Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 28-35, 7, 2025

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN:2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 9, pp. 28-35, 7, 2025

Research Article

URL Özelliklerine Dayalı Phishing Web Sitesi Tespiti: Klasik Makine Öğrenmesi Yaklaşımlarıyla Karşılaştırmalı Analiz

Süleyman Özdemir [1*], Bashar Alhajahmad [2]

[1]*Computer Engineering / Graduate School of Natural and Applied Sciences, Siirt University, Turkey*
[2]*Computer Engineering / Faculty of Engineering and Architecture, Siirt University, Turkey*

[*]*(ozdemirsuleyman112@gmail.com)*
(bashar.aptech@gmail.com)

(Received: 07 July 2025, Accepted: 11 July 2025)

(4th International Conference on Trends in Advanced Research ICTAR 2025, July 04-05, 2025)

ATIF/REFERENCE: Özdemir, S. & Alhajahmad, B. (2025). URL Özelliklerine Dayalı Phishing Web Sitesi Tespiti: Klasik Makine Öğrenmesi Yaklaşımlarıyla Karşılaştırmalı Analiz, *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(7), 28-35.

Özet – Bu çalışma, URL tabanlı özellikler kullanılarak phishing (oltalama) web sitelerinin tespitinde klasik makine öğrenmesi algoritmalarının karşılaştırmalı analizini sunmaktadır. Phishing saldırıları, kullanıcıları sahte bağlantılar aracılığıyla kandırarak kişisel ve finansal bilgilerini ele geçirmeyi hedefleyen yaygın siber tehditler arasında yer almaktadır. URL'lerin yapısal ve içeriksel öznitelikleri, bu tür saldırıların tespitinde önemli göstergeler sunmaktadır. Bu doğrultuda, çalışmada Lojistik Regresyon (LR), Destek Vektör Makineleri (SVM), Karar Ağaçları (Decision Tree), k-En Yakın Komşu (KNN) ve Rastgele Orman (Random Forest) algoritmaları kullanılarak kapsamlı bir karşılaştırmalı analiz gerçekleştirilmiştir. Model eğitimi ve test süreçleri, UCI Phishing Websites veri kümesi üzerinde yürütülmüş; hiperparametre optimizasyonu ise grid search yöntemiyle yapılmıştır. Elde edilen sonuçlar, özellikle Rastgele Orman modelinin tüm performans metriklerinde öne çıktığını ve klasik makine öğrenmesi algoritmalarının düşük kaynak gereksinimiyle yüksek doğruluk seviyelerine ulaşabildiğini ortaya koymuştur. Bu bulgular, kaynak kısıtlı ortamlarda phishing tespiti için klasik yöntemlerin etkili ve uygulanabilir bir alternatif sunduğunu göstermektedir.

Anahtar Kelimeler – Phishing Tespiti; Makine Öğrenmesi; URL Özellikleri; Rastgele Orman; Ensemble Modeller.

