Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 9, S. 90-98, 8, 2025
© Telif hakkı IJANSER'e aittir
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. 90-98, 8, 2025
Copyright © 2025 IJANSER
Research Article

Siber Tehditlerin Tanımlanmasında Model Performanslarının Karşılaştırılması: CNN, MLP ve Random Forest

Hatice Bat*, Bashar Alhajahmad*

[1]*Computer Engineering/ Faculty of Engineering and Architecture, Siirt University, Turkey*

**(haticekahraman0138@gmail.com)*
**(bashar.aptech@gmail.com)*

(Received: 25 July 2025, Accepted: 31 July 2025)

(3rd International Conference on Modern and Advanced Research ICMAR 2025, July 25-26, 2025)

ATIF/REFERENCE: Bat, H. & Alhajahmad, B. (2025). Siber Tehditlerin Tanımlanmasında Model Performanslarının Karşılaştırılması: CNN, MLP ve Random Forest, *International Journal of Advanced Natural Sciences and Engineering Researches*, 9(8), 90-98.

Özet – Siber güvenlik alanında, özellikle ağ trafiği üzerindeki anomali tespiti, artan saldırı çeşitliliği ve karmaşıklığı nedeniyle her geçen gün daha kritik hâle gelmektedir. Bu çalışma, KDDTest+ veri seti üzerinde Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP) ve Random Forest algoritmalarının anomali tespit performanslarını karşılaştırmalı olarak incelemektedir. Modeller; doğruluk oranı, F1 skoru, ROC eğrisi ve öznitelik önem değerleri gibi metrikler üzerinden değerlendirilmiştir. Random Forest modeli, %99 genel doğruluk ve yüksek F1 skorları ile öne çıkarken, özellikle **src_bytes** ve **dst_bytes** gibi veri aktarımını temsil eden öznitelikler karar verme sürecinde belirleyici olmuştur. CNN modeli %96,7 doğrulukla başarılı sonuçlar üretmiş; ancak eğitim süresi diğer modellere kıyasla daha uzun olmuştur. MLP modeli ise daha sade bir yapıya sahip olmasına rağmen %97 doğruluk ve yüksek F1 skoru ile hızlı ve etkili bir performans sergilemiştir. Sonuçlar, her üç modelin de ağ tabanlı siber saldırıların tespitinde etkili olduğunu göstermektedir. Model seçimi, uygulama alanına ve veri yapısına göre değişiklik gösterebilir. Gelecekte bu modellerin hibrit yaklaşımlarla birleştirilmesi, daha güvenli ve proaktif ağ güvenliği çözümlerine katkı sağlayabilir.

Anahtar Kelimeler – Siber Güvenlik, Anomali Tespiti, Convolutional Neural Network (CNN), MLP, Random Forest, Saldırı Tespiti.

I. GİRİŞ

Dijital ağların hızla genişlemesiyle birlikte siber tehditlerin sayısı ve çeşitliliği de artmaktadır. Bu durum, ağlarda gerçekleşen yetkisiz faaliyetlerin tespiti ve önlenmesi için daha akıllı ve uyarlanabilir çözümlerin geliştirilmesini zorunlu kılmaktadır. Bu bağlamda, **İzinsiz Giriş Tespit Sistemleri (IDS - Intrusion Detection Systems)**, geleneksel güvenlik önlemlerinin ötesine geçerek, ağ trafiğini izleme ve analiz etme yeteneğiyle siber güvenlik mimarilerinde kritik bir rol üstlenmektedir.

Geleneksel güvenlik duvarları ve antivirüs yazılımlarının aksine, IDS'ler hem bilinen saldırı kalıplarını tespit edebilir hem de öğrenme tabanlı yöntemlerle yeni ve öngörülemeyen tehditleri ortaya çıkarabilir. Ancak etkili bir IDS sisteminde aşağıdaki üç temel özellik ön plana çıkmaktadır:

- **Uyarlanabilirlik:** IDS'lerin, sürekli gelişen siber tehdit ortamına karşı güncel kalabilmesi ve sıfırıncı gün (zero-day) saldırılarını yalnızca imza tabanlı değil, davranışsal ve anomali tabanlı yöntemlerle de tespit edebilmesi gerekmektedir.

- **Ölçeklenebilirlik ve Performans:** Artan veri hacmiyle birlikte IDS sistemlerinin yüksek doğruluk oranlarını koruyarak verimli çalışması, özellikle büyük ölçekli ağlar ve bulut ortamlarında büyük önem taşımaktadır.
- **Yanlış Pozitif/Negatif Oranı:** Etkili bir IDS, hem yanlış alarmları (false positive) hem de gözden kaçan saldırıları (false negative) en aza indirerek, güvenlik operasyonlarının etkinliğini artırmalıdır [1].

