Fırat Üniversitesi Müh. Bil. Dergisi
35(2), 569-579, 2023

*Araştırma Makalesi*
https://doi.org/10.35234/fumbd.1291388

# Siber Güvenlikte CIC-Darknet2020 Veri Seti Kullanarak VPN/NoVPN ve Tor/NoTor Sınıflandırması: Basit ve Karmaşık Modellerin Kullanımı

**Yusuf ALACA**[1*]
[1] Bilgisayar Teknolojileri Bölümü, Osmancık Ömer Derindere MYO, Hitit Üniversitesi, Çorum, Türkiye
[*1] yusufalaca@hitit.edu.tr

**(Geliş/Received: 02/05/2023; Kabul/Accepted: 01/07/2023)**

**Öz:** İnternet kullanımı günümüzde hızla artmakta ve birçok işlem dijital ortamda gerçekleştirilmektedir. Ancak, bu durum aynı zamanda internetin kötüye kullanımına zemin hazırlamaktadır. Siber suçlar ve saldırılar her geçen gün artmaktadır ve siber güvenlik konusu son derece önemli hale gelmiştir. CIC-Darknet2020 adlı veri seti, siber güvenlik alanında çalışan araştırmacılar tarafından hazırlanmış ve Darknet ağlarında gerçekleşen trafiği içermektedir. Bu trafiğin analizi, Darknet ağlarındaki faaliyetler hakkında önemli bilgiler sağlayabilmektedir. Bu çalışmada, CIC-Darknet2020 veri seti üzerinde modeller kullanılarak VPN/NoVPN ve Tor/NoTor sınıflandırması yapılmıştır. OneR ve Ensemble OneR modelleri kullanılarak yapılan sınıflandırma sonuçları incelenmiştir. Sonuçlar, VPN/NoVPN sınıflandırması için Ensemble OneR modelinin ROC-AUC değerinin 0.779 olduğunu göstermiştir. Tor/NoTor sınıflandırması için ise Ensemble OneR modeli, son derece iyi sonuçlar elde ederek ROC-AUC değeri 0.980 olmuştur. Bu çalışma, siber güvenlik alanında basit modellerin bile önemli sonuçlar elde edebileceğini ve kullanılabilir olduğunu göstermektedir. Ancak, daha karmaşık modellerin kullanımının da gerekliliği ortaya çıkmaktadır. Siber güvenlik alanında hem basit hem de karmaşık modellerin kullanılması gerektiği sonucuna varılmaktadır. Sonuç olarak, CIC-Darknet2020 veri seti üzerinde yapılan çalışmalar sonucunda elde edilen sonuçlar siber güvenlik alanında farklı modeller kullanarak VPN/NoVPN ve Tor/NoTor sınıflandırması yapılabilirliğini göstermektedir. Bu çalışmanın sonuçları, daha karmaşık modellerin kullanımının gerekliliği ortaya koysa da, basit modellerin bile önemli sonuçlar elde edebileceğini göstermektedir.

**Anahtar kelimeler:** Siber güvenlik, VPN, Tor, Ensemble OneR modeli, sınıflandırma.

## Classification of VPN/NoVPN and Tor/NoTor Using CIC-Darknet2020 Dataset in Cybersecurity: Utilizing Simple and Complex Models

**Abstract:** Internet usage is rapidly increasing today, and many transactions are being carried out in the digital environment. However, this situation also paves the way for the misuse of the internet. Cybercrimes and attacks are increasing day by day, and the issue of cybersecurity has become extremely important. The CIC-Darknet2020 dataset, prepared by researchers working in the field of cybersecurity, contains traffic occurring in Darknet networks. The analysis of this traffic can provide important information about activities on Darknet networks. In this study, VPN/NoVPN and Tor/NoTor classification were made using models on the CIC-Darknet2020 dataset. The classification results obtained using OneR and Ensemble OneR models were examined. The results showed that the ROC-AUC value of the Ensemble OneR model was 0.779 for VPN/NoVPN classification. For Tor/NoTor classification, the Ensemble OneR model achieved excellent results with a ROC-AUC value of 0.980. This study demonstrates that even simple models can achieve significant results in the field of cybersecurity and are usable. However, the use of more complex models also becomes necessary. It is concluded that both simple and complex models need to be used in the field of cybersecurity. In conclusion, the results obtained from the studies conducted on the CIC-Darknet2020 dataset demonstrate the possibility of performing VPN/NoVPN and Tor/NoTor classification using different models in the field of cybersecurity. Although the results of this study emphasize the necessity of using more complex models, they also demonstrate that even simple models can achieve significant results.

**Key words:** Cybersecurity, VPN, Tor, Ensemble OneR model, classification.

## 1. Giriş

Siber güvenlik alanında gerçekleştirilen araştırmalar ve çalışmalar, internet kullanımının yaygınlaşmasına paralel olarak siber suçlar ve zafiyetlerin artmasına yol açtığını göstermektedir. Bu durum, siber güvenlik konusunun son derece kritik bir öneme sahip olmasını beraberinde getirmektedir.

VPN (Sanal Özel Ağ) ve Tor (The Onion Router) hizmetleri, internet kullanıcılarının çevrimiçi gizliliklerini ve güvenliklerini artırmak için kullanılan araçlardan oluşmaktadır. Her ikisi de farklı çalışma prensiplerine ve zafiyetlere sahiptir.

* Sorumlu yazar: yusufalaca@hitit.edu.tr. Yazarların ORCID Numarası: [1] 0000-0002-4490-5384

VPN, internet trafiğini şifreleyerek kullanıcının IP adresini gizler ve verilerin güvenli bir şekilde iletilmesini sağlamaktadır. VPN kullanmak, internet sağlayıcısının veya diğer izleyicilerin izlemesini engellemekte ve internete bağlantısının konum bilgisini gizlemektedir. Ancak, VPN hizmetlerinde zafiyetler olabilmektedir.

Tor, internet trafiğini gizlemek için farklı sunucular üzerinden yönlendirilmiş bir ağ kullanmaktadır. Bu ağ üzerinden iletilen veriler, şifrelenir ve Tor ağındaki sunucular arasında rastgele yönlendirilir, bu nedenle kimlik bilgilerinin izlenmesi zorlaşmaktadır. Tor, anonimliği artırırken bazı zafiyetlere de sebep olabilmektedir.

