2026 34th Signal Processing and Communications Applications Conference (SIU) | 979-8-3195-1046-4/26/$31.00 ©2026 IEEE | DOI: 10.1109/SIU71813.2026.11636987

Çok Sınıflı Ağ Saldırı Tespiti: Canlı Akış Dağıtımı ile Makine ve Derin Öğrenme Karşılaştırması

Multi-Class Network Intrusion Detection: Machine and Deep Learning Benchmark with Live Stream Deployment

Betül Danışmaz ve Mustafa Emre Bıyık
Bilgisayar Mühendisliği Bölümü
İstanbul Sağlık ve Teknoloji Üniversitesi
İstanbul, Türkiye
betul.danismaz@istun.edu.tr
mustafa.emre.biyik@istun.edu.tr

Necip Gozüaçık
Yazılım Mühendisliği Bölümü
İstanbul Sağlık ve Teknoloji Üniversitesi
İstanbul, Türkiye
necip.gozuacik@istun.edu.tr

***Özetçe*— Gelişmiş siber tehditlerin hızla artması, geleneksel, imza tabanlı ağ saldırı tespit sistemlerinin sınırlarını ortaya koymaktadır. Makine öğrenimi ve derin öğrenme modelleri proaktif savunma mekanizmaları sunarken, mevcut araştırmalar genellikle zamansal veri sızıntıları, pratik olmayan tehdit sınıflandırmaları ve çevrimdışı değerlendirme ile çevrimiçi dağıtım arasındaki önemli farklar nedeniyle tehlikeye girmektedir. Bu çalışma, tamamen işlevsel bir gerçek zamanlı çıkarım hattına entegre edilmiş geleneksel makine öğrenimi ve derin öğrenme mimarilerinin karşılaştırmalı değerlendirmesini sunmaktadır. Ayrıca, olaylara müdahaleyi anlamlandırmak için Zararsız, Hacimsel ve Semantik trafiğini kapsayan, operasyonel olarak motive edilmiş üç sınıflı bir sınıflandırma önerilmiştir. Eğitilen XGBoost, Rastgele Orman, Karar Ağacı, LSTM, BiLSTM modelleri aynı kısıtlamalar altında değerlendirilerek karşılaştırıldığında BiLSTM ağı, %97,72 ile en yüksek Makro F1 puanını elde etmiştir. Ancak, XGBoost algoritması %95,87 ile 15,5 kat daha hızlı çıkarım sergilemiştir. Bu bulguları pratiğe aktarmak için, gerçek zamanlı akış çıkarımı, sıfır kesintili model değişimi ve otomatik tehdit yanıtı özelliklerini bir arada barındıran Kafka tabanlı bir canlı sistem mimarisi tasarlanmıştır.**

Anahtar Kelimeler*— *ağ saldırı tespiti; makine öğrenimi; derin öğrenme; gerçek zamanlı dağıtım; çok sınıflı saldırı; CICIDS2017.

***Abstract*— The rapid rise of advanced cyber threats is exposing the limitations of traditional, signature-based network intrusion detection systems. While machine learning and deep learning models offer proactive defense mechanisms, current research is often compromised due to temporal data leakage, impractical threat classifications, and significant discrepancies between offline evaluation and online deployment. This study presents a comparative evaluation of traditional machine learning and deep learning architectures integrated into a fully functional real-time inference pipeline. Additionally, we propose an operationally motivated three-class classification encompassing Benign, Volumetric, and Semantic traffic to contextualize incident response. When the trained XGBoost, Random Forest, Decision Tree, LSTM, and BiLSTM models were evaluated and compared under the same constraints, the BiLSTM model achieved the highest Macro F1 score at 97.72%. However, XGBoost closely followed with a Macro F1 of 95.87%, while achieving 15.5 times faster inference. To translate these findings into practice, a Kafka-based live system architecture was designed that integrates real-time stream inference, zero-downtime model switching, and automated threat response capabilities.**

Keywords*— *network intrusion detection; machine learning; deep learning; real-time deployment; multi-class attack; CICIDS2017.