Bu bağlamda, geleneksel IDS yaklaşımlarının sınırlılıklarını aşmak amacıyla **yapay zekâ (AI) temelli yöntemler**, özellikle makine öğrenmesi ve derin öğrenme tabanlı modeller, ağ güvenliği alanında öne çıkmaktadır.

Nitekim literatürde bu konuda çeşitli çalışmalar mevcuttur. Örneğin, AI2DS (Advanced Autoencoder-Guided Method for Smart Network Intrusion Detection Systems) adlı sistem, normal ağ davranışlarından sapmaları tanımlamak üzere otomatik kodlayıcı mimarisi kullanmakta ve yeniden yapılandırma hataları üzerinden uyarlanabilir eşikleme ile anomali tespiti gerçekleştirmektedir. Model, yüksek doğruluk, F1 skoru, hassasiyet ve geri çağırma değerleri ile dikkat çekmiştir [2].

Bir başka çalışmada, Wi-Fi saldırılarını tespit etmek amacıyla AWID ve AWID3 veri setleri üzerinde CNN ve MLP modelleri değerlendirilmiş; CNN modelinin, MLP'ye kıyasla daha üstün performans sergilediği görülmüştür [3]. Benzer şekilde, IoT ortamlarına yönelik bir çalışmada SICNN modeli önerilmiş ve CIC IDS2017 ile CICIoT2023 veri kümelerinde üstün başarı sağlamıştır [4]. SCADA sistemlerinde ise, eksik verilerin etkisini azaltmak amacıyla federated learning (FL) ve merkezi öğrenmeyi birleştiren hibrit öğrenme yöntemi önerilmiş, bu yöntem görünmeyen saldırıları tespit etmede başarılı sonuçlar vermiştir [5].

Bu çalışmada ise, **KDDTest+** veri seti üzerinde üç farklı makine öğrenmesi algoritması olan **Convolutional Neural Network (CNN)**, **Multi-Layer Perceptron (MLP)** ve **Random Forest** kullanılarak anomali tespiti gerçekleştirilmiştir. Modellerin doğruluk, kayıp değeri, ROC eğrisi ve F1 skoru gibi performans ölçütleri karşılaştırmalı olarak analiz edilmiştir. Elde edilen bulgular, bu modellerin ağ güvenliği uygulamalarında kullanım potansiyelini ortaya koymakta ve gelecekteki hibrit yaklaşımlara ışık tutmaktadır.

II. MATERYAL VE YÖNTEM

A. Veri Seti

Bu çalışmada, ağ trafiği üzerinde anomali tespiti yapmak amacıyla yaygın olarak kullanılan KDDTest+ veri seti tercih edilmiştir. Veri seti .arff (Attribute-Relation File Format) formatında sağlanmış olup, ağ trafiğini temsil eden toplam 41 özellik (feature) ve bir sınıf etiketi (normal/anomaly) içermektedir. Veri setindeki her kayıt, belirli bir ağ bağlantısına karşılık gelmekte olup, davranışsal özelliklerle birlikte bu bağlantının normal mi yoksa anormal (izinsiz giriş) mi olduğunu belirtmektedir.

Ham veriler, Python ortamında pandas kütüphanesi kullanılarak işlenmiş ve daha kolay analiz yapılabilmesi için .csv formatına dönüştürülmüştür. İşlenen veri kümesinde toplam 4.509 örnek yer almakta; bunlardan 2.584'ü "anomaly", 1.925'i ise "normal" olarak etiketlenmiştir. Veri setindeki bu dengesizlik, model performansının değerlendirilmesinde dikkate alınmış ve sınıflar arası dengesizliğin etkilerini azaltacak teknikler uygulanmıştır.

B. Model Ve Yöntemler

Anomali tespiti görevinde üç farklı makine öğrenmesi yaklaşımı kullanılarak model karşılaştırmaları gerçekleştirilmiştir: 1D Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP) ve Random Forest (RF) algoritması [6],[7].

CNN Modeli: Model, bir boyutlu evrişimli sinir ağı (1D CNN) yapısında tasarlanmıştır. Bu yapı, her ağ trafiği kaydını zaman serisi benzeri bir vektör olarak ele alarak, yerel örüntüleri öğrenme kapasitesi sağlar. Modelde ReLU aktivasyon fonksiyonu, Dropout katmanı (aşırı öğrenmeyi azaltmak için) ve MaxPooling katmanı (özellik boyutunu indirgemek için) kullanılmıştır. Bu yapı sayesinde modelin genelleme yeteneği artırılmış ve overfitting riski minimize edilmiştir [8],[9].

