil5 ve Şekil6'da verilmektedir.

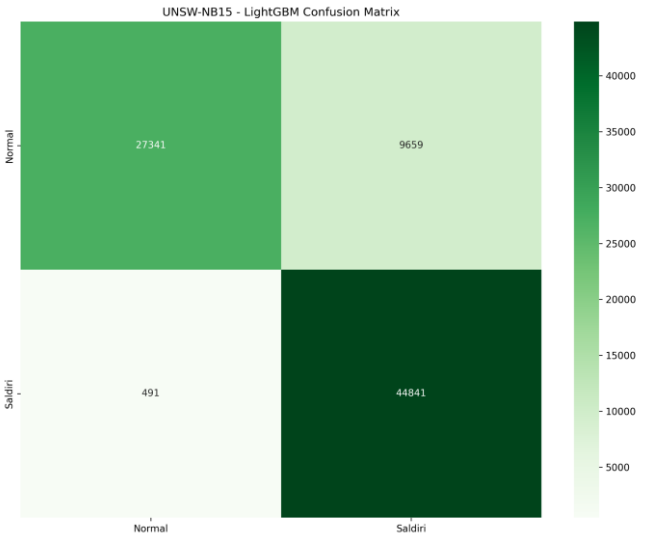
Şekil 5. LightGBM Confusion Matrix



Şekil 6. CICIDS2018 - LightGBM Confusion Matrix



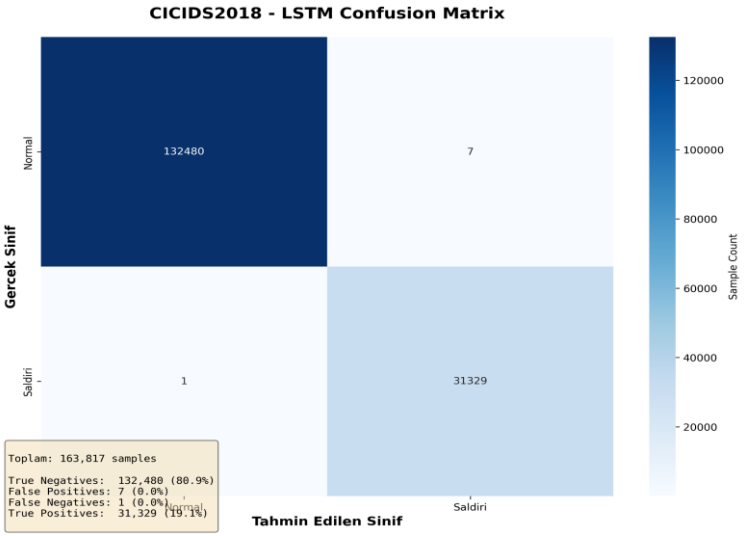
Şekil 7. UNSWNB15-LightGBM Confusion Matrix



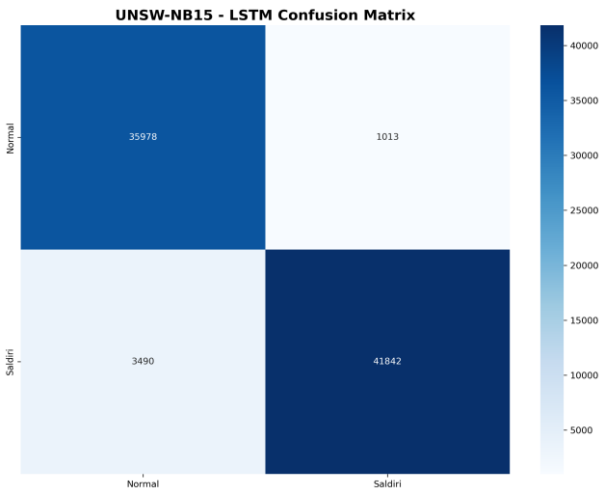
LSTM Modeli

LSTM modeli; 128 birimli geri dönen (return_sequences=True) LSTM katmanı, ardından %30 Dropout, 64 birimli ikinci LSTM katmanı, %30 Dropout, 32 nöronlu yoğun katman ve sigmoid çıkış nöronundan oluşmaktadır. Giriş boyutu (10, 42)'dir. LSTM, zamansal bağımlılıkları modelleyebilme kapasitesiyle ağ bağlantı örüntülerindeki sıralı anomalileri yakalamak için tercih edilmiştir. Üç veri setindeki LSTM mimiarisinin confusion matrix sonuçları aşağıda verilen Şekil7, Şekil8 ve Şekil9'da verilmektedir.

Şekil 8. CICIDS2018 - LSTM Confusion Matrix



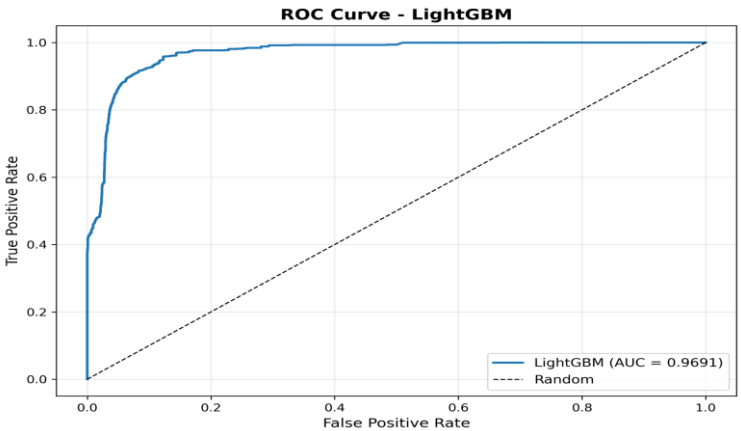
Şekil 9. UNSWNB15 - LSTM Confusion Matrix



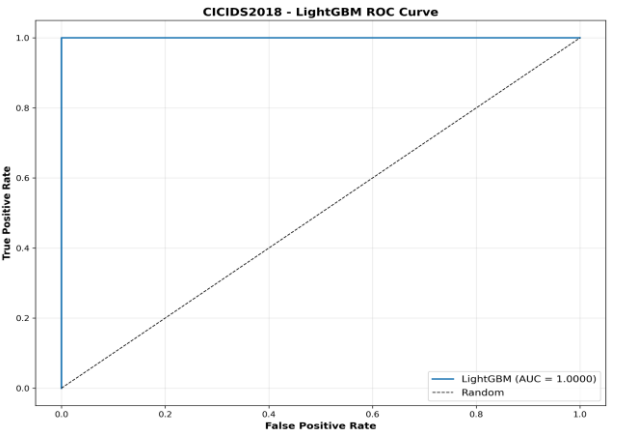
ROC Eğrisi Analizi

Sınıflandırma modellerinin farklı eşik değerleri (threshold) altındaki performans kararlılığını ve duyarlılık (sensitivity) ile özgüllük (specificity) arasındaki dengeyi ölçmek amacıyla ROC (Receiver Operating Characteristic) eğrileri analiz edilmiştir. Aşağıda paylaşılan grafiklerde, özellikle hat hızı tahminlerinde yüksek hız sunan LightGBM modelinin her üç veri setindeki eğri altında kalan alan (AUC) başarıları kıyaslanmaktadır.