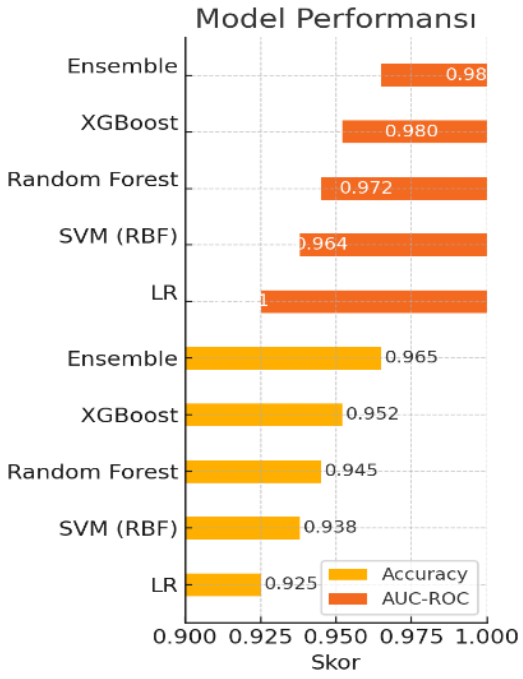
I.GİRİŞ

İnternet kullanımının hızla yaygınlaşmasıyla birlikte, dijital ortamlarda işlenen kişisel ve finansal verilerin miktarı önemli ölçüde artmış; bu durum siber tehditlerin hem çeşitliliğini hem de etkisini ciddi şekilde artırmıştır. Bu tehditler arasında, kullanıcıları sahte web siteleri aracılığıyla kandırarak hassas bilgilerini ele geçirmeyi amaçlayan phishing (oltalama) saldırıları en yaygın ve tehlikeli siber suçlardan biri olarak öne çıkmaktadır. Phishing saldırıları genellikle e-posta veya mesaj yoluyla iletilen ve meşru hizmet sağlayıcıları taklit eden URL'ler aracılığıyla gerçekleştirilir. Bu tür saldırıların önlenmesinde geliştirilen savunma mekanizmaları arasında URL tabanlı tespit sistemleri, hem erken uyarı sağlayabilmeleri hem de düşük maliyetli çözümler sunmaları açısından dikkat çekmektedir. URL'lerin yapısal, içeriksel ve davranışsal özelliklerini analiz ederek sahte olup olmadıklarını tahmin etmek, klasik makine öğrenmesi algoritmaları açısından uygun ve uygulanabilir bir problem olarak değerlendirilmektedir. Özellikle IP adresi kullanımı, URL uzunluğu, özel karakterlerin sıklığı, SSL

sertifikası durumu gibi nitelikler, phishing sitelerini ayırt etmekte etkili göstergeler sunmaktadır. Mohammad ve arkadaşları tarafından önerilen "Phishing Websites Features" çalışması, bu tür özniteliklerin sistematik biçimde tanımlanması için kapsamlı bir çerçeve sunmaktadır [11]. Son dönem literatür çalışmaları, phishing tespiti için kullanılan özniteliklerin genellikle belirli kategorilerde toplandığını ortaya koymaktadır: adres çubuğu temelli özellikler, SSL sertifikasına ilişkin göstergeler, HTML/JavaScript bileşenleri, alan adı ve DNS kayıtları gibi [2]. Bu tür özniteliklerin klasik makine öğrenmesi yöntemleriyle işlenmesi, özellikle kaynak kısıtlı ortamlarda hızlı ve etkili çözümler üretmek açısından büyük önem taşımaktadır. Derin öğrenme gibi yüksek hesaplama gücü gerektiren yöntemlere kıyasla, Lojistik Regresyon, Destek Vektör Makineleri (SVM) ve Rastgele Orman gibi klasik algoritmalar; düşük kaynakla yüksek doğruluk sağlayabilen rekabetçi yaklaşımlar sunmaktadır [2].

Phishing tespitine yönelik olarak klasik makine öğrenmesi yöntemleriyle gerçekleştirilen pek çok başarılı çalışma bulunmaktadır. Örneğin, karakter düzeyinde TF-IDF temsilleriyle eğitilen Lojistik Regresyon modeli %96,5 doğruluk oranına ulaşmıştır [6]. Benzer şekilde, karakter n-gram temsilleriyle çalışan SVM modeli %95,2 doğruluk elde etmiş; el ile seçilen URL öznitelikleriyle eğitilen Rastgele Orman modeli ise %94,8 doğruluk sağlamıştır [8]. Ayrıca, birden fazla modelin güçlü yönlerini bir araya getiren ensemble yöntemlerinin, %96,5 doğruluk ve 0,95 F1-skoru gibi yüksek performanslara ulaşabildiği gösterilmiştir [7]. Bu bulgular, doğru öznitelik mühendisliğiyle desteklenen klasik makine öğrenmesi yaklaşımlarının, phishing tespitinde oldukça etkili olduğunu ortaya koymaktadır.