MLP Modeli: Tam bağlı katmanlardan (dense layers) oluşan klasik bir yapay sinir ağı modeli olarak yapılandırılmıştır. Girdi katmanından başlayarak gizli katmanlar aracılığıyla örüntüler öğrenilmekte, son

katmanda ise binary sınıflandırma yapılmaktadır. MLP modeli, hem doğruluk oranı hem de ROC eğrisi altındaki alan (AUC) açısından başarılı performans göstermiştir [10],[11].

Random Forest Algoritması: Karar ağaçlarının bir topluluğuna dayanan bu yöntem, özellikle verideki dengesizliklere karşı dayanıklı bir yaklaşım sunmaktadır. Rastgele örnekleme ve öznitelik seçimi sayesinde aşırı öğrenmenin önüne geçilmiş ve istikrarlı sonuçlar elde edilmiştir. Modelin hiperparametreleri, çapraz doğrulama yöntemiyle optimize edilerek en uygun ağaç sayısı ve derinlik belirlenmiştir [12],[13].

III. BULGULAR

Random Forest Modeli Sonuçları

Bu çalışmada kullanılan **Random Forest** modeli, eğitim verisi üzerinde eğitildikten sonra test verisi ile değerlendirilmiş ve çeşitli sınıflandırma metrikleri ile performansı analiz edilmiştir. Modelin hem genel doğruluk düzeyi hem de sınıf bazında başarımı oldukça yüksek bulunmuştur.

Sınıf Bazlı Performans Metrikleri

Anomaly (Anomali) Sınıfı

- **Hassasiyet (Precision)**: 0.99
- **Geri Çağırma (Recall)**: 0.98
- **F1 Skoru**: 0.99

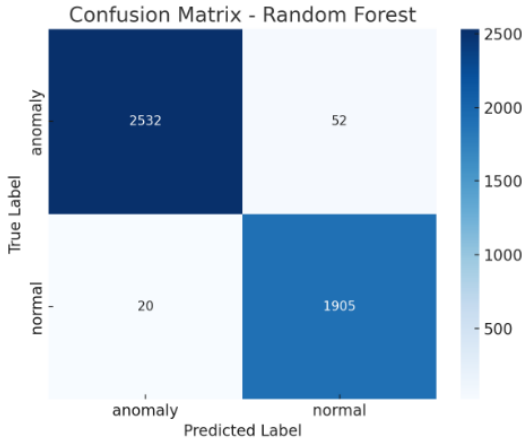
Normal Sınıfı

- **Hassasiyet (Precision)**: 0.98
- **Geri Çağırma (Recall)**: 0.99
- **F1 Skoru**: 0.98

Genel Başarım Değerleri

- **Doğruluk (Accuracy)**: %99
- **Makro Ortalama F1 Skoru**: 0.99

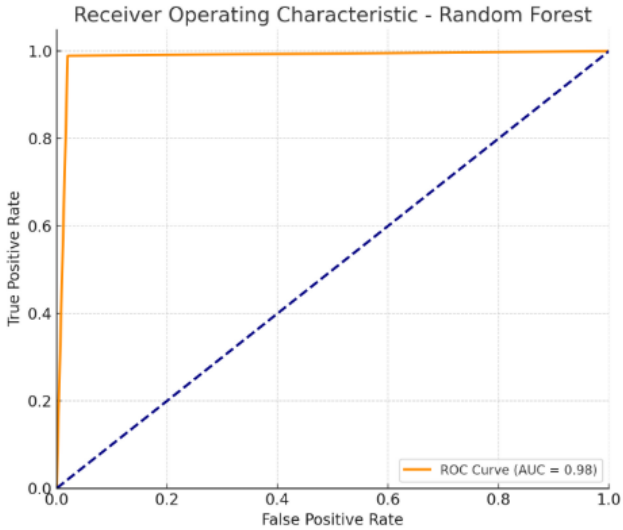
Bu sonuçlar, Random Forest algoritmasının karmaşık ve dengesiz dağılıma sahip ağ trafiği verileri üzerinde hem "normal" hem de "anomaly" sınıflarını başarıyla ayırt edebildiğini göstermektedir. Modelin dengeli sınıf performansı, her iki sınıfta da yüksek F1 skorları ile doğrulanmıştır. Modelin sınıflandırma sonuçları Şekil 1'de sunulan Confusion Matrix (karmaşıklık matrisi) ile detaylandırılmıştır. Matris, doğru ve yanlış sınıflandırılan örneklerin sayısal dağılımını ortaya koymakta olup modelin istikrarlı performansını görsel olarak da desteklemektedir.



