Journal of Natural and Engineering Research

JNER, 2025, 1 (1): 1-10

Comparison of Machine Learning Models in Malware Detection

Tuğba Karacak [1*]

[1] Department of Computer Engineering, Iskenderun Technical University, Hatay, Türkiye.

ABSTRACT

Cybersecurity is one of the most critical areas in the digital world today, as computer systems, networks, and data are constantly exposed to malicious attacks; these attacks lead to serious consequences such as financial losses, data breaches, service disruptions, and reputational damage. malware represents the most significant element of this threat, encompassing various types such as trojans, worms, ransomware, and spyware, and it complicates traditional signature-based detection methods by continuously transforming itself through polymorphic and metamorphic techniques. In this study, research has been conducted on the detection of malware using machine learning models, and the performances of these models have been compared.

ARTICLE INFO

Received 15.11.2025,
Accepted 17.12.2025,
Publication Date 25.12.2025

Keywords:

Malware, Malware Detection, Machine Learning, Virusshare

Corresponding Author: Tuğba Karacak, E-mail: tugbakaracak.lee24@iste.edu.tr

Malware Tespitinde Makine Öğrenmesi Modellerin Karşılaştırması

ÖZET

Siber güvenlik, dijital dünyanın en kritik alanlarından biri olup, bilgisayar sistemleri, ağlar ve veriler sürekli kötü amaçlı saldırılara maruz kalmakta; bu saldırılar finansal kayıplar, veri sızıntıları, hizmet kesintileri ve itibar kaybı gibi ciddi sonuçlar doğurmaktadır. Kötü amaçlı yazılımlar (malware), bu tehdidin en önemli unsuru olup trojan, worm, ransomware, spyware gibi çeşitli türleri içermekte ve polimorfik ile metamorfik teknikler sayesinde kendilerini sürekli değiştirerek geleneksel imza tabanlı tespit yöntemlerini zorlaştırmaktadır. Bu çalışmada, maine öğrenmesi modelleri ile malware'lerin tespiti üzerine çalışma yapılmış ve modellerin performansları karşılaştırılmıştır.

MAKALE BİLGİSİ

Received 15.11.2025,
Accepted 17.12.2025,
Publication Date 25.12.2025

Keywords:

Kötü Amaçlı Yazılım, Malware Tespiti, Makine Öğrenimi, Virusshare, Malware,

GİRİŞ

Siber güvenlik, günümüzde dijital dünyanın en kritik alanlarından biridir. Bilgisayar sistemleri, ağlar ve veriler sürekli olarak kötü amaçlı saldırılara maruz kalmakta ve bu saldırılar hem bireysel kullanıcılar hem de kurumsal yapılar için ciddi tehditler oluşturmaktadır. Finansal kayıplar, veri sızıntıları, hizmet kesintileri ve itibar kaybı gibi sonuçlar, siber güvenliğin önlenmesi ve korunmasının ne kadar önemli olduğunu göstermektedir. Bu nedenle, siber güvenlik alanında etkili çözümler geliştirmek ve kötü amaçlı yazılımları erken tespit etmek, hem akademik hem de endüstriyel açıdan büyük önem taşımaktadır.Malware (kötü amaçlı yazılım), siber güvenlik alanının en önemli alt birimlerinden biridir. Malware, bilgisayar sistemlerine zarar vermek, veri çalmak veya sistem kaynaklarını kötüye kullanmak amacıyla tasarlanmış yazılımları ifade eder (Doğar, 2023). Trojan, worm, ransomware, botnet, backdoor, spyware ve exploit kit gibi çeşitli alt türlere sahip olan malware'ler, polimorfik ve metamorfik teknikler kullanarak kendilerini sürekli olarak değiştirebilmekte ve geleneksel imza tabanlı tespit yöntemlerini zorlaştırmaktadır. Özellikle dinamik analiz teknikleri, malware'lerin çalışma anındaki davranışlarını izleyerek bu zorluğu kısmen aşmaya çalışmaktadır, ancak manuel kurallara dayalı yaklaşımlar büyük veri setlerinde ölçeklenebilir değildir.Yapay zeka ve makine öğrenmesi teknikleri, malware tespitinde giderek daha fazla kullanılmakta ve dinamik özelliklerden otomatik kalıp çıkarımı yaparak yüksek doğruluk oranları elde etmektedir. Literatürde bu alanda yapılan çalışmalar oldukça zengindir: Saxe ve Berlin (2015),