CIC-Darknet2020 veri seti, siber güvenlik alanında çalışan araştırmacılar tarafından hazırlanmış ve Darknet ağlarında gerçekleşen trafiği içermektedir. Bu trafiğin analizi, Darknet ağlarındaki faaliyetler hakkında önemli bilgiler sağlayabilmektedir. Birçok araştırmacı, CIC-Darknet2020 veri seti üzerinde VPN/NoVPN ve Tor/NoTor sınıflandırması yapmak için modeller kullanmaktadır. Bu sınıflandırma, internet trafiğinin analizi için önemlidir. Birçok çalışmada, OneR modeli ve Ensemble OneR modeli kullanılmıştır. Bu modellerin kullanımı ile VPN/NoVPN ve Tor/NoTor sınıflandırması yapılabilmektedir.

Siber güvenlik alanında CIC-Darknet2020 veri seti kullanarak yapılan VPN/NoVPN ve Tor/NoTor sınıflandırması konusunda birçok akademik makale mevcuttur. Bu makalelerde, farklı modeller kullanılarak sınıflandırma sonuçları incelenmiştir. SVM ve Random Forest modelleri kullanılarak VPN tespiti yapılmıştır. Bu çalışmada, Random Forest modeli daha yüksek doğruluk oranı elde etmiştir[1]. Farklı sınıflandırma modelleri (Decision Tree, Naive Bayes, k-NN, SVM) kullanılarak Tor trafiği tespit edilmiştir[2]. Bu çalışmada, SVM modelinin en yüksek doğruluk oranını elde ettiği görülmüştür. Ayrıca, One-Class SVM modeli kullanılarak VPN trafiği tespit edilmiştir[3]. Bu çalışmada, One-Class SVM modelinin yüksek doğruluk oranı elde ettiği görülmüştür.

CIC-Darknet2020 veri seti kullanılarak VPN/NoVPN trafiği sınıflandırması yapılmıştır. Hem Ensemble OneR hem de derin öğrenme yöntemleri kullanılarak sınıflandırma yapılmış ve sonuçlar karşılaştırılmıştır. Sonuçlar, Ensemble OneR modelinin daha yüksek doğruluk ve daha düşük hesaplama maliyeti ile daha iyi performans gösterdiğini ortaya koymuştur[4]. Tor/NoTor trafiği sınıflandırması için farklı sınıflandırma algoritmaları karşılaştırılmıştır. CIC-Darknet2017 veri seti kullanılmıştır. Bu çalışmanın sonuçları, K-NN, SVM ve Decision Tree gibi algoritmaların Ensemble OneR modelinden daha düşük doğruluk oranlarına sahip olduğunu göstermiştir[5–7].Tor trafiğinde kötü amaçlı trafiği tespit etmek için bir makine öğrenmesi yaklaşımı kullanılmıştır. CIC-Darknet2017 veri seti kullanılmıştır. Çalışmada, Naive Bayes, Decision Tree, Random Forest ve SVM gibi farklı sınıflandırma algoritmaları kullanılmıştır. Sonuçlar, SVM ve Random Forest gibi daha karmaşık modellerin daha iyi performans gösterdiğini göstermiştir[8–10]. Bu çalışmaların ortak noktası, siber güvenlik konusunda machine learning tekniklerinin kullanımının incelenmesidir. OneR ve Ensemble OneR modelleri, sınıflandırma için kullanılmıştır ve sonuçlar incelenmiştir. Bu çalışma, basit modellerin bile siber güvenlik alanında önemli sonuçlar elde edebileceğini göstermektedir. Ancak, daha karmaşık modellerin de kullanılması gerekliliği ortaya çıkmaktadır.

CIC-Darknet2020 veri seti üzerinde yapılan çalışmalar sonucunda geliştirilen CICFlowMeter aracı tanıtılmıştır. Bu araç, siber güvenlik analizleri için hafif bir akış özellikleri çıkarma aracı olarak kullanılabilmektedir[11]. Birden çok çalışmada CIC-Darknet2020 veri seti üzerinde gerçekleştirilen bir dizi test sonucunda, DDos saldırılarının SDN ağlarında algılanması için bir makine öğrenimi algoritması kullanılmıştır[12–14]. Son olarak, siber güvenlik alanında makine öğrenimi tekniklerinin kullanımı incelenmiştir. Bu çalışma kapsamında, CIC-Darknet2020 veri seti üzerinde gerçekleştirilen deneysel testler sonucunda yüksek oranda başarı elde edilmiştir.

## 2. Materyal ve Yöntem

### 2.1. Veriseti

CIC-Darknet2020 veri seti[15], Darknet ağlarındaki trafiği içeren bir veri setidir. Toplamda 12 ayrı ağdaki 2,000'den fazla Darknet trafiği kaydını içermektedir. Bu kayıtlar arasında VPN, TOR, SSH ve diğer ağ protokollerinin trafiği bulunmaktadır[16]. Veri seti, siber güvenlik araştırmalarında kullanılmak üzere hazırlanmıştır. Her bir kayıt, aşağıdaki özellikleri içermektedir:

- Kaydın zaman damgası (timestamp)
- Kaynağı ve hedefi belirten IP adresleri
- Kaynağı ve hedefi belirten port numaraları
- Kullanılan ağ protokolü (TCP, UDP, ICMP)
- Kaydın boyutu (bytes)

- Kaydın sınıflandırılması (normal, VPN, TOR, SSH)

Tablo 1'de bu çalışmada kullanılan veri setinde, VPN ve Tor ağları üzerinden gerçekleştirilen normal ve zararlı ağ trafiği verileri bulunmaktadır. Bu veriler VPN kullanılan durumlar için "VPN" ve VPN kullanılmayan durumlar için "NonVPN", Tor kullanılan durumlar için "Tor" ve Tor kullanılmayan durumlar için "NonTor" olarak veri seti etiketlenmiştir. Veri setinde toplam 103,121 örnek bulunmaktadır. Etiketlenmiş örnekler arasında "NonTor" sınıfından 64,804, "NonVPN" sınıfından 20,216, "VPN" sınıfından 16,922 ve "Tor" sınıfından ise sadece 1,179 örnek bulunmaktadır.