Şekil 1. Random Forest için Confusion Matrix

Modelin sınıflandırma başarımı görsel olarak Şekil 2'de yer alan ROC (Receiver Operating Characteristic) eğrisi ile sunulmuştur.

- **AUC (Area Under Curve)** skoru ≈ **0.99** olarak hesaplanmıştır. Bu yüksek AUC değeri, modelin "anomaly" ve "normal" sınıflarını ayırt etme konusundaki etkinliğini açıkça ortaya koymaktadır.



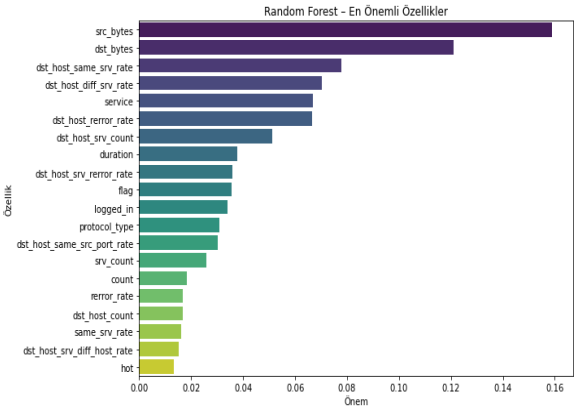
Şekil 2. Random Forest ait ROC Eğrisi

Özellik Önem Değerleri (Feature Importance)

Random Forest algoritmasının sunduğu içsel özellik değerlendirme mekanizması, modelin karar verme sürecinde hangi özniteliklere ne ölçüde önem verdiğini analiz etme imkânı sunmuştur.

- **En Kritik Özellikler**:
  - src_bytes (~0.16) ve dst_bytes (~0.12), veri aktarım miktarına ilişkin özellikler olup, anomali tespitinde belirleyici rol oynamaktadır.
  - dst_host_same_srv_rate, dst_host_diff_srv_rate ve dst_host_rerror_rate gibi sunucu yanıt ve hata oranları da yüksek önem düzeyine sahiptir. Bu, hedef sunucu davranışlarının anomalileri tanımada etkili olduğunu göstermektedir.
- **Orta Düzey Önemli Özellikler**:
  - duration, protocol_type, srv_count, dst_host_srv_count gibi bağlantı süresi, protokol türü ve hizmet sayaçlarına ilişkin öznitelikler modelin karar mekanizmasında önemli katkılar sağlamaktadır.
- **Düşük Önemli Özellikler**:
  - hot değişkeni, en düşük önem değerine sahip olup modelin sınıflandırma performansına sınırlı düzeyde katkı sağlamaktadır.

Bu özellik dağılımı, Random Forest modelinin yüksek doğruluk oranına ulaşmasında özellikle veri aktarım miktarı ve sunucu davranış kalıplarına ilişkin özniteliklerin etkili olduğunu şekil-3'te göstermektedir. Modelin **Anomali sınıfı için F1 skoru: 0.99** ve **Normal sınıf için F1 skoru: 0.98** olması, önerilen yöntemle gerçekleştirilen anomali tespitinin son derece başarılı olduğunu ortaya koymaktadır.



Şekil 3. Random Forest için Feature İmportance

CNN Modeli Sonuçları

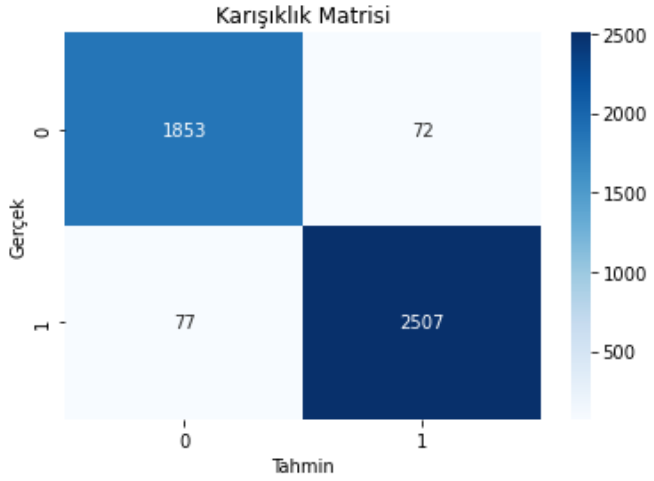
Çalışmanın devamında, CNN modeli için veri seti %80 eğitim ve %20 test olacak şekilde ikiye ayrılmıştır. Model, 10 epoch boyunca ve 32 batch büyüklüğü ile eğitilmiştir. Eğitim süresince modelin başarımı hem doğruluk (accuracy) hem de kayıp (loss) metrikleri üzerinden izlenmiştir.

