**RAWNET-2**

**RawNet-2 Nedir?**

Son yıllarda ses sinyalleri üzerinde çalışan yapay zeka modelleri, özellikle biyometrik tanıma, konuşmacı doğrulama ve anomali tespiti gibi alanlarda önemli ilerlemeler kaydetmiştir. Geleneksel yöntemlerde genellikle **MFCC** (Mel-Frequency Cepstral Coefficients) veya **spectrogram** gibi özellik çıkarım teknikleri kullanılırken, bu yöntemlerin manuel mühendisliğe olan bağımlılığı nedeniyle esneklikleri sınırlıdır. Bu probleme çözüm olarak önerilen **RawNet** ailesi, ham ses dalgalarını doğrudan işleyebilen uçtan uca derin öğrenme modelleridir. Bu ailenin geliştirilmiş versiyonu olan **RawNet-2**, güçlü mimarisi ve performansı ile öne çıkmaktadır.

**RawNet-2**, ses sinyallerini herhangi bir ön işlem veya özellik mühendisliğine gerek kalmadan doğrudan işleyebilen bir **1D Konvolüsyonel Sinir Ağı (CNN)** + **GRU (Gated Recurrent Unit)** mimarisine sahip derin öğrenme modelidir. 2020 yılında **Jung et al.** tarafından geliştirilen bu model, özellikle **konuşmacı tanıma** ve **sahtekarlık tespiti (spoofing detection)** gibi görevlerde oldukça başarılı sonuçlar elde etmiştir.

**Mimari Özellikleri**

RawNet-2 aşağıdaki katmanlardan oluşur:

**1. Ön Blok (Front-end Layer)**

* Ham ses dalgaları doğrudan bu katmana girer.
* 1D convolution + batch normalization + LeakyReLU kullanılır.
* Ses dalgasından temel frekans özelliklerini çıkarır.

**2. Residual Blocks (Artık Bloklar)**

* Derin öğrenme modellerinde öğrenmeyi stabilize etmek için kullanılır.
* Bu bloklar sayesinde model, ses verisindeki ince detayları öğrenebilir.

**3. GRU Katmanı (Zaman Bağımlı Öğrenme)**

* GRU, ses sinyalinin zamanla değişen yapısını anlamak için kullanılır.
* Bu yapı sayesinde model, uzun vadeli bağımlılıkları öğrenebilir.

**4. Feature Aggregation + Dense Layers**

* Özellikler özetlenir ve yoğun katmanlarla (fully connected) sınıflandırma yapılır.
* Bu aşamada konuşmacı embedding’i (veya anomali skorları) oluşturulur.

**5. Output**

* Softmax veya benzeri aktivasyonla sınıflandırma yapılır (örneğin: "anormal" vs "normal").

**Yenilikçi Yönleri**

| **Özellik** | **Açıklama** |
| --- | --- |
| Uçtan Uca Öğrenme | Özellik mühendisliği gerektirmez, ham sesle çalışır. |
| Feature Map Scaling | Katmanlar arası dikkat (attention) mekanizmasıyla önemli özellikleri vurgular. |
| Residual Block'lar | Derin yapıyı daha verimli öğrenmeye yardımcı olur. |
| Hafiflik | IoT ve IoMT gibi düşük güçlü cihazlara uygulanabilecek kadar optimize edilebilir. |

**Neden RawNet-2?**

Geleneksel sistemlerde ses verisi önce **MFCC**, **mel-spectrogram** gibi temsillere dönüştürülür ve bu temsiller makine öğrenmesi modellerine giriş olarak verilir. Bu süreç zaman alıcı ve insan müdahalesine açık bir süreçtir. RawNet-2, bu süreci atlayarak:

* Manuel özellik mühendisliğine olan bağımlılığı azaltır.
* Ham veriden öğrenmeyi mümkün kılar.
* Özellikle **deepfake ses**, **spoofing**, **anomaly detection** gibi uygulamalarda çok daha sağlam modeller üretir.