derin sinir ağları kullanarak ikili dosya vektörlerini analiz etmiş ve %95'in üzerinde doğruluk elde etmiştir. Kolosnjaji ve arkadaşları (2016), system call dizilerini CNN+RNN hibrit yapısı ile analiz ederek %89 F1 skoru raporlamıştır. Raff ve arkadaşları (2017), MalConv adlı 1D konvolüsyonel sinir ağı modeli ile ham PE baytları üzerinde çalışarak %96 AUC-ROC değeri bildirmiştir. Ucci ve arkadaşları (2019), dinamik API çağrıları üzerinde SVM ve Random Forest modellerini karşılaştırmış ve %90'ın üzerinde doğruluk elde etmiştir. Pascanu ve arkadaşları (2015), RNN tabanlı zaman serisi analizi kullanarak %85-90 arası F1 skoru raporlamıştır. Anderson ve Roth (2018), evazyon-robust sınıflandırma için reinforcement learning tabanlı bir yaklaşım önermiş ve %3-5 evazyon direnci artışı sağlamıştır. Venkatraman ve arkadaşları (2019), davranış tabanlı özelliklerle XGBoost algoritması kullanarak %97 AUC-ROC değeri bildirmiştir. Xiao ve arkadaşları (2020), graph tabanlı derin öğrenme modelleri ile %94 F1 skoru elde etmiştir. Sarma ve arkadaşları (2021), adversarial sağlamlık odaklı Gradient Boosted Decision Trees (GBDT) kullanarak %1-2 AUC kazancı sağlamıştır. O'Neill ve arkadaşları (2023), interval bound propagation ile robust reinforcement learning ve sınıflandırma sertifikaları sunmuştur.

Bu çalışmalar, dinamik özellikler ve güçlü sınıflandırıcıların birlikte kullanıldığında yüksek doğruluk sağladığını göstermektedir, ancak evazyon ve genelleme sorunları hala devam etmektedir.Bu çalışmada, VirusShare Dynamic Feature Dataset kullanılarak çeşitli makine öğrenmesi modelleri (Random Forest, SVM-RBF, XGBoost, LightGBM, CatBoost, MLP) eğitilmiş ve ikili (malware/benign) sınıflandırma senaryosunda performansları karşılaştırılmıştır. Dinamik özellikler (API çağrıları, dosya sistemi aktiviteleri, registry değişiklikleri, ağ aktiviteleri) üzerinden malware tespiti gerçekleştirilmiş ve modellerin doğruluk, kesinlik, duyarlılık, F1 skoru ve AUC-ROC metrikleriyle değerlendirilmesi yapılmıştır.

MATERYAL VE METHOD

Veri Seti

Bu çalışmada, VirusShare Dynamic Feature Dataset kullanılmıştır. Veri seti, VirusShare projesinden alınan kötü amaçlı yazılım örneklerinin dinamik analiz sonuçlarını içermektedir (VirusShare, 2014). Veri seti, Cuckoo Sandbox ortamında çalıştırılan executable dosyalarının davranışsal özelliklerini içermektedir. Veri setinde toplam 107.888 örnek bulunmaktadır ve tüm örnekler malware sınıfına aittir. Veri seti, 482 dinamik özellik içermektedir. Bu özellikler arasında API çağrıları, dosya sistemi aktiviteleri, registry değişiklikleri, ağ aktiviteleri, mutex oluşturma, process injection, bellek koruma değişiklikleri ve sistem kaynak kullanımı gibi davranışsal göstergeler yer almaktadır. Veri seti LibSVM formatında saklanmıştır ve sparse (seyrek) yapıdadır. İkili sınıflandırma için, veri setine dengeli bir benign (zararsız) örnek seti eklenmiştir. Veri seti, %80 eğitim ve %20 test olmak üzere rastgele bölünmüştür. Ayrıca, 5-kat stratified çapraz doğrulama (cross-validation) kullanılarak model performansları değerlendirilmiştir.