Eğitim süreci sonunda, modelin test verisi üzerindeki doğruluk oranı %96,7 olarak hesaplanmıştır. Sınıflara göre F1 skorları ise **normal sınıf** için 0.96 ve **anomali sınıfı** için 0.97'dir. Bu sonuçlar, modelin hem normal hem de anormal trafiği yüksek başarımla ayırt edebildiğini göstermektedir. Modelin karışıklık matrisi Şekil-3'te, eğitim ve validasyon sürecine ait doğruluk/kayıp grafiklerine ise Şekil-4'te yer verilmiştir.

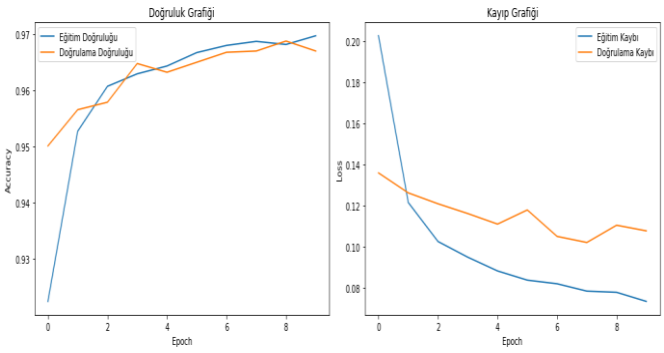
	precision	recall	f1-score	support
0	0.97	0.96	0.96	1925
1	0.97	0.98	0.97	2584
accuracy			0.97	4509
macro avg	0.97	0.97	0.97	4509
weighted avg	0.97	0.97	0.97	4509

Şekil 4. CNN Doğruluk Raporu

Şekil 5 ve Şekil 6, CNN modelinin performansını ve öğrenme sürecini görselleştirmektedir. Şekil 5'te, test verisi üzerinden elde edilen karışıklık matrisi (confusion matrix) sunulmakta olup, modelin doğru ve hatalı sınıflandırmalarına dair kapsamlı bir değerlendirme yapılmaktadır. Şekil 6'da ise modelin eğitim ve doğrulama evrelerinde elde ettiği doğruluk (accuracy) ve kayıp (loss) değerlerinin epoch bazlı değişimi grafiksel olarak gösterilmiştir.

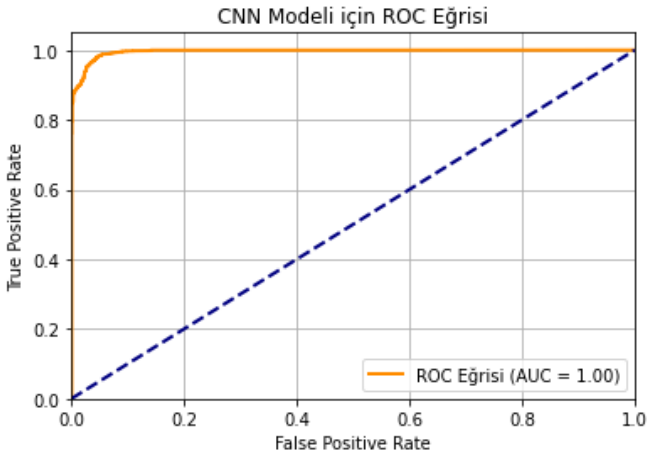


Şekil 5. CNN Sınıflandırma Raporu



Şekil 6. CNN modeline ait Doğruluk ve Kayıp grafiği

Şekil 7, CNN modeline ait ROC (Receiver Operating Characteristic) eğrisini göstermektedir. ROC eğrisi, modelin farklı eşik değerlerindeki sınıflandırma performansını değerlendirmek amacıyla çizilmiştir.



Şekil 7. CNN modeli için ROC eğrisi

MLP Modeli Sonuçları

CNN modeline ek olarak, çok katmanlı algılayıcı (MLP) ile de sınıflandırma gerçekleştirilmiştir. Modelin başarı metrikleri oldukça güçlüdür. MLP modeli, normal ve anomali trafiğini yüksek başarımla sınıflandırmıştır (Şekil-8).