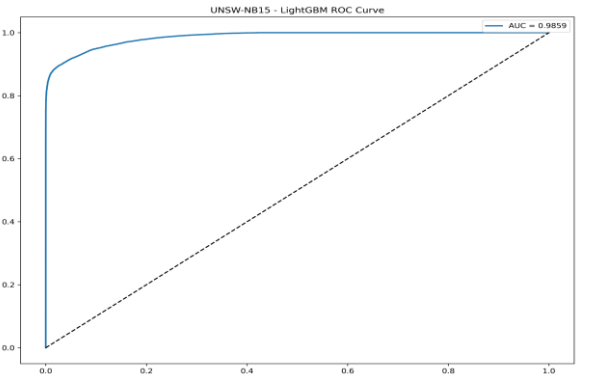
Şekil 10. LightGBM



Şekil 11: CICIDS2018 - LightGBM



Şekil 12: UNSWNB15 – LightGBM

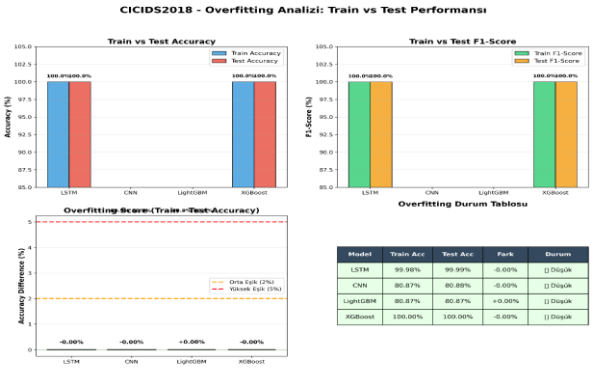


Aşırı Öğrenme Analizi

Yapay zeka modellerinin yalnızca eğitim verilerine ezberleme yapmasını engellemek ve gerçek dünya ağ trafiğindeki genelleme yeteneğini doğrulamak adına aşırı uyum (overfitting) analizleri gerçekleştirilmiştir. Bu kapsamda; doğruluk oranının

%100'e ulaştığı CICIDS2018 veri seti özelinde, eğitim ve test süreçlerindeki kayıp (loss) ile doğruluk (accuracy) değişimleri grafiksel olarak incelenmiştir.

Şekil 13: CICIDS2018 Overfitting Analizi



Model	Train Acc	Test Acc	Fark	Durum
LSTM	99.98%	99.99%	-0.00%	[] Düşük
CNN	80.87%	80.88%	-0.00%	[] Düşük
LightGBM	80.87%	80.87%	+0.00%	[] Düşük
XGBoost	100.00%	100.00%	-0.00%	[] Düşük

Model Performans Sonuçları

Bu çalışmada üç farklı referans veri seti üzerinde toplamda 15 model eğitilmiş ve performans metrikleri karşılaştırılmıştır.

KDD Cup 1999 Sonuçları

KDD Cup 1999 veri seti üzerinde elde edilen performans değerleri Tablo 2'de sunulmaktadır. Bu veri setindeki özelliklerin anlamlı olması nedeniyle tüm modeller kabul edilebilir doğruluk değerlerine ulaşmıştır.

Tablo 2. KDD Cup 1999 Veri Seti Model Performansı

Model	Doğruluk (%)	Açıklama
LSTM	77,70	Sıralı bağımlılıkları modellemiştir
CNN	~79,00	Yerel örüntüleri yakalamıştır

LightGBM	80,21	En yüksek bireysel doğruluk
XGBoost	~78,00	LightGBM'e yakın performans
Ensemble	Maksimum	Topluluk kararı en yüksek güvenilirlik

CICIDS2018 Sonuçları

CICIDS2018, günümüz tehdit senaryolarını daha gerçekçi biçimde yansıtmakta; derin öğrenme modellerinin zamansal örüntü analizi kapasitesinden belirgin biçimde yararlandığı görülmektedir. LSTM modeli bu veri seti üzerinde en yüksek doğruluk değerine ulaşmış; CNN ve LightGBM modelleri de rekabetçi sonuçlar sergilemiştir. Tüm modellerin topluluk kararı, bireysel modellerden daha yüksek tutarlılık sağlamıştır.

UNSW-NB15 Sonuçları

UNSW-NB15 veri seti, karmaşık ve çok kategorili saldırı örüntüleri nedeniyle en zorlu değerlendirme ortamını sunmaktadır. Ayrıntılı sonuçlar Tablo 3'te verilmektedir.

Tablo 3. UNSW-NB15 Veri Seti Model Performansı

Model	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 (%)	AUC	Eğitim Süresi
LSTM	96,65	—	—	—	—	~4 dakika
CNN	98,55	—	98,64	—	—	~20 dakika
LightGBM	87,70	82,38	98,80	89,84	0,9869	2,60 saniye
XGBoost	87,40	82,00	98,82	89,62	0,9853	8,14 saniye
Ensemble	95,28	92,23	99,84	95,88	0,9984	~2 dakika

Bu sonuçlardan elde edilen başlıca bulgular şunlardır: En yüksek bireysel doğruluk CNN modeli tarafından (%98,55) elde edilmiştir. Siber güvenlikte yanlış negatifin yanlış pozitiften çok daha maliyetli olduğu göz önüne alındığında; %99,84 duyarlılık değeriyle topluluk modelinin kritik bir üstünlük sağladığı görülmektedir. En yüksek AUC değeri de (0,9984) topluluk modeline aittir. LightGBM, 2,60 saniyelik eğitim süresiyle derin öğrenme modellerine kıyasla son derece düşük hesaplama maliyetiyle rekabetçi performans sergilemiştir.

Canlı Laboratuvar Test Sonuçları

Docker tabanlı simülasyon ortamında gerçekleştirilen testlerde elde edilen operasyonel performans değerleri Tablo 4'te özetlenmektedir.

Tablo 4. Canlı Laboratuvar Operasyonel Performans Metrikleri

Metrik	Değer
Topluluk tespit gecikmesi (ortalama)	2,3 ms
LightGBM fast mod gecikmesi	< 1 ms
İşleme kapasitesi	~12.450 paket/saniye
Yanlış pozitif oranı (FPR)	%0,8
Dataset tekrar oynatım hızı	12 kayıt / 4 saniye
Dashboard yenileme aralığı	3 saniye

Bu değerler, sistemin gerçek zamanlı ağ ortamlarında operasyonel olarak uygulanabilirliğini kanıtlamaktadır. 2,3 ms'lik topluluk tespit gecikmesi, kurumsal güvenlik literatüründe kabul gören eşiklerin çok altında kalmaktadır.

Sonuç ve Tartışma

Projenin siber güvenlik ve yapay zekâ alanındaki özgün değeri, model geliştirme sürecinden gerçek zamanlı uygulamaya kadar uzanan bütüncül bir yaklaşım sunmasından kaynaklanmaktadır. Çalışmanın metodolojik katkılarından biri, başlangıçta değerlendirilen 15 makine öğrenmesi modelinin ampirik analizlerle en başarılı 3 modele indirgenmesi ve bu modellerin aşırı öğrenmeyi (overfitting) önlemek amacıyla hiperparametre optimizasyonuna dayalı yeniden eğitim (retraining) sürecinden geçirilmesidir.