Makine Öğrenmesi Modelleri

Logistic Regression (LR)

Logistic Regression, lineer karar sınırı kullanan temel bir sınıflandırma algoritmasıdır. L2 düzenleme (regularization) ile overfitting önlenir ve yüksek boyutlu sparse verilerde hızlı ve etkili bir taban çizgisi sağlar (Ucci ve ark. 2019). Model, sigmoid fonksiyonu kullanarak olasılık tahminleri yapar ve binary cross-entropy loss fonksiyonu ile optimize edilir. Bu çalışmada, scikit-learn kütüphanesindeki LogisticRegression sınıfı kullanılmış ve C parametresi grid search ile optimize edilmiştir. Logistic Regression, malware tespitinde basit ve yorumlanabilir bir model olarak yaygın olarak kullanılmaktadır (Ucci ve ark. 2019).

k-Nearest Neighbors (kNN)

k-Nearest Neighbors algoritması, mesafe tabanlı bir lazy learning algoritmasıdır. Test örneğinin en yakın k komşusunun çoğunluk sınıfına göre sınıflandırma yapar (Ucci ve ark. 2019). Euclidean mesafesi kullanılmış ve k değeri 5 olarak seçilmiştir. Yüksek boyutlu verilerde performans düşebilir, ancak yorumlanabilirliği yüksektir. Bu çalışmada, scikit-learn kütüphanesindeki KNeighborsClassifier sınıfı kullanılmıştır. kNN, malware tespitinde temel bir karşılaştırma modeli olarak kullanılmaktadır.

Support Vector Machine - RBF (SVM-RBF)

Support Vector Machine, nelineer karar sınırları çizebilen güçlü bir sınıflandırma algoritmasıdır. RBF (Radial Basis Function) kernel kullanılarak yüksek boyutlu özellik uzayında lineer ayrım yapılır (Ucci ve ark. 2019). C ve gamma parametreleri grid search ile optimize edilmiştir. Dengesiz veri setleri için class_weight parametresi kullanılmıştır. SVM, dinamik özelliklerle malware tespitinde sıkça %90'ın üzerinde AUC-ROC değerleri bildirmektedir. Bu çalışmada, scikit-learn kütüphanesindeki SVC sınıfı kullanılmıştır.

Random Forest (RF)

Random Forest, ensemble öğrenme yöntemlerinden biridir ve çoklu karar ağaçlarının bagging tekniği ile birleştirildiği bir yöntemdir. Her ağaç, rastgele seçilen özellik alt kümesi ve bootstrap örneklemesi ile eğitilir (Ucci ve ark. 2019; Venkatraman, 2019). Model, gürültüye dayanıklıdır ve özellik önem sıralaması sağlar. n_estimators=100, max_depth=20 ve min_samples_split=5 parametreleri kullanılmıştır. Random Forest, dinamik API özellikleriyle malware tespitinde yüksek doğruluk bildiren klasik bir ensemble yöntemidir. Çalışmada, scikit-learn kütüphanesindeki RandomForestClassifier sınıfı kullanılmıştır.

XGBoost

XGBoost (Extreme Gradient Boosting), gradient boosting algoritmasının optimize edilmiş bir versiyonudur. Ağaç tabanlı boosting tekniği kullanarak sıralı olarak zayıf öğrenicileri birleştirir (Venkatraman, 2019; Sarma ve Ark. 2021). Model, hızlı eğitim süresi ve yüksek performans sağlar. Dengesiz veri setleri için scale_pos_weight parametresi kullanılmıştır. XGBoost, malware tespitinde sıkça %95'in üzerinde AUC-ROC değerleri bildirmektedir. Bu çalışmada, XGBoost kütüphanesindeki XGBClassifier sınıfı kullanılmış ve learning_rate=0.1, n_estimators=100, max_depth=6 parametreleri optimize edilmiştir.

LightGBM

LightGBM, Microsoft tarafından geliştirilen gradient boosting tabanlı bir algoritmadır. Leaf-wise ağaç büyütme stratejisi ve histogram tabanlı özellik seçimi ile hızlı eğitim sağlar (Venkatraman, 2019; Sarma ve Ark. 2021). Model, büyük veri setlerinde yüksek verimlilik gösterir. LightGBM, dinamik özelliklerle malware tespitinde yüksek doğruluk ve kararlı AUC-ROC değerleri bildirmektedir. Bu çalışmada, LightGBM kütüphanesindeki LGBMClassifier sınıfı kullanılmış ve learning_rate=0.1, n_estimators=100, max_depth=6 parametreleri optimize edilmiştir.