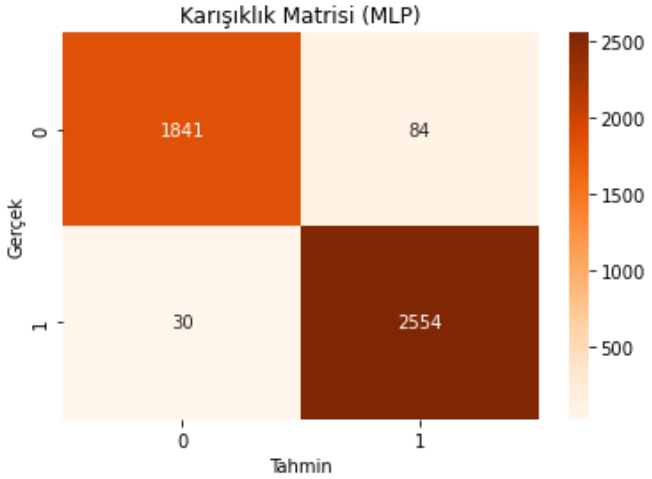
	precision	recall	f1-score	support
0	0.97	0.96	0.97	1925
1	0.97	0.98	0.98	2584
accuracy			0.97	4509
macro avg	0.97	0.97	0.97	4509
weighted avg	0.97	0.97	0.97	4509

Şekil 8. MLP Doğruluk Raporu

Bu değerler, modelin hem normal hem de anomali örneklerini yüksek doğrulukla ayırt edebildiğini ortaya koymaktadır. Özellikle anomali sınıfı için elde edilen %98'lik **recall** değeri, modelin çok az sayıda anormal durumu atladığını (false negative düşük) ve güvenilir bir algılama sağladığını göstermektedir. Bu durum, ağ güvenliği açısından kritik önemdedir; çünkü tespit edilmeyen anomali durumları, ciddi güvenlik açıklarına yol açabilir.

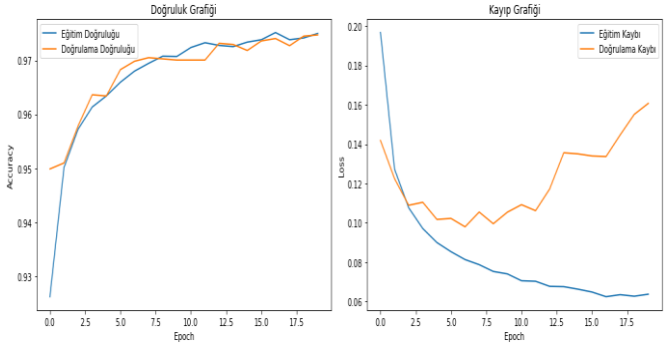
MLP modelinin ROC eğrisi altında kalan alan (AUC) değeri yaklaşık **0.97** olarak hesaplanmıştır. Bu da modelin genel sınıflandırma başarısının oldukça yüksek olduğunu göstermektedir. Karışıklık matrisi (Şekil-7), yanlış sınıflandırmaların düşük seviyelerde olduğunu destekler niteliktedir.

Şekil 9, MLP modeline ait karışıklık matrisini (confusion matrix) göstermektedir. Bu matris, modelin test verisi üzerindeki tahmin sonuçlarını gerçek etiketlerle karşılaştırarak, hangi sınıflarda doğru ya da hatalı tahminler yaptığını ortaya koymaktadır.



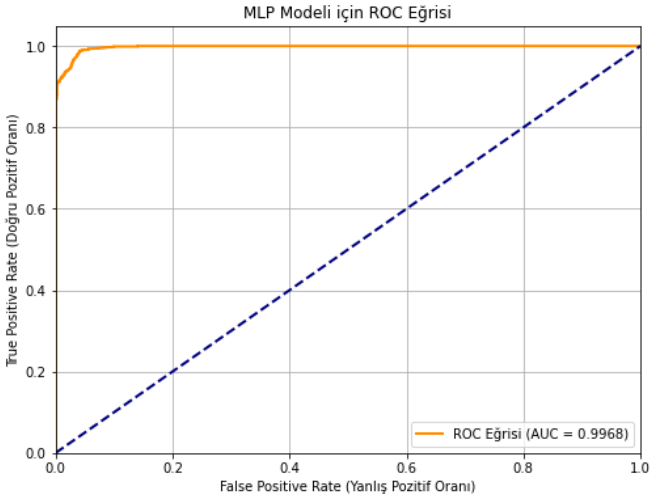
Şekil 9. MLP modeli için Confusion Matrix

Şekil 10'da, MLP modelinin eğitim ve doğrulama süreçlerinde elde ettiği doğruluk (accuracy) ve kayıp (loss) değerlerinin epoch bazlı değişimi sunulmaktadır.