I. GİRİŞ

Günümüzde finansal sistemlerden kritik ulusal altyapılara uzanan ağ güvenliği, kurumsal sürekliliğin temel güvencesi hâline gelmiştir. Siber saldırılar artık yalnızca basit ihlallerden ibaret olmayıp; Dağıtık Hizmet Aksatma (DDoS), sızma ve botnet komuta-kontrol iletişimlerini eşzamanlı kullanan çok vektörlü kampanyalara dönüşmüştür [1]. Bu tehdit ortamında geleneksel Ağ Saldırı Tespit Sistemi (NIDS) yaklaşımları yapısal kısıtlamalar sergilemektedir. İmza tabanlı sistemler yalnızca önceden kataloglanmış saldırı profillerini tanıyabilirken sıfırıncı gün açıklarına karşı etkisiz kalmaktadır. Kural tabanlı sistemler ise değişen trafik davranışlarına uyum sağlayamamakta, yüksek yanlış pozitif üretmekte ve yoğun manuel yapılandırma gerektirmektedir [2].

Bu kısıtlamaları aşmak amacıyla Makine Öğrenmesi (ML) ve Derin Öğrenme (DL) tabanlı NIDS yaklaşımları öne çıkmaktadır. Rastgele Orman (RF) ve XGBoost gibi geleneksel ML algoritmaları tablo tabanlı öznitelik vektörlerinde güçlü performans sunarken [3]; Uzun Kısa Vadeli Bellek (LSTM) ve Çift Yönlü LSTM (BiLSTM) gibi ardışık DL mimarileri ağ trafiğinin zamansal örüntülerini modelleyebilmektedir [4],[5].

Ancak bu iki yaklaşımı karşılaştıran mevcut çalışmalar üç kritik metodolojik sorun barındırmaktadır: (i) CICIDS2017 gibi çoklu günlük veri setlerinde küresel rastgele karıştırma uygulanması zamansal veri sızıntısına ve yapay yüksek doğruluk değerlerine yol açmaktadır [6], [7], [8]; (ii) kullanılan saldırı taksonomileri Güvenlik Operasyon Merkezlerinin (SOC) gerçek triyaj süreçlerinden kopuktur; (iii) ML ve DL modelleri farklı deneysel koşullar altında değerlendirildiğinden adil bir karşılaştırma yapılamamaktadır. Bu çalışma söz konusu boşlukları aynı anda kapatan uçtan uca bir mimari sunmaktadır. Temel katkılar şöyle sıralanabilir: **(K1)** zamansal sızıntıyı matematiksel olarak ortadan kaldıran Dosya Bazlı Katmanlı Bölme protokolü; **(K2)** SOC triyajını hızlandırmak üzere tasarlanmış Zararsız/Hacimsel/Anlamsal üç sınıflı operasyonel taksonomi; **(K3)** beş modelin özdeş koşullar altında sistematik karşılaştırması; **(K4)** sıfır kesintili model değişimi ve otomatik tehdit yanıtını destekleyen Kafka tabanlı gerçek zamanlı üretim mimarisi.

II. Literatür Taraması

A. Geleneksel Makine Öğrenmesi ve Derin Öğrenme Karşılaştırmaları

RF ve XGBoost gibi geleneksel makine öğrenmesi algoritmaları, 2 boyutlu tablo tabanlı öznitelik vektörleri üzerinde yüksek başarım gösterdikleri için tercih edilmektedir [9]. Ağ trafiğinin zaman serisi doğasını modellemek amacıyla LSTM ve BiLSTM gibi 3 boyutlu sıralı derin öğrenme mimarileri giderek daha fazla kullanılmaktadır. Ancak, literatürde gradyan artırımlı ağaç modelleri ile derin sıralı modellerin; aynı veri bölütleme, aynı öznitelik kümesi ve aynı sınıf ağırlıklandırma koşulları altında nesnel olarak değerlendirildiği adil bir deneysel karşılaştırma çalışması bulunmamaktadır.