**Tablo 1.** Veri setindeki veri tipi ve büyüklükleri oranları.

| **Veri Tipi** | **Büyüklük** |
|---|---|
| **NonTor** | 64804 |
| **NonVPN** | 20216 |
| **VPN** | 16922 |
| **Tor** | 1179 |

Veri seti, VPN trafiği, TOR trafiği, SSH trafiği ve normal trafiği sınıflandırmak için kullanılabilmektedir. Bu sınıflandırmalar, siber güvenlikte çeşitli amaçlar için kullanılabilir, örneğin kötü amaçlı yazılımları tespit etmek, ağ güvenliğini artırmak ve güvenlik açıklarını belirlemektedir[17]. CIC-Darknet2020 veri seti, siber güvenlik araştırmacılarına, siber saldırıları analiz etmek için gerçekçi bir veri kaynağı sunmaktadır. Ancak, veri seti sadece Darknet ağlarında gerçekleşen trafiği içerdiği için tam bir ağ trafiği analizi yapmak mümkün değildir[18].

Bu çalışmada, CIC-Darknet2020 veri kümesinde OneR ve Ensemble OneR modelleri kullanılarak VPN/NoVPN ve Tor/NoTor sınıflandırması yapılmıştır. Veri setinin ayrımı öncesinde, rastgele bir çekirdek seçilmiştir. Çekirdek, modelin başlangıç noktasını belirlemek ve sonuçların tekrarlanabilirliğini sağlamak amacıyla seçilmiştir. Seçilen çekirdek, veri kümesinin ilk sıralama veya belirli bir özelliğine dayanmamaktadır, sadece rasgele bir seçimdir. Bu yaklaşım, araştırmacıların analizlerini başlatmak için rastgele bir başlangıç noktası seçmelerini sağlamakla birlikte sonuçların tarafsız ve yeniden üretilebilir olmasını sağlamak amacıyla kullanılmaktadır. Verileri eğitim, doğrulama ve test kümelerine ayırma seçimini veri kümesi özellik seçimi yaparak, sonuçlarda daha fazla değişkenlik ve dolayısıyla daha az tekrarlanabilirlik sağlanmaktadır.

### 2.2. OneR (One Rule) Modeli

OneR (One Rule), basit bir kural tabanlı sınıflandırma modelidir. Bu model, veri setindeki her özelliğin sınıf etiketi üzerindeki etkisini tek bir kural olarak özetler. OneR, her özellik için en iyi kuralı seçmek ve bu kurala göre sınıflandırmak için veri setini analiz eder. Bu kural, özelliklerin kategorik olması durumunda "en sık görülen sınıf" olarak tanımlanırken, özelliklerin sayısal olması durumunda sınıf etiketlerinin belirli bir aralıkta toplanması ve en fazla sınıfın hangi aralıkta olduğuna bakılarak belirlenir. OneR, basit ve anlaşılır olması nedeniyle küçük veri kümeleri üzerinde etkili sonuçlar verir, ancak büyük veri kümeleri için yeterli olmayabilir.

OneR modeli, sınıflandırma problemleri için basit bir karar ağacı yöntemidir ve kolayca anlaşılabilir bir kural kümesi oluşturur. OneR modelinin performansını değerlendirmektedir. Yazarlar, birçok veri kümesinde OneR'ın en iyi performansı gösterdiğini ve aynı zamanda diğer algoritmaların performansına yakın olduğunu bulmuşlardır[19]. Eğitim verilerini sınıflandırmak için OneR ve ID3 algoritmalarını karşılaştırmaktadır. Sonuç olarak, OneR'ın daha az hesaplama gücüne ve daha az eğitim verisine ihtiyaç duyduğu ve aynı zamanda daha yüksek doğruluk oranlarına sahip olduğu bulunmuştur[20].

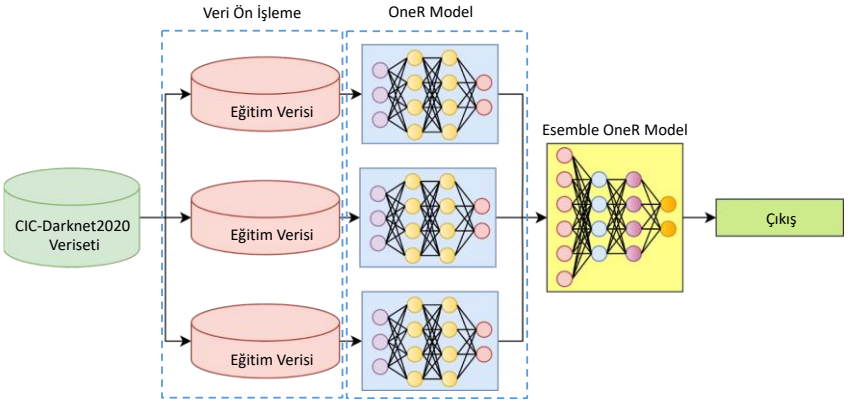
OneR modeli, basit ve anlaşılır bir makine öğrenimi modeli olması sebebiyle birçok uygulama için tercih edilir. OneR'ı yüksek boyutlu verilerin özellik seçiminde kullanmaktadır. Yazarlar, OneR'ın diğer özellik seçim yöntemlerinden daha yüksek bir seçim oranına sahip olduğunu ve aynı zamanda daha az hesaplama gücüne ihtiyaç duyduğunu sonuca varılmıştır[21]. OneR'ı dengesiz veri kümelerinde sınıflandırma yapmak için kullanmaktadır. Yazarlar, OneR'ın diğer yöntemlere göre daha az öğrenme süresine ve daha yüksek doğruluk oranlarına sahip olduğunu sonuca varılmıştır[22].

Bu çalışma, saldırıların tespit edilmesinde sorunlar ikili VPN veya NonVPN olarak ele alınmıştır. Etiket sütunu genellikle sınıfı sunmakta ve birden çok saldırıya sahip bazı sınıflar için bunları ayrı ayrı etiketlenmektedir. Bu çalışmada ilk odak noktası, ikili problemdir, bu nedenle sınıf etiketini daraltılmıştır.