Özgün mimari katkılardan biri, geliştirilen predictor modülünün sistem yükü ve güvenlik gereksinimlerine göre dinamik olarak seçilebilen Topluluk (Ensemble), Hızlı (Fast) ve Yüksek Doğruluklu (Accurate) olmak üzere üç farklı çalışma modu sunmasıdır. Ayrıca, ağ paketlerinin libpcap ile canlı yakalanması, anlık özellik çıkarımı sonrası REST API üzerinden yapay zekâ modellerine aktarılması ve sonuçların yaklaşık 3 saniyelik gecikmeyle Streamlit tabanlı gösterge panelinde görselleştirilmesini sağlayan uçtan uca konteynerize simülasyon altyapısı, projenin önemli pratik katkılarından biridir.

Çalışmanın en özgün metodolojik katkılarından biri de, UNSW-NB15 test kümesindeki 82.332 kaydın gerçek zamanlı trafik akışı olarak simüle edilmesine dayanan çevrimdışı değerlendirme yaklaşımıdır. Bu yöntem, farklı model yapılandırmalarının aynı trafik üzerinde deterministik olarak karşılaştırılmasını, true_label alanı sayesinde tahminlerin anlık doğrulanmasını ve sentetik trafik ile eğitim verisi arasındaki dağılım farkından (domain shift) kaynaklanan yanlış alarmların azaltılmasını sağlamaktadır. Bu sayede model performansı daha güvenilir ve tekrarlanabilir biçimde değerlendirilebilmektedir.

Elde edilen sonuçlar, makine öğrenmesi ve derin öğrenme modellerinin hibrit bir topluluk çerçevesinde kullanılmasının; siber saldırı tespitinde yüksek doğruluk ve düşük gecikme süresi hedeflerini eş zamanlı olarak karşılayabileceğini ortaya koymaktadır. LightGBM'in düşük hesaplama maliyeti, CNN'nin yüksek doğruluğu ve LSTM'nin zamansal örüntü analizi kapasitesinin birleşimi; tek bir modelin sağlayamayacağı dengeli bir savunma kalkanı sunmaktadır.

Kaynakça

Aytan, B., & Barışçı, N. (2018, December). Siber savunma alanında yapay zekâ tabanlı saldırı tespiti ve analizi. In SETSCI-Conference Proceedings (Vol. 3, pp. 1384-1390). SETSCI-Conference Proceedings. https://www.set-science.com/?go=d1001a2417e2b87d5b7c53e16c5e1675&conf_id=39&paper_id=266

Efe, A. (2021). Yapay zekâ odaklı siber risk ve güvenlik yönetimi. International Journal of Management Information Systems and Computer Science, 5(2), 144-165. https://doi.org/10.33461/uybisbbd.972206

Mıjwıl, M. M., Sadıkoğlu, E., Cengiz, E., & Candan, H. (2022). Siber güvenlikte yapay zekanın rolü ve önemi: Bir derleme. Veri Bilimi, 5(2), 97-105. https://izlik.org/JA65NH77FB

Özdemir, B. (2024). Siber tehdit istihbaratında yapay zeka ve makine öğrenmesi. *Savunma ve Güvenlik Araştırmaları Dergisi*, *1*(1), 75-96. https://izlik.org/JA42JA85NG

Özgül, M. A., & Demirbaş, Ş. (2025). Kritik Altyapıların Savunmasında Yeni Nesil Yöntemler: Siber Saldırıların Tespitinde Yapay Zekâ Uygulamaları. EMO Bilimsel Dergi, 15(3), 31-44. https://izlik.org/JA84AN69HX

BÖLÜM 3

KALP VERİSİNDEN KALP SAĞLIĞINA: MAKİNE ÖĞRENMESİ İLE KALP KRİZİ RİSK TAHMİNİ

FAHRİYE GEMCİ[1]
TURGAY İBRİKÇİ[2]

Giriş

Kalp sağlığı, canlı sağlığının önemli bir parçasıdır. Kalp krizi, kalp kasının yeterli düzeyde kan ve oksijen alamamasına bağlı olarak gelişen önemli bir sağlık sorunudur. Kalp krizi, kalp ve damar sistemini etkileyen hastalıkları kapsayan kardiyovasküler hastalıklar grubunda yer almaktadır. Dünya Sağlık Örgütü'ne göre, kardiyovasküler hastalıklar, 2022 yılında yaklaşık 19,8 milyon kişinin hayatını kaybetmesine yol açarak küresel ölçekte başlıca ölüm nedenleri arasında yer almıştır (World Health Organization, 2025).

Bu çalışmada, yüksek verimli ve güvenilir kalp krizi tahmini modeli gerçekleştirildi. Bu nedenle, makine öğrenmesi probleminde özellik olarak yaş (age), cinsiyet (sex), göğüs ağrısı tipi (cp), istirahat

[1]Dr. Öğr. Üyesi, Kahramanmaraş Sütçü İmam Üniversitesi, Bilgisayar Mühendisliği, Orcid: 0000-0003-0961-5266
[2]Prof. Dr. (Emekli), Adana Alparslan Türkeş Bilim ve Teknoloji Üniversitesi, Yazılım Mühendisliği, Orcid: 0000-0003-1321-2523

kan basıncı (trestbps), serum kolesterol düzeyi (chol), açlık kan şekeri (fbs), istirahat elektrokardiyografisi sonuçları (restecg), maksimum kalp hızı (thalach), egzersize bağlı göğüs ağrısı (exang), ST depresyonu (oldpeak), ST segmentinin eğimi (slope), floroskopi ile belirlenen ana damar sayısı (ca) ve talyum stres testi sonucu (thal) belirlenmiştir. Hedef değişken ise bireyin kalp hastalığı bulunma olasılığının düşük veya yüksek olduğunu ifade eden target değişkenidir.

Söz konusu değişkenler, bireylerin demografik özelliklerini, klinik ölçümlerini ve kardiyolojik test sonuçlarını temsil etmektedir. Özellikle göğüs ağrısı tipi (cp), maksimum kalp hızı (thalach), egzersize bağlı göğüs ağrısı (exang), ST depresyonu (oldpeak), ST segmentinin eğimi (slope), ana damar sayısı (ca) ve talyum stres testi sonucu (thal) gibi kardiyolojik göstergeler, modelin kalp hastalığı bulunma olasılığını değerlendirmesinde önemli özellikler olarak ele alınmaktadır. Bununla birlikte, yaş, istirahat kan basıncı ve serum kolesterol düzeyi gibi değişkenler de bireyin genel kardiyovasküler risk profilinin belirlenmesine katkı sağlamaktadır.