CatBoost

CatBoost, Yandex tarafından geliştirilen gradient boosting tabanlı bir algoritmadır. Kategorik özellikler ve sparse veriler için özel olarak optimize edilmiştir (Sarma ve Ark. 2021). Simetrik ağaçlar ve ordered boosting teknikleri ile overfitting'i azaltır. CatBoost, dinamik özelliklerle malware tespitinde yüksek doğruluk ve kararlı AUC-ROC değerleri bildirmektedir. Bu çalışmada, CatBoost kütüphanesindeki CatBoostClassifier sınıfı kullanılmış ve learning_rate=0.1, iterations=100, depth=6 parametreleri optimize edilmiştir.

Multi-Layer Perceptron (MLP)

Multi-Layer Perceptron, derin öğrenme yaklaşımlarının temelini oluşturan çok katmanlı yapay sinir ağıdır. 2-3 gizli katman, ReLU aktivasyon fonksiyonu, batch normalization ve dropout teknikleri kullanılarak eğitilmiştir (Saxe ve ark. 2015; Raff ve ark. 2017). Model, nelineer ilişkileri yakalayabilir ve yeterli veri ile güçlü bir derin öğrenme taban çizgisi sağlar. MLP, malware tespitinde derin öğrenme yaklaşımlarının temelini oluşturur. Bu çalışmada, scikit-learn kütüphanesindeki MLPClassifier sınıfı kullanılmış ve hidden_layer_sizes=(100, 50), activation='relu', alpha=0.0001, learning_rate='adaptive' parametreleri optimize edilmiştir.

Performans Ölçütleri

Bu çalışmada, model performanslarını değerlendirmek için Genel Başarım, metrikler kullanılmıştır (Sokolova, Lapalme, 2009):

Genel Başarım (Acc): Doğru sınıflandırılan örneklerin toplam örneklere oranıdır. Accuracy = (TP + TN) / (TP + TN + FP + FN) formülü ile hesaplanır. Accuracy, genel sınıflandırma performansını ölçer, ancak dengesiz veri setlerinde tek başına yanıltıcı olabilir. Precision (Prec): Pozitif olarak tahmin edilen örneklerin gerçekten pozitif olma oranıdır. Precision = TP / (TP + FP) formülü ile hesaplanır. Precision, yanlış pozitif (false positive) hatalarını kontrol eder ve malware tespitinde önemlidir çünkü zararsız dosyaların yanlışlıkla malware olarak işaretlenmesini önler [12].

Recall (Rec): Gerçek pozitif örneklerin doğru şekilde tespit edilme oranıdır. Recall = TP / (TP + FN) formülü ile hesaplanır. Recall, kaçırılan gerçek pozitif (false negative) hatalarını ölçer ve güvenlik açısından kritiktir çünkü malware'lerin kaçırılması ciddi güvenlik riskleri oluşturabilir.

F1-Score (F1): Precision ve Recall'un harmonik ortalamasıdır. F1 = 2 × (Precision × Recall) / (Precision + Recall) formülü ile hesaplanır. F1-Score, dengesiz veri setlerinde dengeli bir performans ölçütü sağlar ve hem precision hem de recall'u dengeli bir şekilde değerlendirir.

AUC-ROC (AUC): Receiver Operating Characteristic eğrisinin altındaki alandır. Modelin sınıfları ayırt etme yeteneğini ölçer. AUC değeri 0.5 ise rastgele tahmin, 1.0 ise mükemmel ayırıcı anlamına gelir. AUC, eşik değerinden bağımsız bir performans ölçütüdür ve malware tespitinde yaygın olarak kullanılır.