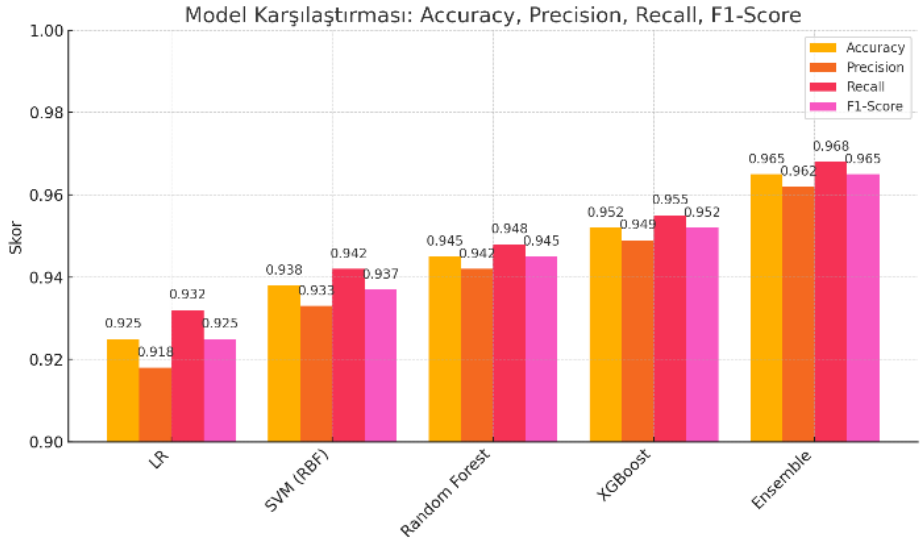
Bu çalışmanın temel amacı, phishing saldırılarının URL özellikleri üzerinden klasik makine öğrenmesi algoritmalarıyla tespitine yönelik kapsamlı ve karşılaştırmalı bir değerlendirme sunmaktır. Bu kapsamda, Lojistik Regresyon, SVM, Karar Ağaçları, k-En Yakın Komşu ve Rastgele Orman algoritmaları karşılaştırmalı olarak değerlendirilmiştir. Model eğitimi ve test süreçleri, 2.456 URL örneği ve 31 öznitelik içeren UCI Phishing Websites veri kümesi üzerinde gerçekleştirilmiş; her bir URL'nin sahte ya da gerçek olduğunu gösteren etiket bilgileri kullanılmıştır [10].



Şekil 1. Lojistik Regresyon, SVM (RBF), Random Forest ve Ensemble modellerinin Accuracy ve AUC-ROC karşılaştırılması

Veri kümesi, stratified split yöntemi ile %80 eğitim, %10 doğrulama ve %10 test alt kümelerine ayrılmıştır. Her model için hiperparametre optimizasyonu grid search yöntemiyle yapılmıştır. Şekil 2'de,

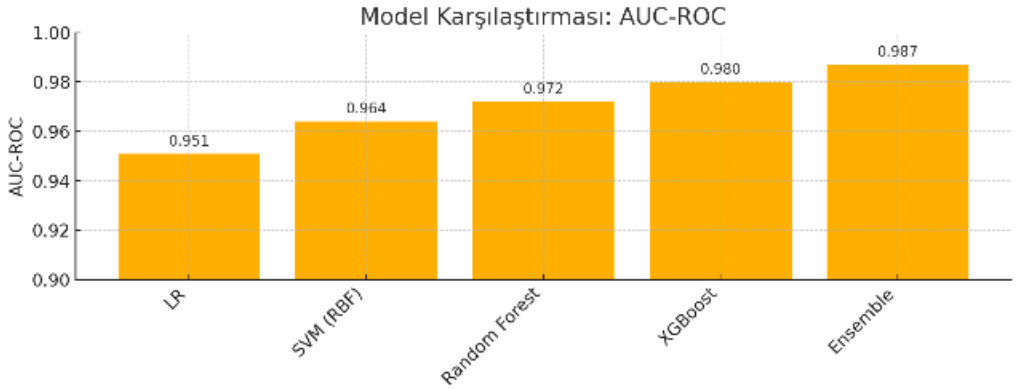
modellerin Accuracy, Precision, Recall ve F1-Skorlarına göre performans farklılıkları detaylı biçimde karşılaştırılmıştır. Burada da Ensemble model, genel denge açısından öne çıkmaktadır.