B. Saldırı Taksonomisi ve Operasyonel Gereksinimler

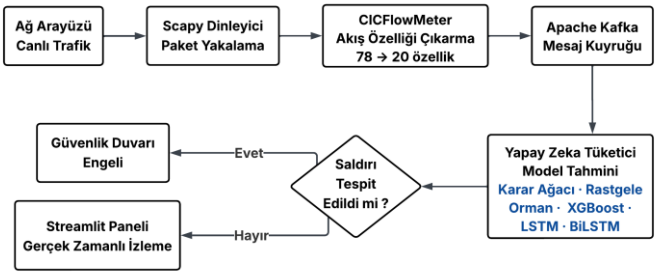
Çalışmaların pek çoğu, KDD99'dan miras kalan çok sınıflı saldırı kategorilerini kullanmakta veya operasyonel olarak yetersiz teorik gruplandırmalar yapmaktadır [10]. SOC için tehdit önceliklendirme ve triyaj süreçlerini hızlandıracak; ağ trafiğini Normal (Benign), Hacimsel (Volumetric) ve Anlamsal (Semantic) saldırı türleri olarak ayıran 3 sınıflı pratik bir taksonomi eksikliği literatürde göze çarpmaktadır [11].

C. Gerçek Zamanlı Dağıtım ve MLOps Rejimi

Mevcut NIDS araştırmalarının %12'sinden azı bağımsız bir şekilde yeniden üretilebilir MLOps konfigürasyonları ve hiperparametre şemaları sunmaktadır [12]. Üretime geçiş odaklı araştırmalar ise genellikle yalnızca veri akışı, güvenlik duvarı entegrasyonu veya gösterge paneli gibi izole bileşenleri ele almaktadır. Canlı ağ trafiği analizi sırasında, 2 boyutlu tablo tabanlı geleneksel ML modelleri ile 3 boyutlu sıralı DL modelleri arasında sistem kesintisi yaşanmadan çalışma anında geçiş yapılmasına (hot-swapping) olanak tanıyan, uçtan uca doğrulanmış bir üretim mimarisi mevcut NIDS literatüründe bulunmamaktadır [13].

III. Metodoloji

Önerilen çalışmada ağ trafiğini gerçek zamanlı olarak analiz edip sınıflandıran uçtan uca yapay zeka tabanlı saldırı tespit sisteminin metodolojik altyapısı sunulmaktadır. Yalnızca statik çevrimdışı veri seti değerlendirmeleriyle sınırlı kalmayıp, canlı ağ trafiği üzerinde çalışabilen dağıtık bir "Canlı Köprü (Live Bridge)" mekanizması üzerine Şekil 1'de görüldüğü gibi inşa edilmiştir.



Şekil 1. Sistem Mimarisi

İlk aşamada, ağ arayüzü üzerinden Scapy aracı ile yakalanan canlı trafik paketleri, CICFlowMeter ile akış tabanlı özniteliklere dönüştürülmekte ve boyut indirgeme adımıyla model eğitimi için en kritik 20 öznitelik seçilmektedir. İkinci aşamada, bu öznitelik vektörleri Apache Kafka mesaj iletim hattı üzerinden eşzamansız olarak yapay zeka tüketim bileşenine aktarılmaktadır. Tüketim katmanında; RF, Karar Ağacı (DT), XGBoost, LSTM ve BiLSTM olmak üzere beş modelin çalışma anında kesintisiz olarak tahminleme yapabildiği bir altyapı tasarlanmıştır.