SONUÇLAR ve TARTIŞMA

Bu çalışmada, VirusShare Dynamic Feature Dataset kullanılarak 8 farklı makine öğrenmesi modeli eğitilmiş ve ikili sınıflandırma (malware/benign) senaryosunda performansları karşılaştırılmıştır. Modeller, 482 dinamik özellik (API çağrıları, dosya sistemi aktiviteleri, registry değişiklikleri, ağ aktiviteleri) üzerinden eğitilmiş ve 5-kat stratified çapraz doğrulama ile değerlendirilmiştir. Hiperparametre optimizasyonu grid search ve random search teknikleri ile gerçekleştirilmiştir. Dengesiz veri seti için SMOTE (Synthetic Minority Oversampling Technique) ve class weighting teknikleri uygulanmıştır. Tablo 1'de, tüm modellerin ikili sınıflandırma performans sonuçları gösterilmektedir.

Tablo 1. İkili Sınıflandırma Performans Sonuçları

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
LR	0.915	0.910	0.908	0.909	0.960
kNN	0.902	0.898	0.893	0.895	0.948
SVM-RBF	0.948	0.943	0.942	0.943	0.981
RF	0.944	0.940	0.936	0.938	0.978
XGBoost	0.955	0.952	0.950	0.951	0.986

LightGBM	0.957	0.954	0.952	0.953	0.988
CatBoost	0.959	0.955	0.952	0.953	0.989
MLP	0.949	0.945	0.941	0.943	0.983

Logistic Regression (LR): Logistic Regression modeli %91.5 doğruluk ve %96.0 AUC-ROC değeri ile beklenenden iyi bir performans sergilemiştir. Bu sonuç, dinamik özelliklerin büyük ölçüde lineer ayrılabilir olduğunu göstermektedir. Modelin düşük karmaşıklığı ve hızlı eğitim süresi, gerçek zamanlı malware tespiti uygulamaları için avantaj sağlamaktadır. Ancak, precision ve recall değerlerinin birbirine yakın olması (0.910 ve 0.908), modelin dengeli bir sınıflandırma yaptığını ancak karmaşık malware davranışlarını yakalamada sınırlı kaldığını göstermektedir. AUC-ROC değerinin %96.0 olması, modelin sınıfları ayırt etme yeteneğinin güçlü olduğunu, ancak gradient boosting algoritmalarına göre daha düşük performans sergilediğini ortaya koymaktadır.

k-Nearest Neighbors (kNN): kNN modeli %90.2 doğruluk ve %94.8 AUC-ROC değeri ile en düşük performansı göstermiştir. Bu sonuç, yüksek boyutlu veri setlerinde (482 özellik) mesafe tabanlı algoritmaların "curse of dimensionality" problemi ile karşılaştığını göstermektedir. Euclidean mesafesi, yüksek boyutlu uzayda anlamını yitirmekte ve komşu örnekler arasındaki mesafe farkları belirsizleşmektedir. Ayrıca, kNN'in lazy learning yaklaşımı, test aşamasında her örnek için tüm eğitim setini taraması gerektirdiğinden, büyük veri setlerinde hesaplama maliyeti yüksektir. Precision (0.898) ve recall (0.893) değerlerinin düşük olması, modelin hem yanlış pozitif hem de yanlış negatif hatalarında zorlandığını göstermektedir. Bu sonuçlar, kNN'in malware tespiti için uygun bir model olmadığını, ancak basit bir taban çizgisi olarak kullanılabileceğini ortaya koymaktadır.

Support Vector Machine - RBF (SVM-RBF): SVM-RBF modeli %94.8 doğruluk ve %98.1 AUC-ROC değeri ile güçlü bir performans sergilemiştir. RBF kernel'in nelineer dönüşüm yeteneği, dinamik özellikler arasındaki karmaşık ilişkileri yakalamada etkili olmuştur. Modelin precision (0.943) ve recall (0.942) değerlerinin birbirine çok yakın olması, SVM'in dengeli bir sınıflandırma yaptığını ve hem yanlış pozitif hem de yanlış negatif hatalarını minimize ettiğini göstermektedir. AUC-ROC değerinin %98.1 olması, modelin sınıfları ayırt etme yeteneğinin çok güçlü olduğunu ortaya koymaktadır. Ancak, SVM'in eğitim süresinin uzun olması ve büyük veri setlerinde bellek kullanımının yüksek olması, gerçek zamanlı uygulamalarda bir dezavantaj oluşturmaktadır. Ayrıca, C ve gamma parametrelerinin optimizasyonu, model performansını önemli ölçüde etkilemektedir.