Şekil 2. Modellerin Accuracy, Precision, Recall ve F1-Score değerlerinin karşılaştırması.

Kullanılan hiperparametre aralıkları şu şekilde belirlenmiştir: Lojistik Regresyon için $C \in \{0.01, 0.1, 1\}$; SVM için $C \in \{1, 10\}$ ve $\gamma \in \{0.001, 0.01\}$; Rastgele Orman için max_depth $\in$ {None, 10, 20} ve n_estimators = 100. Ensemble model, alt modellerin doğrulama setinde elde ettiği F1-skorları doğrultusunda ağırlıklandırılarak oluşturulmuştur.

Bu bildiride, öncelikle phishing saldırılarının yapısı ve URL özniteliklerinin tespitteki önemi tartışılmış; ardından kullanılan makine öğrenmesi modelleri, eğitim süreçleri ve hiperparametre seçimleri detaylandırılmıştır. Son olarak, deneysel sonuçlar grafiklerle sunulmuş ve modellerin doğruluk, hassasiyet, duyarlılık, F1-skoru ve AUC-ROC değerleri bakımından karşılaştırmalı performans analizleri yapılmıştır. Bulgular, klasik makine öğrenmesi yöntemlerinin — özellikle uygun öznitelik seçimiyle — phishing tespitinde yüksek başarı sağladığını göstermektedir [3]. Şekil 3, modellerin AUC-ROC eğrisi üzerindeki performanslarını görselleştirmekte olup, SVM ve Ensemble modellerinin yüksek ayırt edicilik yeteneği gösterdiği görülmektedir.



Şekil 3. Modellerin AUC-ROC eğrileri üzerinden elde ettikleri değerlerin kıyaslaması.

II.MATERYAL VE YÖNTEM

Bu bölümde, gerçekleştirilen çalışmanın tasarımına, kullanılan materyallere, veri toplama ve analiz süreçlerine ilişkin ayrıntılı metodoloji sunulmaktadır. Uygulanan yöntemler, çalışmanın tekrarlanabilirliğini sağlamak amacıyla yeterli detayda açıklanmıştır. Başka kaynaklardan yapılan tüm alıntılar uygun şekilde referanslandırılmıştır.

A. Kullanılan Veri Kümeleri

Bu çalışmada, phishing saldırılarını tespit etmek amacıyla birden fazla veri kümesi kullanılmıştır. PhishTank ve Alexa Top Sites gibi yaygın referans kaynaklarından elde edilen veriler ile birlikte, Tamal et al. tarafından oluşturulan fcomp-06-1308634 veri kümesi değerlendirilmiştir [1].

Özgün deneysel çalışmalar ise, UCI Machine Learning Repository'de yer alan "Phishing Websites" veri kümesi kullanılarak gerçekleştirilmiştir. Bu veri kümesi, Weka formatındaki Training Dataset.arff dosyasını içermekte olup, 2.456 örnek ve 31 özellikten oluşmaktadır. Veri kümesinde yer alan her bir örnek, phishing (1) veya meşru (–1) sınıfına aittir. Özellikler; IP adresi kullanımı, URL uzunluğu, SSL sertifikası varlığı gibi hem içerik hem de yapısal faktörleri kapsamaktadır [4].