### 2.3. Esemble OneR (One Rule) Modeli

Ensemble OneR modeli, birden fazla OneR modelinin bir araya getirilerek oluşturulmuş bir sınıflandırma modelidir. OneR modelinin temel mantığı, her bir özellik (feature) için en iyi ayrımı yapacak bir kural (rule) oluşturmak ve bu kuralları bir araya getirerek sınıflandırma yapmaktır. Ensemble OneR modeli ise, farklı özellik seçimleri ve veri kümesi örneklemleri kullanarak birden fazla OneR modeli oluşturur ve bunların sonuçlarını birleştirir. Ensemble OneR modeli, farklı OneR modellerinin farklı hatalarını bir araya getirerek genel bir hatayı azaltabilmektedir. Ayrıca, farklı özelliklerin bir arada kullanılması, tek bir özellik kullanımına göre daha iyi sonuçlar verebilmektedir. Ensemble OneR modeli, özellikle küçük boyutlu veri setlerinde başarılı sonuçlar vermektedir. Sınıflandırma problemlerinin yanı sıra, regresyon problemleri için de kullanılabilmektedir. Ensemble OneR modeli, basit bir yapıya sahip olduğu için kolay anlaşılır ve yorumlanabilir sonuçlar vermektedir. Ensemble OneR modelinin kullanımı, özellikle diğer sınıflandırma modellerinin yetersiz kaldığı durumlarda, veri setinin özelliklerini ve örneklem büyüklüğünü değiştirerek yapılan tekrarlı denemeler sonucunda optimize edilebilir.

Şekil 1'de önerilen yöntemin akış şeması gösterilmiştir. Sınıflandırma işlemi yapılmadan önce veri ön işleme adımı gerçekleştirilmiştir. Öncelikle eksik veriler temizlenmiş ve modelin eğitilmesinde katkısı olmayan Flow ID,Fwd Header Length.1, Source IP, Src IP,Source Port, Src Port, Destination IP, Dst IP,Destination Port,Dst Port,Timestamp sütunları çıkarılmıştır. Böylelikle veri seti 78 kolona düşürülmüştür. Veri setinde VPN ve NonVPN ile ilgili rasgele çekirdek sayesinde %20 rasgele seçilerek 7428 satır eğitim verisi ve 29710 satır uzunluğunda da test verisi oluşturulmuştur. Ayrıca Tor ve NonTor veri seti de rastgele seçilerek 13197 satır eğitim ve 52786 satır test verisi elde edilmiştir.




**Şekil 1.** Önerilen yöntemin genel akış şeması.

## 3. Bulgular

### 3.1. Performans Metriklerinin Hesaplanması

Bu çalışmada önerilen yöntemlerin başarısını ölçmek için sırasıyla şu kriterler kullanılmıştır. Eşitlik 1 ve Eşitlik 2'te Doğruluk ve Kesinlik ölçümü yapılmıştır. Bu eşitliklerde DN doğru negatifler, DP doğru pozitifler, YN yanlış negatifler ve YP yanlış pozitifler olmak üzere parametreler kullanılmıştır. Eşitlik 3 ve Eşitlik 4'te Duyarlılık ve Hassasiyet değerleri hesaplanmıştır. Doğruluk ve Kesinlik 'in kümülatif toplamından F-skor Eşlik 5'te hesaplanmıştır.

$$\text{Doğruluk} = \frac{DP+DN}{DP+DN+YP+YN} \quad (1)$$

$$\text{Kesinlik} = \frac{DP}{DP+YN} \quad (2)$$

$$\text{Duyarlılık} = \frac{DN}{DN+YP} \quad (3)$$

$$\text{Hassasiyet} = \frac{DP}{DP+YP} \quad (4)$$

$$\text{F} - \text{Skor} = \frac{2*TP}{2*TP+FP+FN} \quad (5)$$

ROC AUC (Receiver Operating Characteristic Area Under the Curve), bir sınıflandırma modelinin performansını değerlendirmek için kullanılan bir ölçüttür. ROC eğrisi, duyarlılık (sensitivite) ve özgüllük (specificity) arasındaki ilişkiyi gösteren bir grafiktir.

ROC eğrisinin altında kalan alan, yani AUC (Area Under the Curve), sınıflandırma modelinin performansını ölçmektedir. AUC değeri, 0 ile 1 arasında bir değer almaktadır. Eğer AUC değeri 1'e yakınsa, model mükemmel bir performans sergilerken, AUC değeri 0.5'e yaklaştıkça modelin performansı rastgele tahmin etmeye yaklaşmaktadır.

Bu nedenle, ROC AUC eğrisi, bir sınıflandırma modelinin duyarlılık ve özgüllük performansını bir arada değerlendiren ve modelin sınıflandırma yeteneğini özetleyen bir ölçüttür. Yüksek bir ROC AUC değeri, modelin iyi bir ayırma gücüne sahip olduğunu gösterirken, düşük bir ROC AUC değeri, modelin zayıf performans sergilediğini gösterebilmektedir

ROC AUC eğrisinde iki önemli oran hesaplanmaktadır. Bunlardan biri denklem 6'da gösterilen Gerçek Pozitif Oranı'dır. Diğeri de denklem 7'de gösterilen Gerçek Negatif Oranı'dır. Grafiğin x ekseninde daha küçük değerler yani daha düşük yanlış pozitifleri ve daha yüksek gerçek negatifleri göstermektedir. Grafiğin y ekseni de daha büyük değerler yani daha yüksek gerçek pozitifleri ve daha düşük yanlış negatifleri göstermektedir. Bu da şunu göstermektedir iyi bir model grafikte kesikli çizgilerle gösterilen kısım yani eşik değeri 0,5'den daha yüksek bir değer göstermektedir. Bu da modelin iyi bir sonuç ortaya koyduğunu göstermektedir.