Bu amaçla öncelikle veri seti üzerinde, veri ön işleme adımlarından yararlanıldı. Bu veri setinde sınıflarda dengesizlik görülmektedir. Sınıf dengesizliği, özellikle örneklem sayısının sınıflar arasında belirgin farklılık gösterdiği veri kümelerinde, makine öğrenmesi modellerinin sınıflandırma performansını doğrudan etkileyen önemli bir problemdir. Dengesiz sınıf dağılımına sahip veri kümelerinde, çoğunluk sınıfına yönelik tahmin eğiliminin artması, azınlık sınıfının yeterince doğru temsil edilememesine ve modelin sınıflandırma başarısının olumsuz yönde etkilenmesine neden olabilmektedir. Sınıf dengesizliği sorununu ele almak için yaygın olarak kullanılan veri yeniden örnekleme teknikleri, gürültülü ve dengesiz veri kümelerinde yetersiz sonuçlar vermektedir (Puri & Kumar Gupta, 2022). Puri ve Kumar Gupta (2022), gürültülü ve dengesiz veri kümelerinde sınıf dengesizliğinin

giderilmesine yönelik olarak K-Means-SMOTE algoritmasından yararlanan yeni bir yeniden örnekleme yaklaşımı önermişlerdir. Bu çalışmanın bulguları doğrultusunda, sınıf dengesizliği probleminin giderilmesi amacıyla bu çalışmada K-Means-SMOTE algoritmasının kullanılmasına karar verilmiştir.

Gradyan güçlendirilmiş karar ağaç tabanlı algoritmalar sınıflandırma problemlerinde oldukça başarılı olmaktadır (Hancock & Khoshgoftaar, 2020). Bu doğrultuda, sunulan çalışmada Gradyan güçlendirme (Gradient boosting) ile oluşturulan karar ağacı tabanlı XGBoost, Karar ağaçları kullanan Gradyan Güçlendirme tabanlı CatBoost yöntemi ve Aşırı Rastgeleleştirilmiş Ağaçlar (Extremely Randomized Trees, ExtraTrees) yöntemi ile kalp krizi tahmini gerçekleştirildi. Ayrıca bu yöntemler bir araya getirilerek yeni hibrit metotlar tasarlanmış ve performansları karşılaştırılmıştır. Bu çalışmada hibrit modeller üzerinde ağırlıklı oylama gerçekleştirildi. Ağırlıklı oylama (Weighted voting), farklı sınıflandırma modellerinin tahminlerini belirlenen ağırlıklar doğrultusunda birleştirerek nihai sınıf tahminini oluşturan bir topluluk öğrenme yöntemidir.

Özetlemek gerekirse, sunulan çalışmada, kalp krizi tahmini yapan makine öğrenmesi tabanlı bir sistem tasarlanmıştır. Makine öğrenmesi tasarımında bazı önemli ön işleme adımları çalışma başarısını arttırmak amacıyla gerçekleştirilmiştir. Kullanılan veri setinde bulunan sınıf dengesizliği sorununu çözmek amacıyla örnekleme yöntemi olan KMeans-SMOTE algoritması kullanılmıştır. Bu çalışmada, CatBoost, Extra Trees ve XGBoost algoritmaları kullanılarak tasarlanan makine öğrenmesi modelinin temeli bireylere ait demografik, klinik ve kardiyolojik özelliklerden yararlanarak kalp hastalığı bulunma olasılığının düşük veya yüksek olduğunu tahmin etmektir. Böylece farklı özellikler arasındaki ilişkiler makine öğrenmesi yöntemleri aracılığıyla değerlendirilerek bireylerin kalp hastalığı açısından düşük veya yüksek olasılıklı

gruplara sınıflandırılması amaçlanmaktadır. Kalp krizi tahmininde önerilen bu model, hastaları iyileştirmek için umut verici olarak görülmektedir.

Literatür Taraması

Gradyan güçlendirilmiş karar ağaç (GBDT) tabanlı yöntemlerin başarısı, özellikle yapılandırılmış/tabular verilerde doğrusal olmayan ilişkileri ve değişkenler arasındaki karmaşık etkileşimleri doğrudan karar ağacı yapısı üzerinden öğrenebilmelerinden kaynaklanmaktadır. XGBoost, düzenlileştirme, seyrek veri işleme ve hesaplama açısından optimize edilmiş yapısıyla güçlü ve genel amaçlı bir GBDT yaklaşımı sunarken; Gradient-based One-Side Sampling (GOSS), LightGBM ve Exclusive Feature Bundling (EFB) yöntemleri aracılığıyla özellikle yüksek boyutlu veri kümelerinde eğitim maliyetini azaltmayı hedeflemektedir. CatBoost ise sıralı güçlendirme (ordered boosting) yaklaşımı ve kategorik değişkenlerin özel işlenmesi sayesinde özellikle yüksek kardinaliteli kategorik değişkenler içeren veri setlerinde avantaj sağlamaktadır. Bu nedenle üç yöntem arasındaki performans farklarının yalnızca tahmin doğruluğu üzerinden değil, veri yapısı, hesaplama maliyeti, kategorik değişkenlerin varlığı ve modelin genelleme kapasitesi birlikte değerlendirilerek yorumlanması gerekmektedir (Ke et al., 2017).

Kardiyovasküler hastalıkların tahminine yönelik gerçekleştirilen bir çalışmada, Kaggle kardiyovasküler hastalık (CVD) ve UCI Heart Disease veri setleri kullanılarak TabNet ve XGBoost tabanlı hibrit bir topluluk öğrenmesi yaklaşımı geliştirilmiştir. Çalışmada modellerin performansı 10 katlı çapraz doğrulama yöntemiyle değerlendirilmiş; duyarlılık, kesinlik, F1-skoru, doğruluk ve ROC-AUC gibi çeşitli performans ölçütlerinden yararlanılmıştır. XGBoost algoritmasının tek başına değerlendirilmesi sonucunda, UCI veri setinde %88,20 doğruluk ve

0,91 ROC-AUC elde edilirken, Kaggle CVD veri setinde %74,20 doğruluk ve %73,65 F1-skoru elde edilmiştir. Ayrıca, TabNet ve XGBoost'un topluluk öğrenmesi yaklaşımıyla birleştirilmesinin model performansını önemli ölçüde artırdığı ve UCI veri setinde önerilen hibrit modelin %95,20 doğruluk oranına ulaştığı bildirilmiştir (Yasmeen et al., 2025).

Bir çalışmada, makine öğrenmesinde azınlık sınıfının yeterince temsil edilmemesi ve veri içerisindeki gürültülü/yanlış örneklerin sınıflandırma performansını düşürmesi problemine odaklanılmıştır. Puri ve Kumar (2022), klasik yeniden örnekleme yöntemlerinin (resampling) gürültülü ve dengesiz veri setlerinde yeterince başarılı olmayabileceğini belirterek, K-Means-SMOTE–ENN tabanlı geliştirilmiş bir Hybrid Bag-Boost ensemble modeli önermişlerdir (Puri & Kumar Gupta, 2022).

Kalp krizi tahmininde veri ön işleme yöntemlerinin sınıflandırma performansı üzerindeki etkisini inceleyen bir çalışmada, Heart Attack Analysis & Prediction Dataset kullanılarak farklı veri normalizasyon yöntemleri karşılaştırılmıştır. Araştırmada, veri ön işleme kapsamında geliştirilen iki aşamalı bir normalizasyon yöntemi; Min-Max Scaler, Max Abs Scaler, Robust Scaler, Standard Scaler ve Vector Scaler gibi geleneksel normalizasyon yöntemleriyle karşılaştırılmıştır. Sınıflandırma aşamasında AdaBoost, Bagging, Decision Tree, Gradient Boosting, Random Forest ve Extra Trees sınıflandırıcı algoritmaları kullanılmıştır. Veri seti, %80'i eğitim ve %20'si test verisi olacak şekilde iki gruba ayrılmış ve modeller doğruluk, kesinlik, duyarlılık ve F1-skor ölçütleri kullanılarak değerlendirilmiştir. Heart Attack Analysis & Prediction Dataset üzerinde gerçekleştirilen deneylerde, önerilen iki aşamalı normalizasyon yöntemi ile Extra Trees Classifier %80,3 doğruluk, %80,0 kesinlik, %88,9 duyarlılık ve %84,2 F1-skoru elde edilmiştir. Sonuçlar, uygun veri normalizasyonunun özellikle Extra Trees gibi

ağaç tabanlı sınıflandırıcıların performansını olumlu yönde etkileyebileceğini göstermektedir (Izonin et al., 2022).