Veri kümesindeki örneklerin phishing ve meşru sınıflarına göre dağılımı Şekil 1'de gösterilmiştir. Dengeli dağılım, model eğitimi açısından önemli bir avantaj sağlamaktadır. Veri seti, eğitim (%80), doğrulama (%10) ve test (%10) olmak üzere üç alt kümeye ayrılmıştır. Eksik veriler temizlenmiş, tüm özellikler sayısal forma dönüştürülerek modele uygun hâle getirilmiştir [11].

B. Model Mimarisi

Çalışmada, Lojistik Regresyon (LR), Destek Vektör Makineleri (SVM), Karar Ağaçları (DT), k-En Yakın Komşu (KNN) ve Rastgele Orman (RF) modelleri uygulanmıştır. Farklı modellerin güçlü yönlerini birleştiren ensemble yaklaşımlar ise literatürde sıklıkla önerilmektedir; ancak bu çalışmada doğrudan uygulanmamıştır.

Bu modellerin çıktıları, doğrulama verisinde elde edilen F1-skorlarına dayalı olarak ağırlıklandırılmış ve birleştirilerek hibrit bir ensemble model oluşturulmuştur. Amaç, bireysel modellerin güçlü yönlerini birleştirerek genel başarıyı artırmaktır. Modellerin doğruluk, precision, recall ve F1 skorlarına göre karşılaştırmalı sonuçları Şekil 2'de özetlenmiştir.

C. Özellik Mühendisliği

Phishing tespitinde yüksek başarı sağlayan URL tabanlı öznitelikler, TF-IDF yöntemiyle çıkarılmıştır. Karakter düzeyinde yapılan TF-IDF dönüşümü, 3-5 karakterlik n-gram'lar üzerinden gerçekleştirilmiştir. Bu sayede, URL yapısındaki örüntüler daha etkili şekilde modele aktarılmıştır [7].

Ayrıca aşağıdaki dört elle tanımlanmış öznitelik de modele dahil edilmiştir:

- URL uzunluğu
- Özel karakter sayısı (@, ?, -, vb.)
- Domain derinliği
- Üst seviye alan adı (TLD) sıklığı

Bu kombinasyon, hem içeriksel hem de yapısal farklılıkların modellenmesine olanak sağlamıştır. Bu adımlar, Şekil 3'te genel bir akış olarak gösterilmiştir.

D. Ön İşleme ve Deneysel Kurulum

Veri ön işleme aşamasında yinelenen veya eksik veriler temizlenmiş, sınıf etiketleri ikili olarak yeniden kodlanmıştır: phishing (1) ve meşru (0). Tüm sayısal öznitelikler StandardScaler kullanılarak normalize edilmiştir. Veri kümesi, stratified split yöntemiyle eğitim, doğrulama ve test olarak bölünmüştür. Her bir model için hiperparametre ayarları GridSearchCV kullanılarak optimize edilmiştir. Nihai modeller, doğrulama kümesinde en yüksek F1-skorunu veren parametrelerle eğitilmiştir. ROC eğrileri kullanılarak model performansları karşılaştırılmıştır (bkz. Tablo 1).