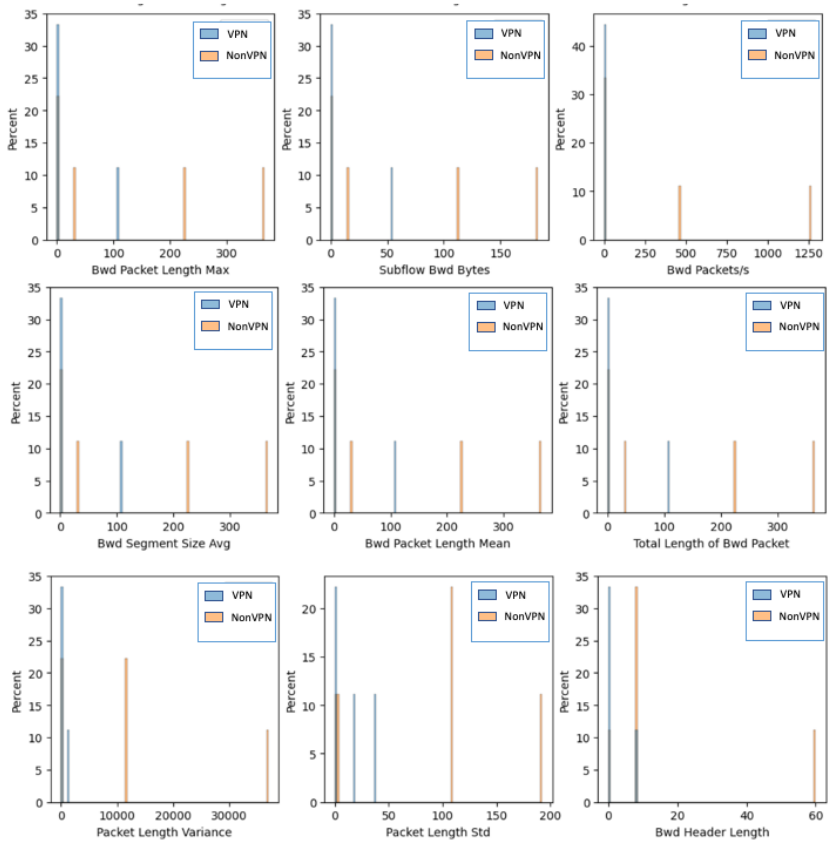
$$Gerçek\ Pozitif\ Oranı = \frac{|DP|}{|YN|+|DP|} \quad (6)$$

$$Gerçek\ Negatif\ Oranı = \frac{|DN|}{|YN|+|DN|} \quad (7)$$

### 3.2. Deneysel Test Sonuçları

CIC-Darknet2020 veri kümesi, VPN ve Tor ağları üzerinden gerçekleştirilen normal ve zararlı ağ trafiği verilerini içermektedir. Bu veri kümesi, eğitim ve test veri setleri olarak ayrılmamıştır, bu nedenle bu çalışmada rastgele bir çekirdek belirleyerek veriyi eğitim, doğrulama ve test veri setlerine ayırılmıştır. Bu çalışmada, çok basit modeller olan One Rule per feature (OneR) ve ensemble OneR kullanarak, VPN/NoVPN ve Tor/NoTor sınıflarını tahmin edilmektedir.

OneR modeli, her bir özellik için bir kural belirler ve tahminlerin doğruluğunu hesaplamak için bunları kullanmaktadır. Şekil 2'de gösterildiği üzere OneR modeli, her bir özellik için bir kural belirlemekte ve tahminlerin doğruluğunu hesaplamak için bunları kullanmaktadır. Böylelikle veri seti üzerinde yapılan hesaplamalar sonucunda, VPN/NoVPN sınıflandırmasında Ensemble OneR modelinin roc-auc puanının 0.779 olduğu tespit edilmiştir. Bu değer, diğer CIC OneR ensemble modellerinden daha düşüktür.



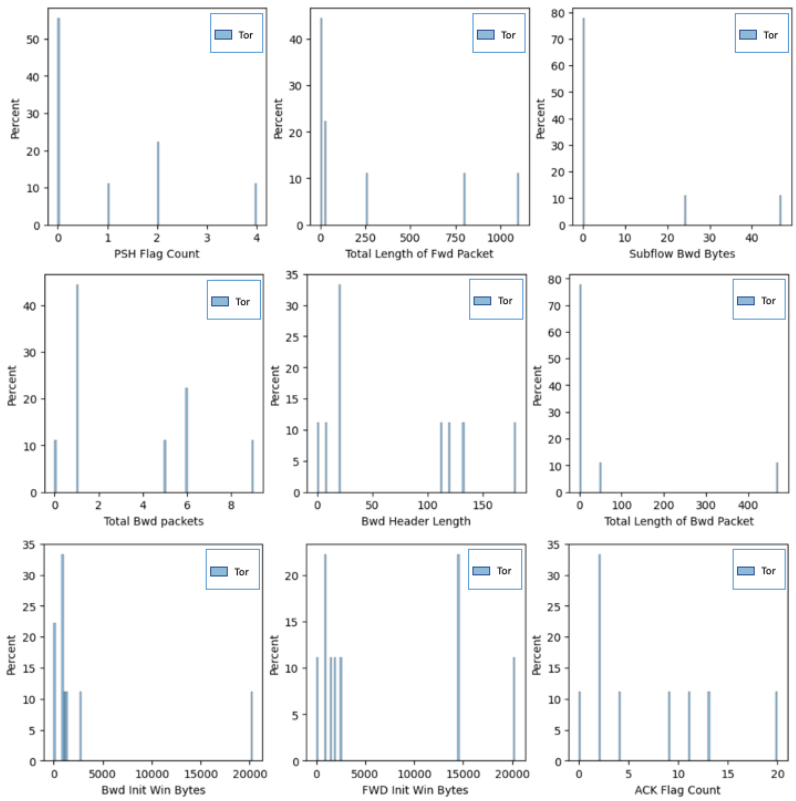

**Şekil 2.** Her bir OneR modelinin VPN/NonVPN tahmin değerleri.

Ensemble OneR modeli, etkili özellikleri kullanarak tek özellikli modeller oluşturur ve bu modelleri tüm örnekler için kullanarak sınıflandırma yapar. Örneklerin yeni tahmin edilen çıktı sınıfı, her bir OneR modelinin tahmin edilen çıktı sınıflarının ortalamasıdır.

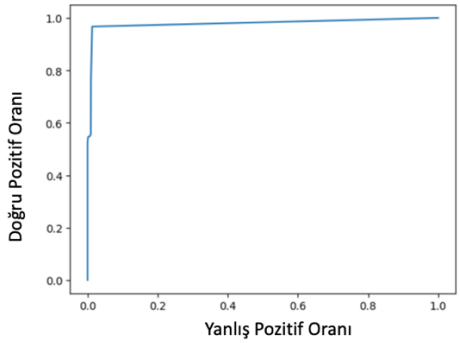
Ensemble OneR modeli, tahminlerin doğruluğunu artırmak için bir dizi OneR modeli kullanmaktadır. Bu model, tüm özellikleri kullanarak tahminler yapar ve her bir OneR modelinden gelen tahminlerin ortalama değerini kullanarak yeni bir tahmin oluşturmaktadır. Şekil 3'te gösterildiği üzere birkaç OneR modelinin sonuçlarını birleştirerek oluşturulan bir sınıflandırma modelidir. Bu model, veri setindeki her bir özelliği ayrı ayrı ele alır ve tek özellikli OneR modellerini kullanarak her bir özellik için bir sınıflandırma modeli oluşturmaktadır. Daha sonra, bu modellerin sonuçları birleştirilerek Tor/NonTor sınıflandırmasına ait bir çıktı sınıfı elde edilmiştir.