A. Veri Seti ve Veri Mühendisliği

Beş günlük çoklu profil trafik mimarisi, gerçekçi kullanıcı davranış modelleri ve heterojen saldırı kategorileriyle NIDS literatüründe standart kıyaslama aracı konumundaki CICIDS2017 veri seti kullanılmıştır. Veri setindeki 14 saldırı alt kategorisinin sınıf dağılımı incelendiğinde istatistiksel genelleme için yetersiz örneklem içerdiği görülmektedir. Bu sorunu gidermek amacıyla, saldırıların baskın etki mekanizmaları temel alınarak üç sınıflı operasyonel bir taksonomi tanımlanmıştır. Önerilen şema, farklı müdahale prosedürleri gerektiren hacimsel saldırıları (DDoS, DoS, Botnet) ve anlamsal saldırıları (Web Saldırıları, Kaba Kuvvet, Port Tarama, Sızma) bilinçli olarak ayrıştırmaktadır.

Taksonomi ve sınıf dağılımı Tablo I'de sunulmaktadır.

TABLO I. Üç Sınıflı Tehdit Taksonomisi

Türetilmiş Sınıf	Etiket	Saldırı Çeşitleri	Veri Miktarı	Oran
0	Zararsız	Normal trafik	2.265.000	~%80
1	Hacimsel	DDoS, DoS, Botnet	396.000	~%14
2	Anlamsal	Web Saldırıları, Kaba Kuvvet, Port Tarama, Sızma	170.000	~%6

Zamansal veri sızıntısını matematiksel olarak ortadan kaldırmak amacıyla, bu çalışmada özgün bir "Dosya Bazlı Katmanlı Bölme" protokolü geliştirilmiştir. Bölütleme işlemi, veri seti birleştirilmeden önce her günlük dosya üzerinde bağımsız olarak uygulanmıştır. Böylece aynı saldırı oturumuna ait zamansal bağlamın eğitim ve test kümeleri arasında geçişi engellenmiş, azınlık sınıflarının (%6'lık Anlamsal sınıf) her bölütte (eğitim/doğrulama/test) orantısal temsili ise korunmuştur. Operasyonel açıdan en kritik kategori olan Anlamsal sınıfın bu baskı altında ezilmesini önlemek amacıyla, tüm modellerde ortak bir ters-frekans sınıf ağırlıklandırması stratejisi benimsenmiştir [14].

$$wc = \frac{N_{total}}{K \times N_c} \qquad (1)$$

(1) ile ifade edilen yapıda K sınıf sayısını (3), N_c ise c sınıfına ait eğitim örneği sayısını ifade etmektedir. Uygulama düzeyinde ise model mimarisine özgü bir ayrım gözetilmiştir: XGBoost, RF ve DT modellerinde yerleşik sample_weight parametresi kullanılırken, LSTM ve BiLSTM mimarilerinde sınıf ağırlıkları ön işleme aşamasında hesaplanarak eğitim sürecine statik biçimde beslenmiştir.

B. Öznitelik Mühendisliği

Ham ağ trafiğinden CICFlowMeter aracıyla her akış için 78 çift yönlü istatistiksel öznitelik çıkarılmış; Inf ve NaN değerler sıfırla ikame edilerek veri temizlenmiştir. Hesaplama yükünü azaltmak ve genelleme kapasitesini artırmak amacıyla öznitelik önem skorları çapraz doğrulanarak en belirleyici 20 öznitelik seçilmiştir.

C. Yapay Zeka Geliştirmesi

Beş modelin performanslarını nesnel olarak karşılaştırmak amacıyla tüm deneylerde aynı hiperparametreler, öznitelikler ve veri bölütleme stratejisi kullanılmıştır. RF, DT ve XGBoost modelleri için ağ akışları 2 boyutlu (N × 20) vektörler halinde değerlendirilirken, LSTM ve BiLSTM modelleri için 10 adımlık kayan pencere (stride=1) ile oluşturulan 3 boyutlu tensörler kullanılmıştır.