Şekil 10. MLP modeline ait Doğruluk ve Kayıp grafiği

Şekil 11 ise, MLP modelinin ROC (Receiver Operating Characteristic) eğrisini göstermektedir. ROC eğrisi, modelin farklı sınıflandırma eşik değerlerinde gösterdiği performansı yansıtarak, sınıflar arasındaki ayrım gücünü değerlendirme imkânı sunar.



Şekil 11. MLP modeline ait ROC Eğrisi

IV. TARTIŞMA

Gerçekleştirilen çalışma kapsamında kullanılan üç farklı makine öğrenmesi ve derin öğrenme modeli – CNN, MLP ve Random Forest – siber saldırıların tespiti konusunda oldukça başarılı sonuçlar vermiştir. Her bir modelin kendine özgü avantajları ve sınırlılıkları, sistem tasarımında farklı senaryolar için uygunluklarını ortaya koymaktadır.

CNN modeli, özellikle büyük ve karmaşık veri setlerinde yüksek öğrenme kapasitesi sayesinde üstün performans göstermiştir. Derin yapay sinir ağları aracılığıyla veriden özellik çıkarma yeteneği, bu modeli karmaşık desenlerin tanınmasında son derece güçlü kılmaktadır. Test verisi üzerindeki yüksek doğruluk (%96,7) ve güçlü F1 skorları, CNN'in anomali tespitinde etkili bir sınıflandırıcı olduğunu göstermektedir. Ancak, modelin eğitim süresi, çok katmanlı yapısı ve parametre sayısının fazlalığı nedeniyle diğer modellere kıyasla daha uzundur. Bu durum, gerçek zamanlı sistemler için performans-maliyet dengesi açısından dikkatle değerlendirilmelidir.

MLP (Çok Katmanlı Algılayıcı) ise daha sade yapısına rağmen etkileyici sonuçlar üretmiştir. Özellikle %98 gibi yüksek bir recall değeriyle anomali sınıflarını neredeyse eksiksiz tanıyabilmesi, ağ güvenliği açısından önemli bir avantaj sunmaktadır. Ayrıca ROC eğrisi altında kalan alanın (AUC) 0.97 seviyesinde olması, modelin pozitif sınıfları ayırt etme başarısının oldukça yüksek olduğunu göstermektedir. MLP modeli, hızlı eğitim süresi ve düşük hesaplama maliyetiyle özellikle kaynakların sınırlı olduğu senaryolarda uygulanabilirliği yüksek bir seçenek sunmaktadır.

Random Forest modeli ise diğer derin öğrenme tabanlı modellere kıyasla daha az karmaşık olmasına rağmen oldukça rekabetçi sonuçlar elde etmiştir. En büyük avantajı ise modelin yüksek yorumlanabilirliğidir. Özellikle öz nitelik önem derecelerinin analiz edilebilmesi, güvenlik uzmanlarının hangi özelliklerin saldırıların tespitinde daha etkili olduğunu anlamalarına olanak tanımaktadır. Ayrıca paralel işlem yapabilme kapasitesi sayesinde büyük veri kümeleriyle hızlı çalışabilmesi, Random Forest'ı pratik bir alternatif haline getirmektedir.

Bu üç modelin karşılaştırmalı analizi göstermektedir ki, kullanılacak modelin seçimi, veri setinin özelliklerine, gerçek zaman gereksinimlerine ve sistemin performans/yorumlanabilirlik ihtiyaçlarına bağlı olarak değişebilir. Derin öğrenme tabanlı yöntemler yüksek doğruluk sunarken, geleneksel yöntemler daha az kaynakla benzer sonuçlar elde edebilmektedir.

Bununla birlikte, her bir modelin güçlü yönlerinin bir araya getirildiği karma (ensemble) yaklaşımlar, gelecekte daha yüksek doğruluk, daha az hata ve daha güçlü genelleme yetenekleri sağlayabilir. Örneğin, CNN ve MLP modellerinin çıktılarının Random Forest ile desteklenmesi, hem derin özellik öğrenme hem de yorumlanabilirlik açısından daha dengeli bir çözüm sunabilir.

Sonuç olarak, bu çalışma göstermektedir ki siber saldırıların tespitinde tek bir "en iyi" modelden ziyade, veri yapısına ve uygulama amacına göre en uygun model veya modellerin belirlenmesi kritik öneme sahiptir. Bu alandaki ilerlemeler, çok modelli sistemler, sürekli öğrenme mekanizmaları ve gerçek zamanlı uygulamalarla daha da geliştirilebilir.