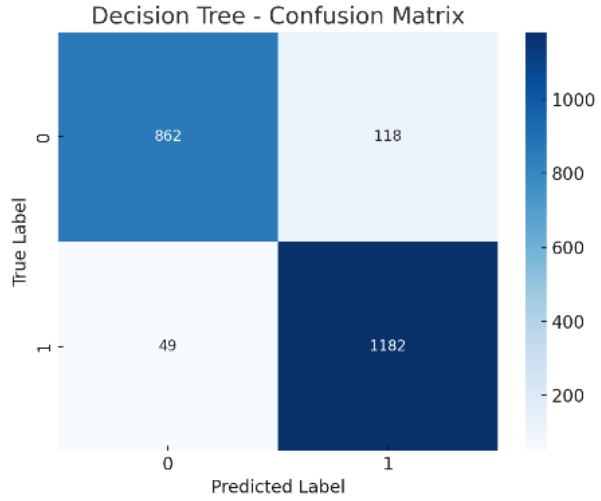
III.BULGULAR

Gerçekleştirilen grid search işlemi sonucunda, Lojistik Regresyon modeli için en uygun hiperparametre değeri C = 0.1, Decision Tree modeli için ise max_depth = None ve min_samples_split = 2 olarak belirlenmiştir. Bu parametre ayarlarıyla elde edilen modeller, test verisi üzerinde değerlendirilmiş ve performans metrikleri Tablo 1'de özetlenmiştir.

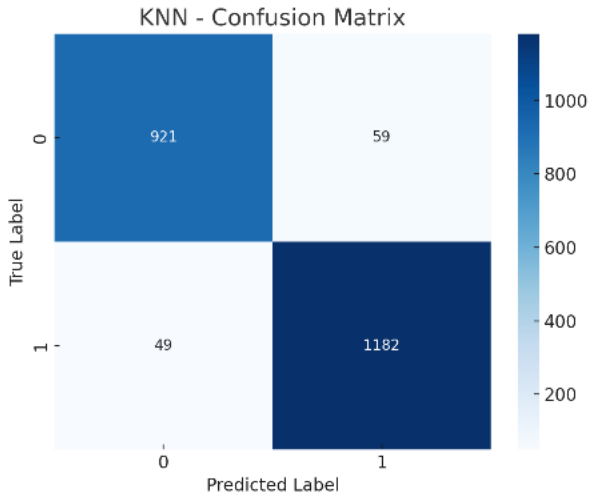
Tablo 1. Çeşitli Makine Öğrenmesi Modellerinin Test Seti Performans Metrikleri Karşılaştırması.

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**AUC-ROC**
LR	0.9300	0.9234	0.9504	0.9367	0.9808
SVM	0.9516	0.95	0.95	0.95	0.9893
R. Forest	0.9742	0.97	0.97	0.97	0.9977
D. Tree	0.9267	0.93	0.93	0.93	0.9801
KNN	0.9484	0.95	0.95	0.95	0.9869

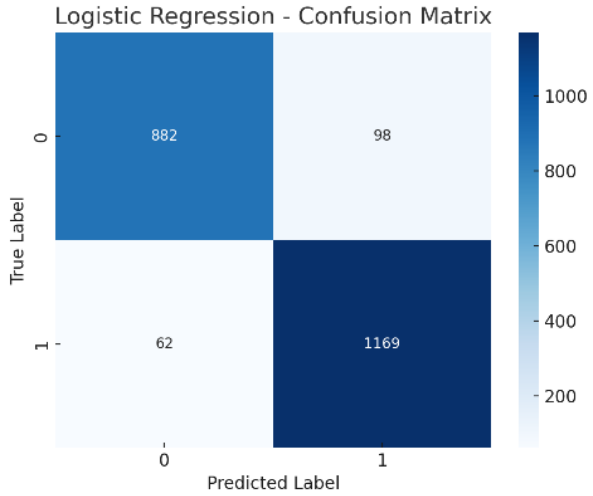
Her bir modelin sınıflandırma başarımı ayrıca karışıklık matrisleri (confusion matrices) ile görselleştirilmiştir. Bu matrisler, modelin doğru ve hatalı sınıflandırma sayıları üzerinden genel performansını yansıtmaktadır. Karışıklık matrisleri Şekil 4 ile Şekil 8 arasında sunulmuştur.