**Performans**

RawNet-2, konuşmacı tanıma alanında kullanılan **VoxCeleb1** veri seti üzerinde %2.56 EER (Equal Error Rate) ile çalışarak, o dönemki en iyi sonuçlardan birini elde etmiştir. Bu başarı, modelin farklı ses kaynakları veya anomali tespiti gibi görevlerde de etkili olabileceğini göstermektedir.

**Kullanım Alanları**

* **Konuşmacı Tanıma** (Speaker Recognition)
* **Sahtekarlık Tespiti** (Anti-Spoofing)
* **IoT ve IoMT Güvenlik Sistemleri** (Anomali tespiti)
* **Sesli Kimlik Doğrulama** (Voice Authentication)
* **Duygu Analizi** (Emotion Recognition)

**IoMT Cihazlarında Kullanımı**

IoMT (Internet of Medical Things) cihazlarında veri genellikle **sensörlerden gelen sürekli sinyaller** şeklindedir. RawNet-2’nin ses dalgalarına benzer bu veri yapısıyla doğrudan çalışabilme yeteneği sayesinde:

* Anormal davranışların/saldırıların ses/sinyal verisi üzerinden tespiti yapılabilir.
* Saldırıya uğrayan cihazların sesli uyarı mekanizmaları analiz edilebilir.
* Sesli hasta komutlarının doğruluğu kontrol edilebilir.

Bu özellikleriyle RawNet-2, IoMT ortamlarında **gerçek zamanlı, kaynak dostu ve yüksek doğrulukta bir anomali tespit sistemi** için güçlü bir temel sunar.

**Uygulamada Dikkat Edilmesi Gerekenler**

* Ham ses verisi genellikle çok büyük boyutlu ve gürültülüdür; bu nedenle veri temizliği önemlidir.
* Modelin yüksek başarı göstermesi için yeterli çeşitliliğe sahip veri seti gerekir.
* IoMT gibi gömülü sistemlerde çalıştırılacaksa, model sadeleştirme (pruning, quantization) yapılmalıdır.

**Örnek Uygulamalar**

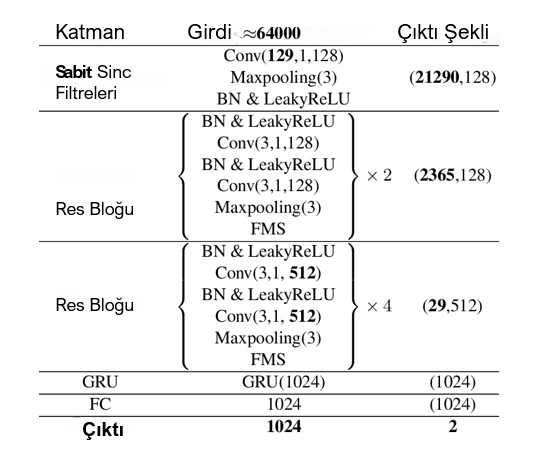
1. **IoMT Ağ Güvenliği**: IoMT cihazlarından gelen ses/sinyal verileri analiz edilerek, olası ağ saldırıları (DoS, MITM vb.) tespit edilebilir.
2. **Konuşmacı Kimlik Doğrulama**: Bankacılık gibi alanlarda sesle kimlik doğrulama yapılabilir.
3. **Anomali Tespiti**: Fabrika makinelerinden gelen ses verilerinde arıza tespiti.

**Sonuç**

RawNet-2, ham ses verisiyle doğrudan çalışabilen modern ve güçlü bir derin öğrenme mimarisidir. Özellikle veri ön işleme adımlarını en aza indirerek esneklik ve doğruluk arasında dengeli bir yapı sunar. IoMT gibi sınırlı kaynaklara sahip sistemlerde optimize edilerek kullanılması, hem güvenlik hem de performans açısından büyük katkı sağlayabilir.