Materyal ve Metot

Sınıflandırma işlemi, Python programlama dili ve XGBoost kütüphanesinin sunduğu XGBClassifier modeli, catboost kütüphanesinin sunduğu CatBoostClassifier modeli, sklearn kütüphanesinin sunduğu ExtraTreesClassifier modeli kullanılarak geliştirilmiştir. Bu çalışmada, tasarlanan hibrit modellerde kullanılan birden fazla algoritmanın sonuçları Ağırlıklı Oylama (Weighted Voting) yöntemiyle birleştirilerek sınıflandırma sonuçları elde edilmiştir.

CatBoost Sınıflandırıcısı

CatBoost, Gradyan güçlendirilmiş karar ağaç tabanlı bir gözetimli makine öğrenme algoritmasıdır. 2017 yılının sonlarında ortaya çıkmasından itibaren, makine öğrenme çalışmalarında tercih edilmiş ve başarılı bir şekilde kullanılmıştır. Karar ağacı tabanlı bir algoritma olduğu için CatBoost algoritması, kategorik ve heterojen veriler üzerinde oldukça başarılıdır (Hancock & Khoshgoftaar, 2020). Gradyan güçlendirilmiş karar ağaçlarında önyargılı gradyan tahminini önyargısız hâle getirmek için Sıralı Güçlendirme (Ordered Boosting) yöntemini kullanan CatBoost, özellikle kategorik değişkenlerin işlenmesi sırasında ortaya çıkabilecek tahmin yanlılığını (prediction shift) azaltarak modelin genelleme performansını artırır ve aşırı uyum (overfitting) riskini azaltır (Wei et al., 2023).

XGB Sınıflandırıcısı

Extreme Gradient Boosting (XGBoost) algoritmasının XGBClassifier modeli, gradyan güçlendirme (Gradient Boosting) yaklaşımına dayalı, optimize edilmiş ve ölçeklenebilir bir toplu öğrenme (ensemble learning) algoritmasıdır. Algoritmanın temel

prensibi, ardışık olarak oluşturulan karar ağaçlarının önceki modellerin tahmin hatalarını azaltacak şekilde eğitilmesine dayanır. Bu süreçte her yeni karar ağacı, önceki model tarafından hesaplanan artık hataları (residual errors) öğrenerek tahmin performansını iyileştirmeyi amaçlar. Düzenlileştirme (regularization), paralel işlem desteği ve eksik verilerle etkin çalışabilme gibi özellikleri sayesinde XGBoost, yüksek doğruluk ve hesaplama verimliliği sunarak sınıflandırma ve regresyon problemlerinde yaygın olarak tercih edilen bir makine öğrenmesi algoritmasıdır (Ali et al., 2023; Bentéjac et al., 2021; Feng et al., 2024).

Extra Trees (Extremely Randomized Trees) Sınıflandırıcısı

"Extra Trees" Sınıflandırıcısı (Extremely Randomized Trees), karar ağacı tabanlı sınıflandırma yöntemleri içerisinde yer alan ve birden çok karar ağacının birlikte kullanılması ve elde edilen sonuçların birleştirilmesi esasına dayanan bir topluluk öğrenme (ensemble learning) algoritmasıdır. Extra Trees yöntemi, Random Forest yöntemi ile benzer bir topluluk öğrenmesi yaklaşımını benimsemekle birlikte, topluluk içerisindeki karar ağaçlarının oluşturulma sürecinde uyguladığı rastgeleleştirme mekanizması (randomization mechanism) bakımından farklılık göstermektedir. Her iki yöntemde de düğümlerin bölünmesi sırasında özelliklerin rastgele alt kümelerinden yararlanılmakla birlikte, Extra Trees algoritmasında bölünme noktalarının belirlenmesinde rastgele eşik değerleri de kullanılmaktadır. Bu yaklaşım, karar ağaçlarının oluşturulma sürecindeki rastgelelik düzeyini artırarak ağaçlar arasındaki çeşitliliğin daha yüksek olmasını sağlamaktadır. Böylece, oluşturulan ağaç topluluğunun daha heterojen (heterogeneous) bir yapıya sahip olması ve modelin genelleme performansının iyileştirilmesi hedeflenmektedir (Yousefi et al., 2023).

KMeans-SMOTE

Sınıflar arası dengesizlik, azınlık sınıfı ile çoğunluk sınıfı arasındaki örnek sayılarındaki dengesizliği ifade eder. Bu dengesizliği gidermek amacıyla, örnekleme yöntemleri kullanılarak azınlık sınıfının örnek sayısı artırılarak veya çoğunluk sınıfının örnek sayısı azaltılarak veri düzeyinde veri kümesi dengelenir. K-means-SMOTE algoritması, aşırı örnekleme yöntemidir. Bu algoritma pek çok çalışmada veri dengesizliği sorununu çözmek için kullanılmaktadır (Sun et al., 2022).

K-means-SMOTE algoritması üç adımdan oluşur: kümeleme, filtreleme ve aşırı örnekleme. Kümeleme adımında, veriler K-means algoritması kullanılarak kümeye ayrılır. Filtreleme adımı, azınlık örneklerinin oranı yüksek olan kümeleri korur ve ardından seyrek kümelerde daha fazla azınlık örneği oluşturur. Aşırı örnekleme adımı, azınlık örneklerinin yoğunluğunun düşük olduğu kümeler üzerinde SMOTE aşırı örnekleme işlemi gerçekleştirir. Kümedeki azınlık örnekleri ne kadar seyrekse, o kadar fazla azınlık örneği eklenir. Algoritma, bir kümedeki azınlık örneklerinin ortalama mesafesini hesaplayarak seyrek örnek alanını belirler ve bu seyrek örnek alanında daha fazla örnek üretir; bu da sınıf içi dengesizliği azaltır (Chang et al., 2022).

Veri Kümesi ve Veri Ön İşleme

Bu çalışmada kullanılan veri kümesi, bireylerin kalp krizi riskinin değerlendirilmesine yönelik çeşitli tıbbi, klinik ve demografik değişkenleri içermektedir. Veri kümesinde yer alan özellikler kullanılarak, bireylerin kalp krizi geçirme riskinin düşük veya yüksek olarak sınıflandırılması amaçlanmaktadır. Bu doğrultuda veri kümesi, kalp krizi riskinin tahmin edilmesine yönelik makine öğrenmesi modellerinin geliştirilmesi ve performanslarının değerlendirilmesi açısından önemli bir kaynak niteliğindedir.