V. SONUÇLAR

Bu çalışmada, siber saldırıların tespiti amacıyla Convolutional Neural Network (CNN), Multi-Layer Perceptron (MLP) ve Random Forest algoritmaları kullanılarak bir karşılaştırmalı analiz gerçekleştirilmiştir. Model performansları doğruluk, F1 skoru, karışıklık matrisi ve ROC-AUC gibi çeşitli metriklerle değerlendirilmiş; her bir modelin güçlü ve zayıf yönleri ortaya konmuştur.

Elde edilen sonuçlara göre, CNN modeli yüksek doğruluk oranı ve dengeli performansıyla öne çıkarken; MLP modeli özellikle anomali tespitinde sergilediği yüksek recall değeri ile dikkat çekmiştir. Random Forest modeli ise yorumlanabilirliği ve hızlı çalışma süresi ile pratik uygulamalar için uygun bir seçenek olarak değerlendirilmiştir. Üç model de genel anlamda %97 gibi yüksek doğruluk değerlerine ulaşarak, siber saldırıların etkin biçimde tespit edilebileceğini göstermiştir.

Yapılan analizler, tek bir algoritmanın her koşulda en iyi sonuçları vermediğini, veri setinin yapısı, uygulama gereksinimleri ve kaynak kısıtları gibi faktörlerin model seçiminde belirleyici olduğunu ortaya koymuştur. Bu bağlamda, farklı yaklaşımların avantajlarını birleştiren karma (ensemble) modellerin

geliştirilmesi, gelecekte daha yüksek performanslı ve güvenilir siber güvenlik sistemleri oluşturmak için umut vaat etmektedir.

Gelecek çalışmalar kapsamında, gerçek zamanlı veri akışlarının işlendiği çevrim içi sistemlerde model başarımlarının test edilmesi, model güncellemelerinin dinamik olarak yapılabilmesi ve düşük kaynak tüketimiyle çalışan hafif yapay zeka çözümlerinin geliştirilmesi önerilmektedir. Ayrıca, model genelleme yeteneklerinin farklı ağ türleri ve saldırı senaryoları üzerinde de test edilmesi, bu alandaki çalışmalara önemli katkılar sağlayacaktır.

KAYNAKLAR

[1] Diana, L., Dini, P. ve Paolini, D. (2025). Bilgisayarlar için İzinsiz Giriş Tespit Sistemlerine Genel Bakış, Ağ Güvenliği. Bilgisayarlar, 14(3), 87.

[2] Rahman, M. H., Martinez, L., Mishra, A., Nijim, M., Goyal, A., & Hicks, D. (2025, February). AI2DS: Advanced Deep Autoencoder-Driven Method for Intelligent Network Intrusion Detection Systems. In 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

[3] Yonbawi, S., Afzal, A., Yasir, M. H., Rizwan, M., & Kryvinska, N. (2025). Wi-Fi Saldırı Tespit Sistemlerinde Makine Öğrenmesi ve Derin Öğrenme Yaklaşımları ile Aktarılabilirlik Değerlendirmesi. IEEE Erişimi.

[4] Chen, H., Wang, Z., Yang, S., Luo, X., He, D., & Chan, S. (2025). Dinamik Nesnelerin İnterneti ortamları için sinaptik akıllı evrişimli sinir ağları kullanarak izinsiz giriş algılama. İskenderiye Mühendislik Dergisi, 111, 78-91.

[5] Hamdi, N. (2025). A hybrid learning technique for intrusion detection system for smart grid. Sustainable Computing: Informatics and Systems, 46, 101102.

[6] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31.

[7] Leevy, J. L., Khoshgoftaar, T. M., Bauder, R. A., & Seliya, N. (2018). A survey on machine learning algorithms for data classification. *Journal of Big Data, 5*(1), 1–54.

[8] Zhang, C., Song, D., Chen, Y., Feng, X., Lumezanu, C., Cheng, W., ... & Chawla, N. V. (2019). A deep neural network for unsupervised anomaly detection and diagnosis in multivariate time series data. Proceedings of the AAAI Conference on Artificial Intelligence, 33(01), 1409–1416.

[9] Kim, Y., Kim, J., & Kim, H. K. (2016). Anomaly detection of the industrial control system based on deep learning. IEEE Access, 7, 70622–70633.

[10] Gómez, J., Gil, D., & Obrador, S. (2019). Neural network-based intrusion detection system for network infrastructure. International Journal of Interactive Multimedia and Artificial Intelligence, 5(7), 26–32.

[11] Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. Computer Communications, 34(18), 2227–2235.

[12] Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.

[13] Boström, H., & Džeroski, S. (2008). Learning for class imbalance problems in random forests. In International Workshop on Multiple Classifier Systems (pp. 150–161). Springer.