**Model Eğitimi**

Projede kullanılacak RAWNET2 mimarisi Şekil 1’ de verilmiştir. İlk katmanlarda, RawNet2’nin sinir ağı yapısı ham veri üzerinden doğrudan özellik çıkarımı yapabilecek şekilde ayarlanacaktır. Modelin giriş katmanlarında uygulanan sinir ağı yapısı, paketlerin içeriğindeki anormal örüntüleri belirlemekte yardımcı olacaktır. Örneğin, ağ trafiğinde normalin dışında kalan paket davranışlarını tespit etmek için modelin düşük frekansta tekrar eden saldırı örüntülerini tanımlaması sağlanacaktır. Özellikle sınırlı veri işleme kapasitesine sahip olan IoMT cihazlarında modelin hızlı yanıt verebilmesi amacıyla model parametreleri optimize edilip gereksiz katmanlar azaltılacaktır.



Şekil 1. RAWNET2 mimarisi

Modelin eğitilmesi ve doğrulanması için veri toplama aşamasında seçilen veri setleri kullanılacaktır. Veri, %80 eğitim ve %20 doğrulama oranıyla ayrılacak ve modelin performansını en üst düzeye çıkarmak amacıyla çapraz doğrulama uygulanacaktır. Çapraz doğrulama yöntemi ile model, farklı veri alt kümeleri üzerinde test edilerek daha geniş bir örneklem üzerinden eğitilmiş olacak ve bu sayede fazla öğrenme (overfitting) riskini minimize edecektir. Normalizasyon işlemi sayesinde ham verinin homojen bir ölçeğe getirilmesi sağlanarak eğitim sırasında modelin daha kararlı çalışması sağlanacaktır. Özellik çıkarma ve anomali algılama aşamasında model, ham ağ verisi üzerinden saldırıya işaret eden belirgin özellikleri öğrenerek belirli bir eşik değerini aşan davranışları anomali olarak sınıflandıracaktır. RAWNET2 modelinin ilk katmanları, IoMT trafiğinde bulunan ince özellikleri çıkarmakta kullanılırken, derin öğrenme yapısı daha ileri katmanlarda bu özellikleri anomali tespiti yapacak şekilde işleyecektir.[2]

Eğitim süreci boyunca modelin doğruluk, hassasiyet, geri çağırma (recall) ve F1 skoru gibi performans ölçütleri ile değerlendirilmesi yapılacaktır. Eğitim sürecinde modelin IoMT ağ trafiğinde meydana gelen anormallikleri doğru bir şekilde tanımlayabilmesi için hiper parametre ayarları sürekli olarak optimize edilecektir. Bu aşamada öğrenme oranı, katman sayısı ve aktivasyon fonksiyonları gibi parametreler, modelin tespit doğruluğunu en üst seviyeye çıkaracak şekilde ayarlanacaktır. Ayrıca, modelin anormal paketleri yüksek doğrulukla belirleyebilmesi için yanlış pozitif ve yanlış negatif oranları detaylı bir şekilde analiz edilip bu oranların azaltılması hedeflenecektir.

**Sınıflandırma**

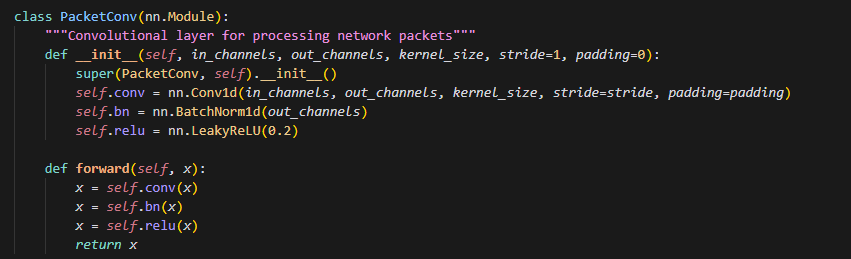
Sınıflandırma aşamasında eğitimi tamamlanan model gerçek zamanlı IoMT trafiğine maruz bırakılacak ve bu veriler üzerinden test edilecektir. Modelin ağ üzerinden gelen paketleri analiz ederek kötücül paketleri yüksek hız ve doğrulukta tespit etmesi beklenmektedir. Bu aşamada doğruluk, geri çağırma, F1 skoru, yanlış pozitif ve yanlış negatif gibi metriklerle performans analizi yapılacaktır ve model üzerinde gerekli iyileştirmeler gerçekleştirilecektir.