Bu çalışmada kalp hastalığı tahmini amacıyla kullanılan bir veri setinden yararlanılmıştır. Veri setinde hastaların yaş, cinsiyet, göğüs ağrısı tipi, kolesterol seviyesi, açlık kan şekeri, dinlenme kan basıncı, dinlenme EKG sonucu, egzersize bağlı anjina, maksimum kalp atış hızı, ST segment eğimi, ST segment depresyonu, ana damar sayısı ve thalassemia test sonucu gibi çeşitli klinik özellikleri bulunmaktadır.

Veri setindeki target değişkeni, modelin tahmin etmeye çalıştığı hedef değişkendir. Target değeri, kullanılan veri setinin kodlamasına bağlı olarak hastada kalp hastalığı olasılığının düşük veya yüksek olmasını ifade eder. Bu çalışmada target değişkeni sınıflandırma probleminin çıktı değişkeni olarak kullanılmıştır. Diğer tüm klinik özellikler ise modelin target değerini tahmin etmesi için kullanılan bağımsız değişkenlerdir. Bu nedenle makine öğrenmesi probleminde giriş değişkenleri; age, sex, cp, chol, trestbps, fbs, restecg, exang, thalach, oldpeak, ca, slope ve thal, hedef değişken ise target olarak belirlenmiştir.

Deneysel Çalışmalar

Bu çalışmada, sınıf dengesizliğinin model performansı üzerindeki etkisini değerlendirmek amacıyla algoritmalar iki farklı deneysel senaryo altında test edilmiştir. İlk senaryoda herhangi bir SMOTE tabanlı ön işleme uygulanmadan modellerin performansları değerlendirilmiştir. İkinci senaryoda ise veri setine KMeansSMOTE ön işleme yöntemi uygulanarak aynı modeller yeniden eğitilmiş ve performansları karşılaştırılmıştır. Her iki deneysel durumda da modeller; kesinlik, duyarlılık, F1-skoru, doğruluk ve ROC-AUC ölçütleri kullanılarak değerlendirilmiştir.

SMOTE ön işlemi uygulanmadan gerçekleştirilen deneylerde, tek başına XGBoost modeli %83,5 doğruluk, kesinlik, duyarlılık ve F1-skoru değerlerine ulaşmıştır. XGBoost + CatBoost ve XGBoost + ExtraTrees modellerinde bu dört performans ölçütü

%82,4 olarak elde edilmiştir. XGBoost + ExtraTrees modelinin ROC-AUC değeri %90,5, XGBoost + CatBoost + ExtraTrees modelinin ise %91,8 olarak belirlenmiştir. Bu sonuçlar, özellikle topluluk tabanlı modellerin sınıfları ayırt etme performansının yüksek olduğunu göstermektedir.

İkinci deneysel senaryoda, veri setine KMeansSMOTE ön işlemi uygulanmıştır. Ön işleme sonrasında XGBoost modelinin doğruluk, kesinlik, duyarlılık ve F1-skoru değerleri %85'e yükselmiştir. XGBoost + CatBoost ve XGBoost + ExtraTrees modellerinde aynı performans ölçütleri %86 olarak elde edilmiştir. XGBoost + CatBoost + ExtraTrees modeli ise %87 doğruluk, kesinlik, duyarlılık ve F1-skoru ile deneylerdeki en yüksek değerleri sağlamıştır. ROC-AUC açısından XGBoost + ExtraTrees modeli %92,4 ile en yüksek değere ulaşırken, XGBoost + CatBoost + ExtraTrees modelinde bu değer %91,8 olarak ölçülmüştür.

Deneysel sonuçlar iki senaryo birlikte değerlendirildiğinde, KMeansSMOTE ön işleminin tüm modellerde temel sınıflandırma performansını artırdığı görülmüştür. Özellikle XGBoost + CatBoost + ExtraTrees modelinde doğruluk ve F1-skorunun %82,4 seviyesinden %87'ye yükselmesi, ön işleme adımının model performansı üzerindeki olumlu etkisini ortaya koymaktadır. Benzer şekilde XGBoost + ExtraTrees modelinin ROC-AUC değerinin %90,5'ten %92,4'e yükselmesi, KMeansSMOTE uygulamasının modelin sınıfları ayırt etme kapasitesini de desteklediğini göstermektedir.

Bu deneysel çalışma sonucunda, KMeansSMOTE uygulanmış modellerin uygulanmamış modellere kıyasla genel olarak daha yüksek performans gösterdiği belirlenmiştir. Bununla birlikte, farklı performans ölçütlerinde en başarılı modellerin değişiklik göstermesi nedeniyle model başarısının tek bir değerlendirme ölçütüne bağlı olarak ele alınmaması gerektiği görülmüştür.

Model Performans Sonuçları

Çalışmada 4 farklı model tasarlanmıştır:

1. modelin eğitimi, sadece XGB Sınıflandırıcısı kullanılarak gerçekleştirilmiştir.
2. modelin eğitimi, XGB Sınıflandırıcısı ve CatBoost Sınıflandırıcısının sırasıyla %40 ve %60 ağırlıklarla katkıda bulunduğu bir ağırlıklı oylama (weighted voting) yaklaşımı kullanılarak gerçekleştirilmiştir. Bu doğrultuda, nihai sınıflandırma kararı, her iki sınıflandırıcının tahminlerinin belirlenen ağırlıklar doğrultusunda birleştirilmesiyle elde edilmiştir.
3. modelin eğitimi, XGB Sınıflandırıcısı ve Extra Trees Sınıflandırıcısının sırasıyla %60 ve %40 ağırlıklarla katkıda bulunduğu bir ağırlıklı oylama (weighted voting) yaklaşımı kullanılarak gerçekleştirilmiştir. Bu doğrultuda, nihai sınıflandırma kararı, her iki sınıflandırıcının tahminlerinin belirlenen ağırlıklar doğrultusunda birleştirilmesiyle elde edilmiştir.
4. modelin eğitimi, XGB Sınıflandırıcısı %40, CatBoost Sınıflandırıcı %35 ve Extra Trees Sınıflandırıcısının %25 ağırlıklarla katkıda bulunduğu bir ağırlıklı oylama (weighted voting) yaklaşımı kullanılarak gerçekleştirilmiştir. Bu doğrultuda, nihai sınıflandırma kararı, her üç sınıflandırıcının tahminlerinin belirlenen ağırlıklar doğrultusunda birleştirilmesiyle elde edilmiştir.

Çalışma kapsamında geliştirilen modellerin performansları, SMOTE tabanlı ön işleme uygulanmadan ve KMeansSMOTE ön işlemi uygulandıktan sonra olmak üzere iki farklı durumda değerlendirilmiştir. Modellerin performanslarının

karşılaştırılmasında doğruluk, kesinlik, duyarlılık, F1-skoru ve ROC-AUC ölçütleri kullanılmıştır.

SMOTE ön işlemi uygulanmadan elde edilen model performansları Tablo 1'de verilmiştir. Tablo 1 incelendiğinde, XGBoost modelinin doğruluk, kesinlik, duyarlılık ve F1-skoru açısından %83,5 değerine ulaşarak bu ölçütlerde en yüksek performansı gösterdiği görülmektedir. XGBoost + CatBoost ve XGBoost + ExtraTrees modellerinde ise söz konusu dört performans ölçütü %82,4 olarak aynı performans elde edilmiştir. XGBoost + CatBoost + ExtraTrees modeli de doğruluk, kesinlik, duyarlılık ve F1-skoru bakımından %82,4 değerine sahiptir.