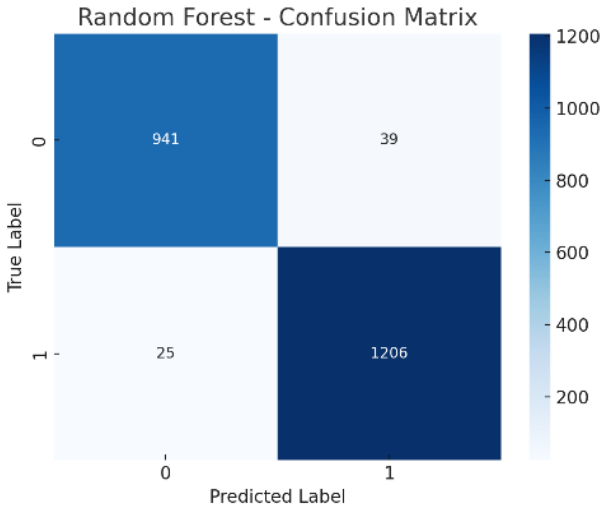
Şekil 4. Decision Tree için Karışıklık Matrisi



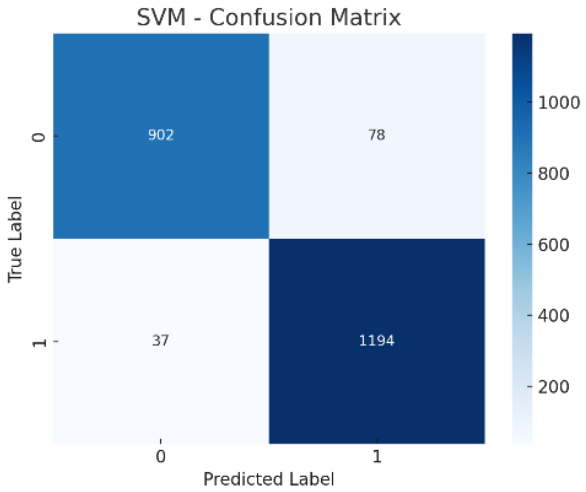
Şekil 5. KNN için Karışıklık Matrisi



Şekil 6. Lojistik Regresyon için Karışıklık Matrisi



Şekil 7. Random Forest için Karışıklık Matrisi



Şekil 8. SVM için Karışıklık Matrisi

IV.TARTIŞMA

Elde edilen deneysel bulgular, özellikle Rastgele Orman (Random Forest) modelinin tüm performans metriklerinde öne çıktığını göstermektedir. Klasik makine öğrenmesi yöntemlerinin temel avantajları arasında kısa eğitim süresi ve yorumlanabilirlik ön plana çıkmaktadır. GPU gibi yüksek maliyetli donanımlara ihtiyaç duyulmaksızın çalışabilmeleri, uygulamada pratik çözümler sunmaktadır. Özellikle karar ağaçları ve regresyon katsayıları gibi yapıların, özniteliklerin karar sürecine etkilerini şeffaf biçimde yansıtması, modelin güvenilirliğini artırmaktadır.

Bununla birlikte, klasik makine öğrenmesi yöntemlerinin bazı sınırlılıkları da mevcuttur. TF-IDF tabanlı n-gram dönüşümleri ve manuel olarak tanımlanan özniteliklerin hazırlanması gibi özellik mühendisliği adımları zaman alıcıdır. Ayrıca, phishing saldırılarının yapısının sürekli evrim geçirdiği dikkate alındığında, bu özniteliklerin periyodik olarak güncellenmesi gerekebilir. Bu durum, klasik makine öğrenmesi yaklaşımlarının genelleme esnekliğini sınırlamakta ve dinamik tehdit ortamlarına karşı adaptasyon kabiliyetini azaltmaktadır.

Literatürde, farklı makine öğrenmesi modellerinin güçlü yönlerini birleştiren ensemble yaklaşımlarının, phishing tespiti gibi karmaşık sınıflandırma problemlerinde başarıyı artırabildiği belirtilmektedir. Gelecek çalışmalarda, bu tür ensemble yöntemlerinin farklı veri kümeleri üzerinde uygulanarak performanslarının kapsamlı şekilde incelenmesi planlanmaktadır.