Son olarak raporlama ve dokümantasyon adımında test sonuçları detaylı olarak raporlanacaktır. Modelin performans değerlendirmeleri, tespit özetleri ve tespit aşamasında yapılan gözlemler gibi önemli bilgiler kaydedilerek sonuç raporu hazırlanacaktır.

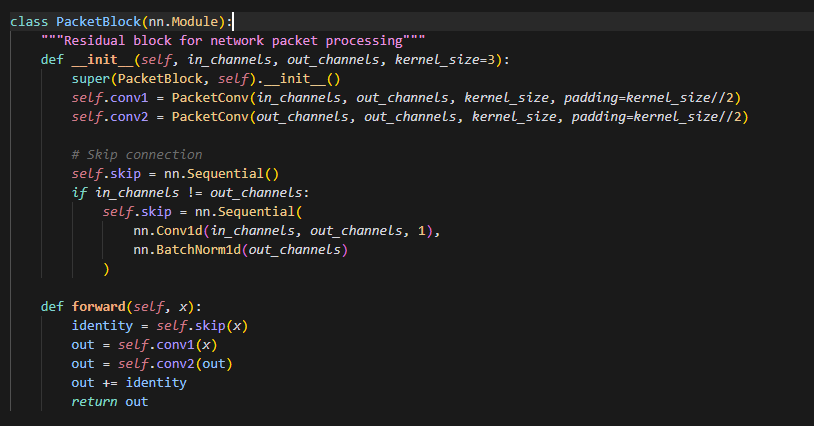
Bu bütünleşik model geliştirme ve eğitim süreci, RawNet2 modelinin IoMT ortamında gerçek zamanlı olarak güvenilir saldırı tespiti sağlamasını mümkün kılacaktır. Böylece IoMT ağ trafiğinde meydana gelen saldırılar daha hızlı tespit edilerek sağlık hizmetlerinde veri güvenliği ve hasta güvenliğinin artırılması sağlanacaktır.

**Model Üzerinde Yapılan Değişiklikler ve İlk Eğitim Sonuçları**

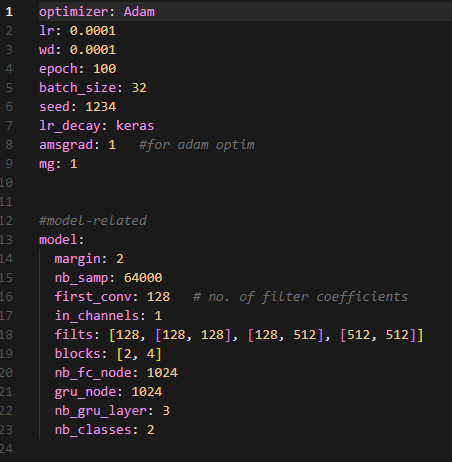
Orijinal RawNet-2 mimarisi ağ trafiği anomali tespiti için yeniden düzenlenmiştir. Orijinal modelde ses işleme için kullanılan SincConv katmanları kaldırılmış, yerine ağ paketlerinden gelen özellikleri işleyebilecek PacketConv ve PacketBlock katmanları eklenmiştir. Ayrıca, veri kümesindeki protokol, kaynak, hedef gibi kategorik alanlar LabelEncoder ile sayısal hale getirilmiştir. Modelin son katmanları ve eğitim parametreleri de ağ trafiği için optimize edilmiştir.