ROC-AUC sonuçları incelendiğinde ise modeller arasındaki sıralamanın farklılaştığı görülmektedir. XGBoost modelinde ROC-AUC değeri %83,5 iken, XGBoost + CatBoost modelinde ROC-AUC değeri %82,4, XGBoost + ExtraTrees modelinde %90,5 ve XGBoost + CatBoost + ExtraTrees modelinde %91,8 olarak elde edilmiştir. Böylece SMOTE ön işlemi uygulanmayan deneylerde en yüksek ROC-AUC değeri XGBoost + CatBoost + ExtraTrees modelinde elde edilmiştir. Tablo1 genel olarak değerlendirildiğinde, tekil XGBoost modelinin temel sınıflandırma ölçütlerinde daha yüksek değerler sağladığı, topluluk modellerinin ise ROC-AUC açısından daha yüksek performans gösterdiği belirlenmiştir.

KMeansSMOTE ön işlemi sonrasında elde edilen model performansları Tablo 2'de sunulmuştur. Ön işleme sonrasında XGBoost modelinin doğruluk, kesinlik, duyarlılık ve F1-skoru değerleri %85 olarak belirlenmiştir. XGBoost + CatBoost ve XGBoost + ExtraTrees modellerinde bu değerler %86'ya yükselirken, XGBoost + CatBoost + ExtraTrees modeli %87 ile en yüksek değerleri elde etmiştir.

Tablo 2'deki ROC-AUC değerleri değerlendirildiğinde, XGBoost modeli için %85 ROC-AUC değeri ile en düşük seviyede

kaydedilmişken, XGBoost + ExtraTrees modelinin %92,4 ile en yüksek başarı oranını göstermektedir. XGBoost + CatBoost modelinin ROC-AUC değeri ise %86 olarak elde edilmiştir. XGBoost + CatBoost + ExtraTrees modelinde ROC-AUC değeri %91,8 olarak belirlenmiştir.

Tablo 1 ve Tablo 2 birlikte değerlendirildiğinde, KMeansSMOTE ön işlemi sonrasında doğruluk, kesinlik, duyarlılık ve F1-skoru değerlerinde tüm modeller açısından artış meydana geldiği görülmektedir. Özellikle XGBoost + CatBoost + ExtraTrees modelinde bu ölçütlerin %82,4'ten %87'ye yükselmesi dikkat çekmektedir. Bunun yanında XGBoost + ExtraTrees modelinin ROC-AUC değerinin %90,5'ten %92,4'e yükseldiği görülmektedir. Elde edilen bu sonuçlar, KMeansSMOTE ön işleminin modellerin performans ölçütleri üzerinde olumlu yönde bir değişim oluşturduğunu ortaya koymaktadır.

Tablo 1. KMeansSmote ön işlemi uygulanmadan önce Algoritma Performans Sonuçları

Model	Doğruluk	Kesinlik	Duyarlılık	F1-Skoru	ROC-AUC
XGBoost	%83,5	%83,5	%83,5	%83,5	%83,5
XGBoost + CatBoost	%82,4	%82,4	%82,4	%82,4	%82,4
XGBoost + ExtraTrees	%82,4	%82,4	%82,4	%82,4	%90,5
XGBoost + CatBoost + ExtraTrees	%82,4	%82,4	%82,4	%82,4	%91,8

Tablo 2. KMeansSmote ön işlemi gerçekleştirildikten sonra Algoritma Performans Sonuçları

Model	Doğruluk	Kesinlik	Duyarlılık	F1-Skoru	ROC-AUC
XGBoost	%85	%85	%85	%85	%85
XGBoost + CatBoost	%86	%86	%86	%86	%86
XGBoost + ExtraTrees	%86	%86	%86	%86	%92,4
XGBoost + CatBoost + ExtraTrees	%87	%87	%87	%87	%91,8

Sonuç ve Tartışma

Bu çalışmada, kalp krizi riski taşıyan kişileri etkili bir şekilde tespit edebilen, güvenilir ve doğru bir tahmin modeli geliştirildi. Bireylerde kalp krizi riskinin tahmin edilmesine yönelik makine öğrenmesi tabanlı bir sınıflandırma yaklaşımı geliştirilmiş ve farklı algoritmaların tahmin performansları karşılaştırılmıştır. Çalışmanın temel amacı, kalp krizi ile ilişkili sınıflandırma problemlerinde yüksek tahmin başarısı sağlayabilecek uygun model yapısının belirlenmesi ve sınıf dengesizliğinin model performansı üzerindeki etkisinin ortaya konulmasıdır. Bu doğrultuda XGBoost, CatBoost ve ExtraTrees algoritmaları tekil ve topluluk tabanlı yapılar içerisinde değerlendirilmiş, ayrıca KMeansSMOTE yöntemi kullanılarak veri dengesizliğinin giderilmesinin tahmin performansına katkısı incelenmiştir.

Elde edilen sonuçlar, sınıf dağılımının dengelenmesinin kalp krizi tahmininde kullanılan makine öğrenmesi modellerinin performansı üzerinde olumlu bir etkiye sahip olduğunu göstermektedir. KMeansSMOTE ön işlemi sonrasında modellerin doğruluk, kesinlik, duyarlılık, F1-skoru ve ROC-AUC değerlerinde

genel olarak artış meydana gelmiştir. Bu durum, sınıf dengesizliğinin giderilmesiyle modellerin kalp krizi görülen ve görülmeyen bireyleri daha dengeli biçimde sınıflandırabildiğini düşündürmektedir. Özellikle sağlık alanındaki sınıflandırma problemlerinde yalnızca genel doğruluk oranının yüksek olması yeterli olmayabileceğinden, bu performans artışı klinik açıdan önemli bir bulgu olarak değerlendirilebilir.

Kalp krizi tahmini açısından duyarlılık ölçütü özel bir öneme sahiptir. Çünkü kalp krizi riski taşıyan bir bireyin düşük riskli olarak sınıflandırılması, yanlış negatif bir sonuç oluşturmakta ve potansiyel olarak önemli bir risk doğurabilmektedir. Bu nedenle modelin risk taşıyan bireyleri doğru biçimde belirleyebilme kapasitesinin yüksek olması, tahmin sisteminin kullanılabilirliği açısından önemlidir. KMeansSMOTE sonrasında duyarlılık ve F1-skorunda gözlenen iyileşmeler, modelin özellikle sınıflar arasındaki dengesizliğin olumsuz etkisini azaltarak daha dengeli tahminler gerçekleştirebildiğini göstermektedir.

Çalışmada kullanılan topluluk öğrenmesi yaklaşımlarının başarılı sonuçlar vermesi de dikkat çekici bir bulgudur. XGBoost, CatBoost ve ExtraTrees algoritmalarının farklı öğrenme stratejilerine sahip olması, bu algoritmaların birlikte kullanılmasının modelin farklı veri örüntülerini yakalama kapasitesini artırmasına katkı sağlayabilmektedir. Özellikle KMeansSMOTE ile dengelenmiş veri üzerinde XGBoost + CatBoost + ExtraTrees modelinin yüksek doğruluk ve F1-skoru elde etmesi, topluluk tabanlı yaklaşımın kalp krizi tahmini açısından etkili bir alternatif olabileceğini göstermektedir.