ROC-AUC (Receiver Operating Characteristic - Area Under the Curve) ölçütü, bir sınıflandırma modelinin performansını değerlendirmek için kullanılan bir metriktir. AUC değeri, modelin gerçek pozitif oranı (GPO) ve yanlış pozitif oranı (YPO) arasındaki ilişkiyi gösterir.

Bu çalışmadaki ensemble OneR modeli, Tor ve NoTor sınıflarını ayırt etmek için kullanılmıştır. Şekil 4'te gösterildiği üzere modelin ROC-AUC skoru 0.980'dir. Bu, modelin oldukça yüksek bir ayırt etme gücüne sahip olduğunu gösterir. Model, veri setindeki özelliklerin tek tek ele alınması ve basit bir birleştirme yöntemi kullanarak oluşturulması nedeniyle oldukça basit bir modeldir. Ancak, veri setindeki özelliklerin OneR modelleri tarafından doğru bir şekilde tahmin edilebildiği ve sonuçların doğru bir şekilde birleştirildiği için yüksek bir performans elde edilmiştir.




**Şekil 3.** Esemble OneR modelinin Tor/NonTor sınıflandırma sonuçları.




**Şekil 4.** Ensemble OneR modeli, Tor ve NoTor AUC-ROC grafiği.

### 3.2. Önerilen Metodun Performans Sonuçları

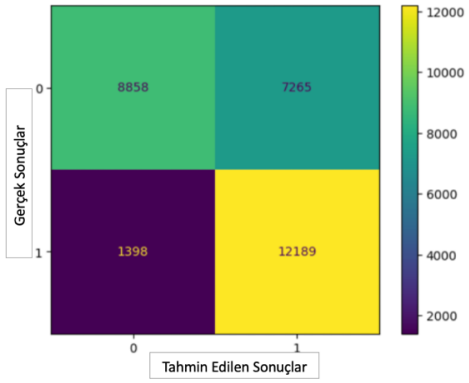
Sınıflandırma performansı karmaşıklık matrisi kullanılarak da değerlendirilmiştir. Karmaşıklık matrisi, sınıflandırma probleminde gerçek ve tahmin edilen sınıf etiketlerine göre oluşan 4 farklı durumu gösteren bir matristir. Bu durumlar gerçek pozitif (GP), yanlış pozitif (YP), gerçek negatif (GN) ve yanlış negatif (YN) olarak adlandırlandırılmaktadır.

Tablo 2'de modelin sınıflandırma performansını ölçmek için kullanılan bir metrikler, bir sınıflandırıcının ne kadar iyi ayırt edici olduğunu göstermektedir. Hassasiyet, doğru pozitif tahminlerin toplam pozitif tahminlere oranını, duyarlılık ise gerçek pozitiflerin toplam pozitifler içindeki oranını ifade etmektedir. F1 ise hassasiyet ve duyarlılığın harmonik ortalamasını ifade etmektedir. Doğruluk, tüm örneklerin doğru şekilde sınıflandırıldığı oranı ifade ederken, dengeli doğruluk, her sınıfın ağırlığını eşit olarak alarak hesaplanan bir doğruluk ölçüsüdür. Burada, VPN/NonVPN problemi için modelin performansı düşükken, Tor/NonTor problemi için oldukça yüksek görünmektedir. Dengelenmiş doğruluk değeri her iki problem için de yüksek olsa da, Hassasiyet değeri Tor/NonTor problemi için düşüktür. Bu sonuçlar, basit bir model olan Ensemble OneR kullanılarak elde edilmiştir.

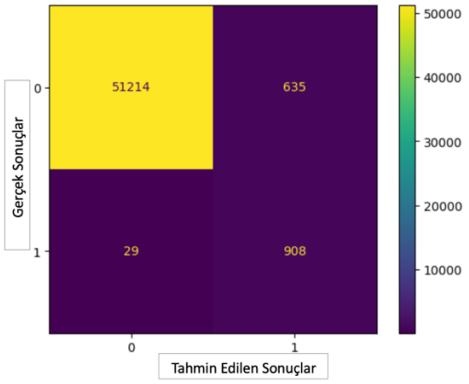
**Tablo 2.** Esemble OneR modelin VPN/NonVPN ve Tor/NonTor değerlerinin perfrormans metriklerin kullanılarak hesaplanan deneysel sonuçlar.

| Model | Doğruluk | Dengelenmiş Doğruluk | Duyarlılık | Hassasiyet | F1 Skoru |
|---|---|---|---|---|---|
| **Esemble OneR(VPN/NonVPN)** | 70.84 | 72.33 | 89.71 | 62.66 | 73.78 |
| **Esemble OneR(Tor/NonTor)** | 98.74 | 97.84 | 96.91 | 58.85 | 73.23 |

Karmaşıklık matrisi, sınıflandırma modelinin doğruluğunu, hassasiyetini, özgüllüğünü ve diğer performans ölçüleri gibi farklı metrikleri hesaplamak için kullanılır. Şekil 5'te VPN/NoVPN ve Şekil 6'da Tor/NoTor sınıflandırma problemleri için ensemble OneR modeli için elde edilen karmaşıklık matrisleri verilmiştir. Bu sonuçlara göre, Ensemble OneR modeli Tor/NoTor sınıflandırma problemi için oldukça yüksek performans göstermiştir. Ancak VPN/NoVPN sınıflandırma problemi için performansı diğer CIC OneR ensemble modellere göre zayıf kalmıştır.