Şekil 2. PacketConv sınıfı



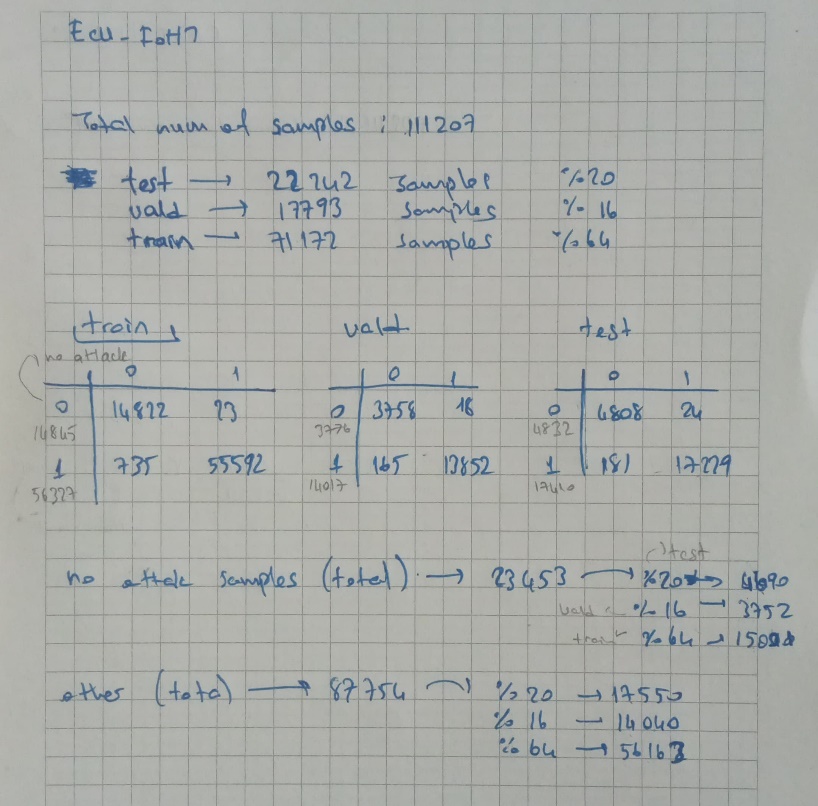
Şekil 3. PacketBlock sınıfı

metin, ekran görüntüsü, yazılım içeren bir resim

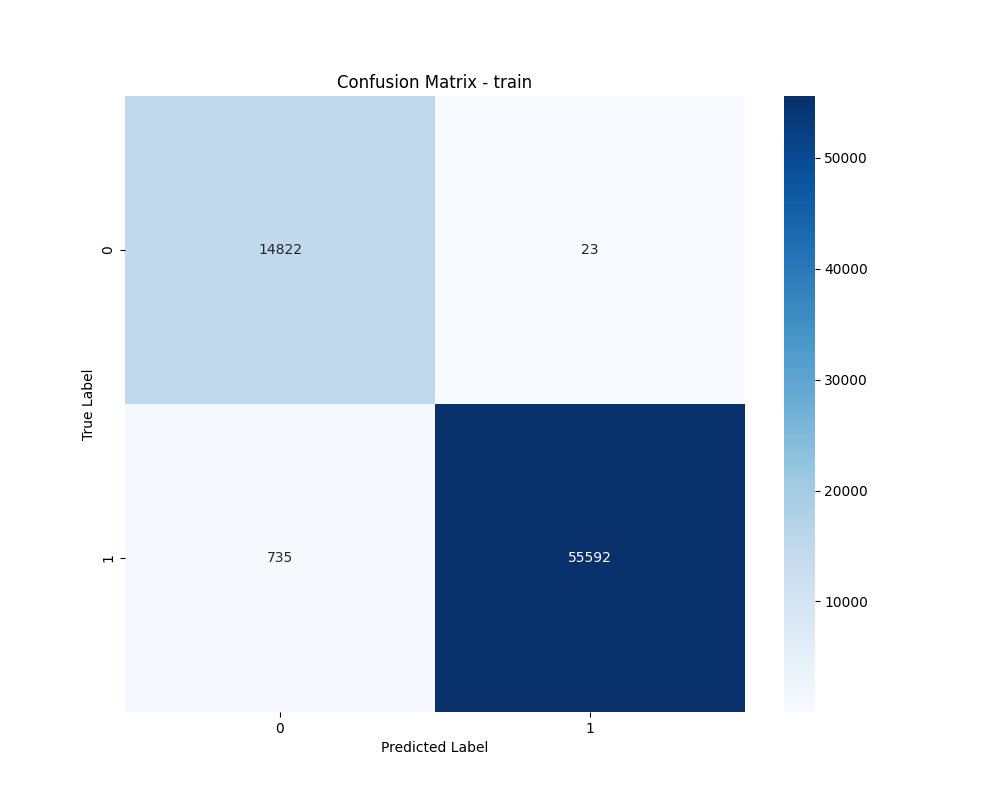
Yapay zeka tarafından oluşturulan içerik yanlış olabilir.