Tablo tabanlı öznitelik uzayında birincil model olarak kullanılan XGBoost algoritması, üç sınıf için olasılık üreten multi:softprob hedef fonksiyonu ile eğitilmiştir. Eğitimde max_depth=7, learning_rate=0.05, subsample=0.8 ve colsample_bytree=0.8 hiperparametreleri kullanılmış ve eğitim, 4 GB VRAM kapasiteli NVIDIA RTX 3050 GPU ve 32 GB sistem belleği barındıran Intel Core i7-12700H tabanlı bir iş istasyonunda, TensorFlow-GPU ve CUDA hızlandırması kullanılarak gerçekleştirilmiştir. Karşılaştırma amacıyla geliştirilen RF modeli 36 kombinasyonluk ızgara araması ile optimize edilirken, Karar Ağacı modeli yorumlanabilir bir referans sınıflandırıcı olarak kullanılmıştır.

Zamansal bağımlılıkları modellemek için LSTM ve BiLSTM mimarileri geliştirilmiştir. LSTM modeli 128 ve 64 birimli iki katmandan oluşmakta olup her katmanın ardından Batch Normalizasyonu ve %30 Dropout uygulanmıştır. BiLSTM modeli daha geniş zamansal bağlamı öğrenebilmek için zaman serisini çift yönlü işleyerek tasarlanmış ve karşılaştırmanın adil olması için katman yapısı ve hiperparametreleri LSTM ile aynı tutulmuştur.

D. Gerçek Zamanlı Üretim Mimarisi

Eğitim ortamı ile üretim ortamı arasındaki boşluğu doldurmak amacıyla "Canlı Köprü" olarak adlandırılan, birbirine entegre dört aşamalı gerçek zamanlı bir üretim mimarisi tasarlanmıştır.

1) Canlı Veri Yakalama ve Eşzamansız İletim: Scapy ile 4 saniyelik pencereler halinde yakalanan trafik, CICFlowMeter ile 78 boyutlu akış özniteliklerine dönüştürülerek Apache Kafka hattı üzerinden eşzamansız iletilmektedir.

2) *Eşzamanlı Çıkarım ve Özellik Hizalama:* Kafka Tüketici modülü, her ağ akışı için 78 boyutlu öznitelik vektörünü çalışma anında Top-20 uzayına indirgemektedir. Eğitim-üretim istatistiksel tutarlılığını sağlamak amacıyla, yalnızca eğitim setine uyarlanan MinMaxScaler nesnesi serileştirilerek canlı çıkarım sürecine entegre edilmiştir.

3) Sıfır Kesintili Model Değişimi: Sistem, makine öğrenmesi modelleri (örn. XGBoost, RF, DT) ile derin öğrenme mimarileri (örn. LSTM, BiLSTM) arasında, mesaj kuyruğunu veya çıkarım servislerini yeniden başlatmadan çalışma anında kesintisiz geçişe olanak tanımaktadır.

4) Kapalı Döngü Doğrulama ve Otomatik Yanıt: Hacimsel veya Anlamsal bir saldırı tespit edildiğinde, platform bağımsız (iptables/Windows Firewall) otomatik yanıt modülü tetiklenerek şüpheli IP adresleri anında engellenmektedir. Yanlış pozitif riskini sınırlamak amacıyla çok katmanlı bir doğrulama mimarisi benimsenmiştir: otomatik sınıflandırma hattı, kayan zaman penceresi içindeki tespit sıklığına dayalı üç aşamalı kademeli yanıt politikası (Uyarı → Şüpheli → Engelleme) uygulayarak tek bir hatalı tahminle doğrudan engelleme kararı verilmesini önlemekte; nihai güvenlik duvarı kuralları ise yalnızca SOC analisti onayıyla uygulanmaktadır.

IV. DENEYSEL SONUÇLAR

Bu bölümde beş modelin sınıflandırma başarımı, sınıf bazlı F1 skorları ve çıkarım gecikmesi açısından karşılaştırmalı olarak analiz edilmektedir.