**Şekil 5.** Esemble OneR VPN/NoVPN performans sonucu.




**Şekil 6.** Esemble OneR Tor/NonTor performans sonuçları.

## 4. Sonuçlar ve Tartışma

Bu çalışma, çok basit modeller olan OneR ve ensemble OneR kullanarak VPN/NoVPN ve Tor/NoTor sınıflarının tahmin edilmesi üzerine odaklanmıştır. Veri kümesinde eğitim ve test veri setleri ayrılmamıştır, ancak rastgele bir çekirdek belirlenerek veri seti eğitim, doğrulama ve test veri setlerine ayrılmıştır. Sonuçlar, ensemble

OneR modelinin Tor/NoTor sınıflarının tahmininde yüksek bir performans sergilediğini göstermektedir. ROC-AUC değeri 0.9804, doğruluğu 0.9874 ve dengelenmiş doğruluğu 0.9784 olarak bulunmuştur. Bununla birlikte, VPN/NoVPN sınıflarının tahmininde ensemble OneR modeli daha düşük bir performans sergilemiştir. ROC-AUC değeri 0.7791, doğruluğu 0.7084 ve dengelenmiş doğruluğu 0.7233 olarak bulunmuştur.

Duyarlılık, hassasiyet ve F1 skoru değerleri, her iki model için de Tor/NoTor sınıflarının tahmininde VPN/NoVPN sınıflarından daha yüksek bulunmuştur. Bu sonuçlar, Tor ağındaki trafiğin diğer sınıflardan daha kolay bir şekilde ayırt edilebileceğini göstermektedir. Ancak, ensemble OneR modelinin VPN/NoVPN sınıfları için daha düşük bir performans sergilemesi, bu sınıfların birbirine daha benzer olması ve birçok benzer özellik taşıması nedeniyle olabilmektedir. Bu nedenle, daha karmaşık modellerin kullanılması veya farklı özelliklerin keşfedilmesi bu sınıfların doğru bir şekilde ayırt edilmesine yardımcı olmaktadır. Önerilen çalışmamızın aynı veriseti ve benzer çalışmaların karşılaştırılması Tablo 3'te verilmiştir.

**Tablo 3.** Önerilen çalışmanın diğer çalışmlarla karşılaştırılması.

| Çalışma | Yıl | Önerilen Model | Doğruluk(%) |
|---|---|---|---|
| [18] | 2023 | Ensemble Öğrenme | 96.74 |
| [23] | 2021 | Evrişimli Sinir Ağı (CNN) ve K-Means (KM) | 97.40 |
| [24] | 2020 | Yapay Sinir Ağı ve Apache Spark (ANN-AS) | 96.66 |
| [25] | 2021 | Tekrarlayan Sinir Ağı (RNN) | 94.51 |
| Mevcut Çalışma | 2023 | OneR ve Ensemble OneR modelleri | 98.74 |

Sunduğumuz yöntem ile karşılaştırdığımız çalışmalar, aynı veri setini kullanmış ancak farklı makine öğrenimi ve yapay zekâ tekniklerini içeren çalışmalardır. Ensemble öğrenme yöntemiyle birbirinden farklı algoritmalar olan Rasgele Orman Algoritması, Destek Vektör Makinaları ve Yapay Sinir Ağları algoritmaları kullanılmıştır [18]. Sınıflandırma aşamasında ise Lojistik Regresyon yöntemi tercih edilmiştir. Farklı algoritmaların kullanılması, ensemble öğrenme yönteminde her bir algoritmanın performansının farklı olmasına yol açmış ve genel başarıyı düşürmüştür. Önerdiğimiz çalışmamızda ise Ensemble OneR yönteminde birbirinden farklı algoritmaları yerine OneR algoritması kullanılmış farklı performans yerine birbirine yakın performanslar elde edilerek daha yüksek genel başarı elde edilmiştir. Yapay sinir ağları ve Apache Spark motoru kullanılarak VPN ve VPN olmayan ağ trafiğinin doğru bir şekilde sınıflandırılması için bir yaklaşım sunulmaktadır [23]. VPN sınıflandırması için %96.76 ve VPN olmayan sınıflandırması için %92,56 doğruluk elde etmektedir. Bu da şifreli ağlarda verimli ve etkili trafik analizi yapmak için yetersizdir çünkü Tor ve Tor olmayan ağlarda deneysel testler yapılmamıştır. Önerdiğimiz yöntemde ise hem VPN ve VPN olmayan hem de Tor ve Tor olmayan trafik analizlerini deneysel testlerde kullanmıştır. Önerdiğimiz çalışmada Tor sınıflandırması için %98.74 Tor olmayan sınıflandırma için %97.84 başarı elde edilmiştir. Gerçek zamanlı olarak sinir ağları çerçevesini kullanan bir yaklaşım sunulmaktadır [24]. Ancak, uygun bir mimariyi belirlemek için önceden işlem yapılması gereken özel ve zaman alıcı bir işlem olması, veri analizi ve açıklama modellerinin araştırma karmaşıklığı eklemesi ve bu nedenle yüksek bir araştırma maliyetinin olmasına sebep olmaktadır. Önerdiğimiz yöntem uygun ve belli bir mimariyle işlem yapıldığı için önceden işlem yapılmasına gerek duymadan kısa zamanda ve araştırma maliyetini düşüren sonuçlar elde edilmiştir. Bu nedenle, önerdiğimiz modelin benzer veri seti ve çalışmalarla karşılaştırıldığında daha yüksek başarı oranı, doğruluk, önceden işlem yapılmasına gerek duymadan ve kısa zaman içinde yüksek başarı sağladığı sonucuna ulaşılmıştır.

Bu çalışma, veri kümesinin basit modellerle bile doğru bir şekilde sınıflandırılabileceğini göstermektedir. Ancak, daha karmaşık modellerin kullanılması ve farklı özelliklerin keşfedilmesi, daha yüksek performans elde etmek için gereklidir.

## 5. Sonuç ve Öneriler

Bu çalışmada, CIC-Darknet2020 veri kümesindeki VPN/NoVPN ve Tor/NoTor sınıflarının tahmin edilmesi için One Rule per feature (OneR) ve ensemble OneR modelleri kullanılmıştır. Model performansı, doğruluk, dengelenmiş doğruluk, duyarlılık, hassasiyet ve F1 skoru ölçütleri kullanılarak değerlendirilmiştir. Sonuçlar, ensemble OneR modelinin Tor/NoTor sınıfı için oldukça yüksek doğruluk, dengelenmiş doğruluk ve duyarlılık

değerlerine sahip olduğunu göstermektedir. Ancak, VPN/NoVPN sınıfı için düşük hassasiyet ve F1 skoru değerleri dikkat çekmektedir.