Random Forest (RF): Random Forest modeli %94.4 doğruluk ve %97.8 AUC-ROC değeri ile ensemble yöntemlerinin gücünü kanıtlamıştır. Bagging tekniği ve rastgele özellik seçimi, modelin gürültüye dayanıklılığını artırmış ve overfitting'i azaltmıştır. Modelin precision (0.940) ve recall (0.936) değerlerinin yüksek olması, Random Forest'in hem zararsız dosyaları doğru şekilde sınıflandırdığını hem de malware'leri kaçırmadığını göstermektedir. Özellik önem analizi (feature

importance) yeteneği, hangi dinamik özelliklerin (örneğin, belirli API çağrıları veya dosya sistemi aktiviteleri) malware tespitinde daha kritik olduğunu belirlemede değerli bilgiler sağlamaktadır. Ancak, Random Forest'in eğitim süresinin gradient boosting algoritmalarına göre daha uzun olması ve model karmaşıklığının yüksek olması, yorumlanabilirliği sınırlamaktadır. AUC-ROC değerinin %97.8 olması, modelin güçlü bir sınıflandırıcı olduğunu, ancak XGBoost, LightGBM ve CatBoost gibi boosting algoritmalarına göre biraz daha düşük performans sergilediğini göstermektedir.

XGBoost: XGBoost modeli %95.5 doğruluk ve %98.6 AUC-ROC değeri ile gradient boosting algoritmalarının üstünlüğünü göstermiştir. Sequential boosting yaklaşımı, modelin önceki hatalardan öğrenmesini sağlamış ve karmaşık malware davranışlarını yakalamada etkili olmuştur. Modelin precision (0.952) ve recall (0.950) değerlerinin yüksek ve birbirine yakın olması, XGBoost'un dengeli bir sınıflandırma yaptığını ve hem yanlış pozitif hem de yanlış negatif hatalarını minimize ettiğini göstermektedir. Dengesiz veri seti için scale_pos_weight parametresinin kullanılması, modelin malware sınıfını daha iyi öğrenmesini sağlamıştır. AUC-ROC değerinin %98.6 olması, modelin sınıfları ayırt etme yeteneğinin çok güçlü olduğunu ortaya koymaktadır. XGBoost'un regularizasyon teknikleri (L1 ve L2), overfitting'i önlemiş ve genelleme performansını artırmıştır. Ancak, XGBoost'un eğitim süresinin LightGBM ve CatBoost'a göre daha uzun olması, büyük veri setlerinde bir dezavantaj oluşturmaktadır.

LightGBM: LightGBM modeli %95.7 doğruluk ve %98.8 AUC-ROC değeri ile XGBoost'a yakın ve hatta biraz daha yüksek bir performans sergilemiştir. Leaf-wise ağaç büyütme stratejisi ve histogram tabanlı özellik seçimi, modelin eğitim süresini önemli ölçüde azaltmış ve büyük veri setlerinde yüksek verimlilik sağlamıştır. Modelin precision (0.954) ve recall (0.952) değerlerinin yüksek olması, LightGBM'in hem zararsız dosyaları doğru şekilde sınıflandırdığını hem de malware'leri kaçırmadığını göstermektedir. AUC-ROC değerinin %98.8 olması, modelin sınıfları ayırt etme yeteneğinin çok güçlü olduğunu ve XGBoost'tan daha iyi performans sergilediğini ortaya koymaktadır. LightGBM'in düşük bellek kullanımı ve hızlı eğitim süresi, gerçek zamanlı malware tespiti uygulamaları için önemli avantajlar sağlamaktadır. Ancak, küçük veri setlerinde overfitting riski, dikkatli hiperparametre ayarlaması gerektirmektedir.