A. Genel Sınıflandırma Başarımı

Beş farklı modelin üç sınıflı taksonomi üzerindeki genel performans sonuçları Tablo II'de sunulmaktadır. Dengelenmiş bir değerlendirme sağlamak amacıyla ana kıyaslama metriği olarak sınıfları eşit ağırlıklandıran Makro F1-Skoru seçilmiştir. Tablo II incelendiğinde, BiLSTM mimarisinin %97,72 Makro F1-Skoru ile en yüksek başarımı sergilediği, beş model arasındaki toplam performans açığının 1,88 yüzde puanı ile sınırlı kaldığı görülmektedir.

TABLO II. MODEL GENEL TEST SETİ BAŞARIMLARI

Model	Doğruluk (%)	Makro Keskinlik (%)	Makro Duyarlılık (%)	Makro F1-Skoru (%)	Gecikme / Verim (ms - Ö/S)
LSTM	98,15	95,79	97,13	96,45	0,0575 - 17.383
XGBoost	97,71	93,62	**98,38**	95,87	0,0070 - 142.428

Karar Ağacı	97,27	94,26	97,83	95,84	0,0001 - 10.534.659
Rastgele Orman	97,34	94,43	97,70	95,91	0,0031 - 319.398
BiLSTM	**98,88**	**97,98**	98,02	**97,72**	0,1085 - 9.212

B. Sınıf Bazlı Analiz

Sınıf bazlı başarımlar incelendiğinde (Bkz. Tablo III), operasyonel açıdan en kritik kategoriyi temsil eden "Anlamsal (Semantic)" saldırıların tespitinde BiLSTM modelinin %97,72 F1-Skoru ile en yüksek başarımı sergilediği görülmektedir. Karar Ağacı (%97,53) ise tüm geleneksel ML modelleri arasında bu sınıfta en yüksek skora ulaşmış; kural tabanlı mimarilerin anlamsal saldırı örüntülerini ayrıştırmadaki etkinliğini ortaya koymuştur.

TABLO III. SINIF BAZLI F1-SKORLARI (%)

Model	Zararsız (Benign)	Hacimsel (Volumetric)	Anlamsal (Semantic)
LSTM	98,84	95,58	94,93
XGBoost	98,56	94,35	94,71
Karar Ağacı	98,28	91,71	97,53
Rastgele Orman	98,32	91,94	97,36
BiLSTM	**99,30**	**96,92**	**97,72**

C. Gerçek Zamanlı Çıkarım Analizi

Sistemin üretim hattındaki uygulanabilirliğini ve canlı ağ trafiği altındaki performansını belirlemek amacıyla, 10.000 örneklemlik bir test protokolü üzerinden ölçülen çıkarım gecikmeleri Tablo II'deki Gecikme/Verim sütununda ayrıca sunulmaktadır. Sonuçlar, ağaç tabanlı geleneksel makine öğrenmesi algoritmalarının, çıkarım hızı bağlamında derin öğrenme mimarilerinden üstün olduğunu ortaya koymaktadır. Karar Ağacı modeli, kurallara dayalı basit yapısı sayesinde saniyede 10 milyonu aşan akışı işleyerek en düşük gecikme süresine ulaşmıştır. Genel sınıflandırma başarımları göz önüne alındığında, XGBoost mimarisi hız ve doğruluk arasında en ideal dengeyi sunmaktadır. XGBoost modeli, saniyede yaklaşık 142.500 akışı sınıflandırabilmekte ve en yakın derin öğrenme rakibi olan BiLSTM'e kıyasla 15,5 kat veri işleme hacmi sağlamaktadır. Bu bulgular, en yüksek tespit başarımı BiLSTM'e ait olsa dahi, gerçek zamanlı siber savunma senaryolarında XGBoost'un Pareto-optimal bir seçenek olduğunu göstermektedir.