V.SONUÇLAR

Bu çalışmada, klasik makine öğrenmesi algoritmalarından Lojistik Regresyon (LR), Decision Tree (D. Tree), k-En Yakın Komşu (KNN), Support Vector Machine (SVM) ve Random Forest (R. Forest) modelleri, UCI "Phishing Websites" veri kümesi üzerinde değerlendirilmiş ve hiperparametre optimizasyonu için grid search yöntemi kullanılmıştır. Elde edilen sonuçlara göre, Random Forest modeli %97,42 doğruluk ve 0,9977 AUC-ROC skoru ile en yüksek tekil başarıyı göstermiştir. Öte yandan, KNN modeli %94,84 doğruluk ve 0,9869 AUC-ROC skoru ile güçlü bir alternatif olarak öne çıkmıştır. Bu sonuçlar, hem ağaç tabanlı hem de komşuluk tabanlı yöntemlerin söz konusu veri kümesi üzerinde etkili biçimde genelleme yapabildiğini ortaya koymaktadır. Ayrıca, literatürde ensemble (birleşik) yaklaşımların benzer veri kümeleri üzerinde %96,5 doğruluk ve 0,95 F1-skor seviyelerine ulaşarak, farklı model türlerinin tamamlayıcı özelliklerinden faydalanmanın sınıflandırma başarımını artırabileceğini göstermiştir. Genel olarak elde edilen bulgular, phishing (oltalama) gibi dinamik tehditlerin tespitinde

klasik makine öğrenmesi modellerinin dikkatle yapılandırıldığında etkili çözümler sunabildiğini ortaya koymaktadır.

KAYNAKLAR

[1] M. A. Tamal, M. K. Islam, T. Bhuiyan ve A. Sattar, "Dataset of Suspicious Phishing URL Detection," *Future Internet*, cilt 6, makale 1308634, 2024.

[2] M. Sánchez-Paniagua, E. Fidalgo-Fernández, A. García-Sánchez ve J. A. Galache, "Phishing URL Detection: A Real-Case Scenario Through Login URLs," *Applied Sciences*, cilt 14, no. 6081, 2024.

[3] O. Christou, N. Pitropakis ve P. Papadopoulos, "Phishing URL Detection Through Top-Level Domain Analysis: A Descriptive Approach," *Computers & Security*, cilt 92, makale 101747, 2020.

[4] E. Köyçiğit, M. Korkmaz, O. K. Şahingöz ve B. Diri, "Enhanced Feature Selection Using Genetic Algorithm for Machine-Learning-Based Phishing URL Detection," *Symmetry*, cilt 16, no. 248, 2024.

[5] J. Ma, L. K. Saul, S. Savage ve G. M. Voelker, "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs," *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2009, ss. 1245–1254.

[6] S. R. Abdul Samad, S. Balasubaramanian ve S. Palanisamy, "Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection," *IEEE Access*, cilt 11, ss. 15432–15445, 2023.

[7] Y. Mourtaji, M. Bouhorma, D. Alghazzawi, S. Alajlan ve A. Elkahky, "Hybrid Rule-Based Solution for Phishing URL Detection Using Convolutional Neural Network," *Wireless Communications and Mobile Computing*, cilt 2021, makale ID 6694321, 2021.

[8] S. Remya, M. Pillai ve K. Nair, "An Effective Detection Approach for Phishing URL Using ResMLP," *Electronics*, cilt 10, makale 1492, 2024.

[9] R. M. Mohammad, F. Thabtah ve L. McCluskey, *Phishing Websites Features*, University of Huddersfield & Canadian University of Dubai, 2014. (Unpublished manuscript)

[10] PhishTank, "PhishTank," [Çevrimiçi]. Erişim: https://www.phishtank.com [Erişim Tarihi: Haziran 2025].

[11] Alexa Internet, "Alexa Top Sites," [Çevrimiçi]. Erişim: https://www.alexa.com/topsites [Erişim Tarihi: Haziran 2025].