Bu çalışma, OneR ve ensemble OneR modelleri, VPN/NoVPN ve Tor/NoTor sınıflarının tahmininde iyi performans göstermiştir. Ancak, VPN/NoVPN sınıflarında düşük hassasiyet değeri dikkat çekmektedir. Bu sonuçlar, benzer veri kümelerinde de benzer modellerin kullanılabileceğini göstermektedir. Ancak, VPN/NoVPN sınıfı için modelin daha iyi performans göstermesi gerektiğini göstermektedir. Bu durumun nedeni, VPN ve NoVPN trafiği arasındaki farkın çok küçük olması ve bu nedenle modele doğru sınıflandırma yapmak için yeterli özniteliklerin olmaması olabilmektedir. Bu sorunu çözmek için daha kapsamlı bir öznitelik seçimi veya daha karmaşık bir model kullanılabilmektedir. Sonuç olarak, bu çalışma, VPN/NoVPN ve Tor/NoTor sınıflarının tahmininde OneR ve ensemble OneR modellerinin kullanılabileceğini göstermektedir. Ancak, bu modellerin daha iyi performans göstermesi için daha kapsamlı bir öznitelik seçimi veya daha karmaşık bir model kullanılması önerilmektedir.

Gelecekte yapılacak çalışmalar, siber güvenlik alanında VPN/NonVPN ve Tor/NonTor sınıflandırması üzerine odaklanarak ve daha geniş kapsamlı araştırma yapılması planlanmaktadır. Bu kapsamda model iyileştirme ve hiperparametre ayarlaması yaparak sınıflandırma modellerinin performansını artırmak için model iyileştirme teknikleri kullanılacaktır. Bu, modelin doğruluğunu, hassasiyetini ve duyarlılığını optimize etmeye yardımcı olacaktır.

## Kaynaklar


[1] Abu Al-Haija Q, Krichen M, Abu Elhaija W. Machine-learning-based darknet traffic detection system for IoT applications. Electronics 2022; 11: 556.

[2] Iliadis LA, Kaifas T. Darknet traffic classification using machine learning techniques. In: 2021 10th International Conference on Modern Circuits and Systems Technologies (MOCAST). IEEE, 2021, pp. 1–4.

[3] Lotfollahi M, Jafari Siavoshani M, Shirali Hossein Zade R, et al. Deep packet: A novel approach for encrypted traffic classification using deep learning. Soft Comput 2020; 24: 1999–2012.

[4] Afuwape AA, Xu Y, Anajemba JH, et al. Performance evaluation of secured network traffic classification using a machine learning approach. Comput Stand Interfaces 2021; 78: 103545.

[5] Lingyu J, Yang L, Bailing W, et al. A hierarchical classification approach for tor anonymous traffic. In: 2017 IEEE 9th International conference on communication software and networks (ICCSN). IEEE, 2017, pp. 239–243.

[6] Sarkar D, Vinod P, Yerima SY. Detection of Tor traffic using deep learning. In: 2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2020, pp. 1–8.

[7] Rao Z, Niu W, Zhang X, et al. Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Netw Appl 2018; 11: 592–601.

[8] Hu X, Gao Y, Cheng G, et al. An Adversarial Learning-based Tor Malware Traffic Detection Model. In: GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022, pp. 74–79.

[9] Johnson C, Khadka B, Ruiz E, et al. Application of deep learning on the characterization of tor traffic using time based features. J Internet Serv Inf Secur 2021; 11: 44–63.

[10] Cuzzocrea A, Martinelli F, Mercaldo F, et al. Tor traffic analysis and detection via machine learning techniques. In: 2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017, pp. 4474–4480.

[11] Ali BH, Sulaiman N, Al-Haddad SAR, et al. DDoS Detection Using Active and Idle Features of Revised CICFlowMeter and Statistical Approaches. In: 2022 4th International Conference on Advanced Science and Engineering (ICOASE). IEEE, 2022, pp. 148–153.

[12] Rahman O, Quraishi MAG, Lung C-H. DDoS attacks detection and mitigation in SDN using machine learning. In: 2019 IEEE world congress on services (SERVICES). IEEE, 2019, pp. 184–189.

[13] Polat H, Polat O, Cetin A. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability 2020; 12: 1035.

[14] Banitalebi Dehkordi A, Soltanaghaei M, Boroujeni FZ. The DDoS attacks detection through machine learning and statistical methods in SDN. J Supercomput 2021; 77: 2383–2415.

[15] Habibi Lashkari A, Kaur G, Rahali A. Didarknet: A contemporary approach to detect and characterize the darknet traffic using deep image learning. In: 2020 the 10th International Conference on Communication and Network Security. 2020, pp. 1–13.

[16] Rust-Nguyen N. Darknet Traffic Classification.

[17] Anyanwu GO, Lee J-M, Kim D-S. Optimized Ensemble Learning Algorithm for Hidden Malicious Traffic Detection in VANET. 2021; 111–112.

[18] Almomani A. Darknet traffic analysis, and classification system based on modified stacking ensemble learning algorithms. Inf Syst E-bus Manag 2023; 1–32.

[19] Holte RC. Very simple classification rules perform well on most commonly used datasets. Mach Learn 1993; 11: 63–90.

[20] Anuradha C, Velmurugan T. A comparative analysis on the evaluation of classification algorithms in the prediction of students performance. Indian J Sci Technol 2015; 8: 1–12.
[21] Gangavarapu T, Patil N. A novel filter–wrapper hybrid greedy ensemble approach optimized using the genetic algorithm to reduce the dimensionality of high-dimensional biomedical datasets. Appl Soft Comput 2019; 81: 105538.
[22] Liu X-Y, Wu J, Zhou Z-H. Exploratory undersampling for class-imbalance learning. IEEE Trans Syst Man, Cybern Part B 2008; 39: 539–550.
[23] Li Y, Lu Y, Li S. EZAC: Encrypted Zero-day Applications Classification using CNN and K-Means. In: 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD). IEEE, 2021, pp. 378–383.
[24] Aswad SA, Sonuç E. Classification of VPN network traffic flow using time related features on Apache Spark. In: 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). IEEE, 2020, pp. 1–8.
[25] Demertzis K, Tsiknas K, Takezis D, et al. Darknet traffic big-data analysis and network management for real-time automating of the malicious intent detection process by a weight agnostic neural networks framework. Electronics 2021; 10: 781.