V. ÇIKARIMLAR

Beş model, Dosya Bazlı Katmanlı Bölme protokolü ve üç sınıflı (Zararsız/Hacimsel/Anlamsal) tehdit taksonomisi çerçevesinde CICIDS2017 üzerinde özdeş koşullar altında karşılaştırmalı olarak incelenmiştir. BiLSTM %97,72 Makro F1-Skoru ile en yüksek başarımı sergilerken, XGBoost yalnızca 1,85 yüzde puanı geride kalarak 15,5 kat daha yüksek çıkarım hacmiyle Pareto-optimal bir seçenek olarak öne çıkmaktadır. Karar Ağacı'nın Anlamsal sınıf tespitinde tüm geleneksel ML modelleri arasında en yüksek skora ulaşması (%97,53), kural tabanlı mimarilerin bu saldırı kategorisindeki ayrıştırıcı gücünü ortaya koymaktadır. Geliştirilen Canlı Köprü mimarisi ise sıfır kesintili model değişimi ile SOC operasyonlarına entegre edilebilir denetlenebilir bir çıkarım altyapısı sunmaktadır.

Gelecek çalışmalarda şu hedefler planlanmaktadır: modellerin CICIDS2018, UNSW-NB15 ve CIC-DDoS2019 veri setleri üzerinde test edilerek genelleme yeteneğinin değerlendirilmesi; Kafka tabanlı mimarinin yüksek trafik altında performans ve ölçeklenebilirlik açısından sınanması; model güven skoruna dayalı dinamik eşikleme ile CIDR tabanlı beyaz liste yönetiminin geliştirilmesi; canlı trafik altyapısı üzerinden analist etiketli akışlarla artımlı model güncelleme mekanizmalarının kurulması. Uzun vadede ise ağ trafiğinin zamansal etkileşim grafı olarak modellenmesi ve Transformer tabanlı mimariler, federe öğrenme ile denetimsiz anomali tespitini birleştiren hibrit yaklaşımlar araştırılacaktır.

KAYNAKLAR

[1] IBM Security, *X-Force Threat Intelligence Index 2024*. IBM Corporation, 2024.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, 2019.

[3] S. S. Dhaliwal, A. A. Nahid, and R. Abbas, "Effective intrusion detection system using XGBoost," *Information*, vol. 9, no. 7, p. 149, 2018.

[4] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[5] C. Imrana, Y. Xiang, L. Ali, and A. Sheraz, "A bidirectional LSTM deep learning approach for intrusion detection," *Expert Systems with Applications*, vol. 185, p. 115524, 2021.

[6] G. Engelen, V. Rimmer, and W. Joosen, "Troubleshooting an intrusion detection dataset: The CICIDS2017 case study," in *Proc. IEEE Security and Privacy Workshops (SPW)*, 2021, pp. 7–12.

[7] L. D'hooge *et al.*, "Discovering non-metadata contaminant features in intrusion detection datasets," in *Proc. 2022 Int. Conf. on Privacy, Security and Trust (PST)*, 2022.

[8] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "A detailed analysis of the CICIDS2017 data set," in Proc. Int. Conf. on Information Systems Security and Privacy (ICISSP), 2018, pp. 108-116.

[9] Ö. B. Mercan, A. G. Toprak, and M. S. Osmanca, "Traditional Machine Learning and Large Language Model Approach in Network Intrusion Detection," in Proc. 2025 33rd Signal Processing and Communications Applications Conference (SIU), pp. 1–4, 2025.

[10] S. J. Stolfo *et al.*, "Cost-based modeling for fraud and intrusion detection," in *Proc. DARPA Information Survivability Conf. and Exposition (DISCEX)*, vol. 2, 1999, pp. 130–144.

[11] Ö. B. Mercan, A. G. Toprak, and M. S. Osmanca, "Multi-Class Classification for IoT Attack Detection: An LLM-Based Approach," in Proc. 2025 33rd Signal Processing and Communications Applications Conference (SIU), pp. 1–4, 2025.

[12] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[13] G. Apruzzese *et al.*, "SoK: Pragmatic assessment of machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2023.

[14] F. Pedregosa *et al.*, "Scikit-learn: Machine learning in Python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.