Şekil 4. Orijinal (solda) ve modifiye edilmiş (sağda) model parametreleri

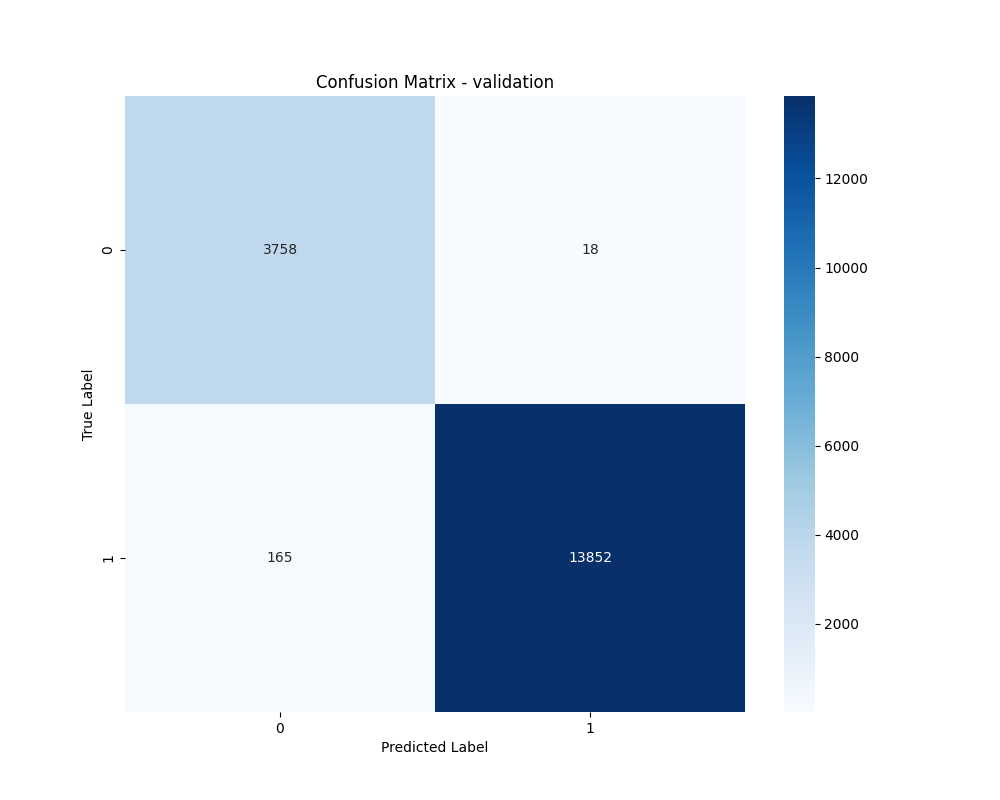
Eğitimde kullanılan ECU\_IoHT veri seti, toplam 111.207 örnekten oluşmaktadır. Bu örnekler %64 eğitim, %16 doğrulama ve %20 test olarak ayrılmıştır. Sınıf dağılımları ve karışıklık matrisleri aşağıda verilmiştir:



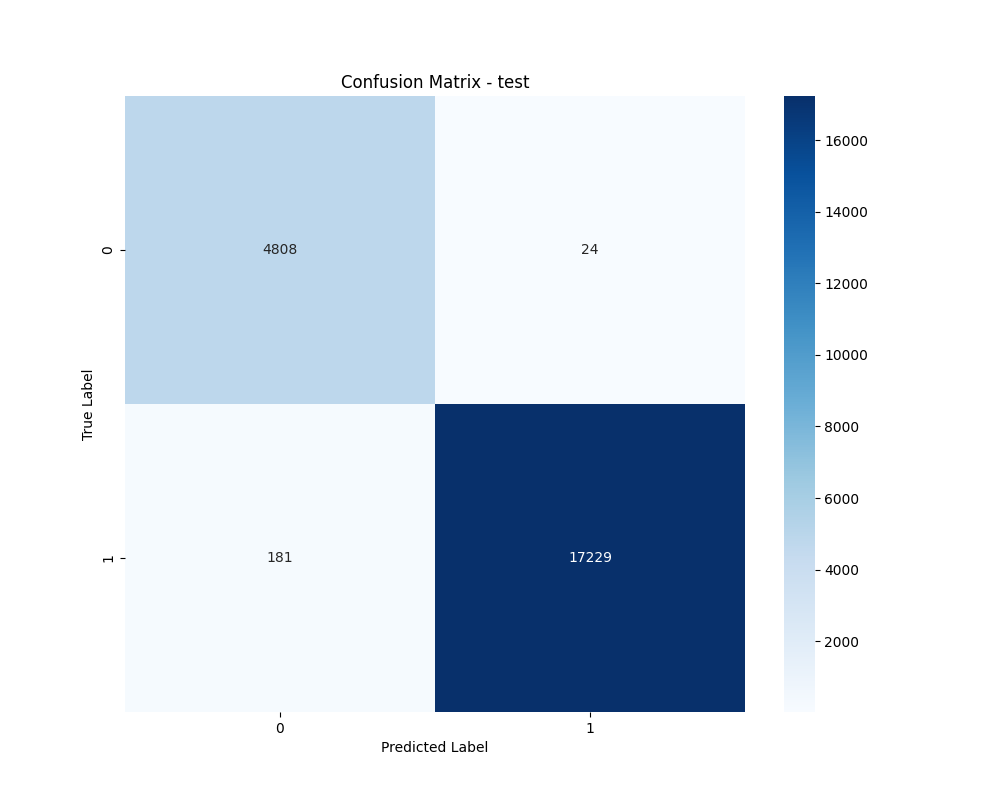
Şekil 5. Veri setinde bulunan sınıfları gösterir



Şekil 6. Eğitim sonuçları



Şekil 7. Validasyon sonuçları



Şekil 8. Test sonuçları

Test seti için hesaplanan metrikler:

- Doğruluk (Accuracy): %99,17

- Kesinlik (Precision): %99,87

- F1 Skoru: %99,43

**İyileştirme Önerileri**

Mevcut model, belirli bir veri kümesi ve ön işleme adımları için optimize edildi. Farklı veri kümeleri veya gerçek zamanlı ağ paketleriyle çalışmak için iyileştirmeler yapılmalı. Bu rapor şimdiye kadar yaptığımız çalışmaların sonuçlarını içeriyor. Çalışmamızın devamında bizim iyileştirilebileceğini düşündüğümüz kısımlar:

* Farklı ağ veri kümelerinde özellik isimleri ve formatları değişebilir. Modelin esnekliğini artırmak için otomatik özellik seçimi ve daha gelişmiş kategorik kodlama yöntemleri eklenebilir.
* Model hazır bir veri setiyle eğitildi ve test edildi, gerçek zamanlı gelen paketler üzerinde aynı keskinlikte çalışıp çalışmadığı test edilerek gerekli düzenlemeler yapılabilir.
* Modelin farklı ağ ortamlarında da yüksek performans göstermesi için çapraz doğrulama ve farklı veri setleriyle test edilebilir.
* Model veri örneklerini binary sınıflandırmada (normal-anormal) başarılı ancak anormal paketleri saldırı türlerine göre sınıflandırma başarısı henüz ölçülmedi. Bu sınıflandırma için düzenlemeler yapılıp sonuçlar gözlemlenebilir.