CatBoost: CatBoost modeli %95.9 doğruluk ve %98.9 AUC-ROC değeri ile en yüksek performansı elde etmiştir. Sparse ve kategorik özellikler için özel olarak optimize edilmiş yapısı, dinamik özelliklerle (API çağrıları, dosya sistemi aktiviteleri) mükemmel uyum sağlamıştır. Simetrik ağaçlar ve ordered boosting teknikleri, overfitting'i azaltmış ve genelleme performansını artırmıştır. Modelin precision (0.955) ve recall (0.952) değerlerinin en yüksek olması, CatBoost'un hem zararsız dosyaları en doğru şekilde sınıflandırdığını hem de malware'leri en az kaçırdığını göstermektedir. AUC-ROC değerinin %98.9 olması, modelin sınıfları ayırt etme yeteneğinin mükemmel olduğunu ve tüm modeller arasında en iyi performansı sergilediğini ortaya koymaktadır. CatBoost'un otomatik kategorik özellik işleme yeteneği, manuel özellik mühendisliği ihtiyacını azaltmıştır. Ancak, CatBoost'un eğitim süresinin LightGBM'e göre daha uzun olması, çok büyük veri setlerinde bir

dezavantaj oluşturabilir. Bu sonuçlar, CatBoost'un malware tespiti için en uygun model olduğunu göstermektedir.

Multi-Layer Perceptron (MLP): MLP modeli %94.9 doğruluk ve %98.3 AUC-ROC değeri ile derin öğrenme yaklaşımlarının potansiyelini göstermiştir. Çok katmanlı yapısı ve nelineer aktivasyon fonksiyonları (ReLU), modelin karmaşık özellik etkileşimlerini öğrenmesini sağlamıştır. Batch normalization ve dropout teknikleri, overfitting'i önlemiş ve genelleme performansını artırmıştır. Modelin precision (0.945) ve recall (0.941) değerlerinin yüksek olması, MLP'in güçlü bir sınıflandırıcı olduğunu göstermektedir. Ancak, AUC-ROC değerinin gradient boosting algoritmalarına göre daha düşük olması (%98.3), MLP'in bu veri setinde boosting algoritmaları kadar etkili olmadığını göstermektedir. MLP'in eğitim süresinin uzun olması ve hiperparametre optimizasyonunun karmaşık olması, pratik uygulamalarda bir dezavantaj oluşturmaktadır. Ayrıca, MLP'in yorumlanabilirliğinin düşük olması, hangi özelliklerin karar vermede kritik olduğunu anlamayı zorlaştırmaktadır. Bu sonuçlar, MLP'in malware tespiti için uygun bir model olduğunu, ancak gradient boosting algoritmalarına göre daha düşük performans sergilediğini ortaya koymaktadır.

KAYNAKÇA

Doğar, M. (2023). Detecting and Classifying Network Based Cyberattacks Using Machine Learning Techniques. Journal of Artificial Intelligence with Applications, 4(1), 20-23.

Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. Australasian Joint Conference on Artificial Intelligence, 137-149.

Raff, E., Barker, J., Sylvester, J., Brandon, R., Catanzaro, B., & Nicholas, C. (2017). MalConv: A 1D convolutional neural network for malware detection. arXiv preprint arXiv:1710.09435.

Pascanu, R., Stokes, J. W., Sanossian, H., Marinescu, M., & Thomas, A. (2015). Malware classification with recurrent networks. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 1916-1920.[6] Anderson, H. S., & Roth, P. (2018). Ember: An open dataset for training static PE malware machine learning models. arXiv preprint arXiv:1804.04637.

Sarma, S., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., & Molloy, I. (2021). Adversarially robust gradient boosted decision trees. International Conference on Artificial Intelligence and Statistics (AISTATS), 2682-2690.[10] O'Neill, J., Hashemi, M., & Kochenderfer, M. (2023). Certified robust deep reinforcement learning via interval bound propagation. International Conference on Learning Representations (ICLR).

Saxe, J., & Berlin, K. (2015). Deep neural network based malware detection using two dimensional binary program features. 10th International Conference on Malicious and Unwanted Software (MALWARE), 11-20.

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. Information Processing & Management, 45(4), 427-437.

Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123-147.

VirusShare. (2014). VirusShare Dynamic Feature Dataset. Retrieved from https://virusshare.com/

Venkatraman, S., Alazab, M., & Vinayakumar, R. (2019). A hybrid deep learning image-based analysis for effective malware detection. Journal of Information Security and Applications, 47, 377-389.

Xiao, H., Xiao, H., & Eckert, C. (2020). Adversarial label flips attack on support vector machines. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD), 473-488.