Bununla birlikte, kalp krizi tahmini gibi sağlık alanındaki uygulamalarda model performansının yalnızca doğruluk veya F1-skoru üzerinden değerlendirilmesi yeterli değildir. Modelin sınıfları birbirinden ayırma kapasitesinin de dikkate alınması gerekmektedir. Bu bağlamda ROC-AUC değerleri, modelin farklı risk

düzeylerindeki bireyleri ayırt edebilme yeteneği hakkında tamamlayıcı bilgi sağlamaktadır. XGBoost ve ExtraTrees algoritmalarının birlikte kullanıldığı modelin yüksek ROC-AUC değerine ulaşması, bu yaklaşımın kalp krizi riski bulunan ve bulunmayan bireyleri ayırt etme konusunda güçlü bir potansiyele sahip olduğunu göstermektedir.

Genel değerlendirme sonucunda, farklı performans ölçütlerinde farklı modellerin öne çıkması, kalp krizi tahmininde "en iyi model" kavramının tek bir ölçüte göre belirlenmemesi gerektiğini ortaya koymaktadır. Genel sınıflandırma performansının öncelikli olduğu durumlarda XGBoost + CatBoost + ExtraTrees modeli öne çıkarken, sınıfları ayırt etme kapasitesinin daha önemli olduğu durumlarda XGBoost + ExtraTrees modeli dikkat çekmektedir. Özellikle sağlık uygulamalarında yanlış negatif tahminlerin oluşturabileceği riskler göz önünde bulundurulduğunda, model seçiminde duyarlılık ve ROC-AUC gibi ölçütlerin doğrulukla birlikte değerlendirilmesi daha uygun bir yaklaşım olacaktır.

Çalışmanın bir diğer önemli sonucu, KMeansSMOTE yönteminin kalp krizi tahmin modelinin performansını destekleyebileceğini göstermesidir. Sınıf dengesizliğinin giderilmesi sayesinde özellikle azınlık sınıfına ilişkin örneklerin öğrenme sürecindeki temsilinin iyileştirilebileceği ve bunun sonucunda modelin daha dengeli tahminler gerçekleştirebileceği görülmektedir. Bununla birlikte, sentetik örnekleme yöntemlerinin gerçek klinik verilerin çeşitliliğini tamamen temsil edemeyebileceği göz önünde bulundurulmalı ve elde edilen sonuçların farklı veri kümeleri üzerinde ayrıca doğrulanması gerekmektedir.

Sonuç olarak, bu çalışma kalp krizi tahmininde makine öğrenmesi ve topluluk öğrenmesi yöntemlerinin kullanılabilirliğine ilişkin olumlu bulgular ortaya koymaktadır. Özellikle KMeansSMOTE ile desteklenen modellerin genel performansındaki iyileşme, veri ön işleme aşamasının tahmin sistemlerinin başarısında

önemli bir rol oynadığını göstermektedir. Bununla birlikte, elde edilen modellerin klinik karar verme süreçlerinde doğrudan kullanılmasından önce farklı hasta gruplarını içeren bağımsız veri kümeleri üzerinde doğrulanması, modelin genellenebilirliğinin test edilmesi ve klinik açıdan anlamlı performans ölçütlerinin ayrıntılı biçimde incelenmesi gerekmektedir. Bu doğrultuda geliştirilen yaklaşımın, hekimlerin karar verme süreçlerini destekleyen yardımcı bir tahmin aracı olarak gelecekte değerlendirilebileceği düşünülmektedir.

Bu bulgular, kalp krizi riskinin erken dönemde öngörülmesi, yüksek riskli bireylerin zamanında belirlenmesi ve kişiye özgü koruyucu ve tedavi edici yaklaşımların planlanması açısından önemli klinik çıkarımlar sunmaktadır. Bunun yanı sıra, sağlık profesyonellerinin kanıta dayalı ve daha bilinçli klinik kararlar almasına katkı sağlayarak, kardiyovasküler olayların önlenmesi ve hasta sonuçlarının iyileştirilmesinde önemli bir potansiyel taşımaktadır.

Kaynakça

Ali, Z. A. (2023). eXtreme gradient boosting algorithm with machine learning: A review. *Academic Journal of Nawroz University, 12*(2), 320-334. https://doi.org/ 10.25007/ajnu.v12n2a1612

Bentéjac, C., Csörgő, A. & Martínez-Muñoz, G. A (2021). Comparative analysis of gradient boosting algorithms. *Artificial Intelligence Review, 54*, 1937–1967. https://doi.org/10.1007/s10462-020-09896-5

Chang, C. C. et al. (2022). Melanoma detection using XGB classifier combined with feature extraction and K-means SMOTE techniques. *Diagnostics, 12*(7), 1747. https://doi.org/10.3390/diagnostics12071747

Feng, M. W. et al. (2024). Enhanced heart attack prediction using extreme gradient boosting. *Journal of Theory and Practice of Engineering Science, 4*(04), 9-16. https://doi.org/10.53469/jtpes.2024.04(04).02

Hancock, J. T. & Khoshgoftaar, T. M. (2020). CatBoost for big data: an interdisciplinary review: *Journal of big data, 7*(1), 1–45. https://doi.org/10.1186/s40537-020-00369-8

Izonin, I. T., Tkachenko, R., Shakhovska, N., Ilchyshyn, B., & Singh, K. K.(2022). A two-step data normalization approach for improving classification accuracy in the medical diagnosis domain. *Mathematics, 10*(11), 1942. https://doi.org/10.3390/math10111942

Ke, G. et al. (2017). Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems, 30* (NIPS 2017), 3146–3154.

Puri, A. , & Kumar Gupta, M. (2022). Improved hybrid bag-boost ensemble with K-means-SMOTE–ENN technique for

handling noisy class imbalanced data. The Computer Journal, 65(1), 124-138. https://doi.org/10.1093/comjnl/bxab039

Sun, L. , Hu, N., Ye, Y., Tan, W., Wu, M., Wang, X., & Huang, Z. (2022). Ensemble stacking rockburst prediction model based on Yeo–Johnson, K-means SMOTE, and optimal rockburst feature dimension determination. *Scientific Reports, 12*, 15352. https://doi.org/10.1038/s41598-022-19669-5

Wei, X. , Rao, C., Xiao, X., Chen, L., & Goh, M. (2023). Risk assessment of cardiovascular disease based on SOLSSA-CatBoost model. *Expert systems with applications, 219*, 119648. https://doi.org/10.1016/j.eswa.2023.119648

World Health Organization. (2025, July 31). *Cardiovascular diseases (CVDs).* https://www.who.int/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds)

Yasmeen, R., Khan, L., & Choi, A. (2025). Heart disease prediction using hybrid TabNet architecture with stacked ensemble learning. *Frontiers in Physiology, 16*, 1665128. https://doi.org/10.3389/fphys.2025.1665128

Yousefi, S., Yin, S., & Alfarizi, M. G. (2023). Intelligent fault diagnosis of manufacturing processes using extra tree classification algorithm and feature selection strategies. *IEEE Open Journal of the Industrial Electronics Society, 4*, 618-628. https://doi.org/10.1109/OJIES.2023.3334429


BİDGE