ANOMALİ TESPİTİ YAKLAŞIMIYLA SALDIRI TESPİTİ

Burak EKİCİ

YÜKSEK LİSANS TEZİ
SAVUNMA TEKNOLOJİLERİ ANA BİLİM DALI

SİVAS BİLİM VE TEKNOLOJİ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ARALIK 2022

Burak EKİCİ tarafından hazırlanan "ANOMALİ TESPİTİ YAKLAŞIMIYLA SALDIRI TESPİTİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Sivas Bilim ve Teknoloji Üniversitesi Savunma Teknolojileri Ana Bilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Danışman: Doç. Dr. Hidayet TAKCI
Bilgisayar Yazılımı Ana Bilim Dalı, Sivas Cumhuriyet Üniversitesi Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……..……..

Başkan: Doç. Dr. Hidayet TAKCI
Bilgisayar Yazılımı Ana Bilim Dalı, Sivas Cumhuriyet Üniversitesi ...……
Bu tezin, kapsam ve kalite olarak Yüksek Lisans olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Kali GÜRKAHRAMAN
Kontrol ve Kumanda Sistemleri Ana Bilim Dalı, Sivas Cumhuriyet Üniversitesi ……
Bu tezin, kapsam ve kalite olarak Yüksek Lisans olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Halit BAKIR
Bilgisayar Bilimleri Ana Bilim Dalı, Sivas Bilim ve Teknoloji Üniversitesi .....……
Bu tezin, kapsam ve kalite olarak Yüksek Lisans olduğunu onaylıyorum.

Tez Savunma Tarihi: 20/12/2022

Jüri tarafından kabul edilen bu çalışmanın Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum

……..…….

Doç. Dr. Emre BİÇER

Lisansüstü Eğitim Enstitüsü Müdürü

ETİK BEYAN

Sivas Bilim ve Teknoloji Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

……..
Burak EKİCİ
20/12/2022

ANOMALİ TESPİTİ YAKLAŞIMIYLA SALDIRI TESPİTİ

(Yüksek Lisans Tezi)

Burak EKİCİ

SİVAS BİLİM ve TEKNOLOJİ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Aralık 2022

ÖZET

Bilgisayar ağlarına yapılan saldırılar günden güne artarken ve saldırıların nitelikleri de sürekli olarak değişmektedir. Ağ saldırıları, bilgisayar ağlarına zarar vererek bilgi güvenliğini ortadan kaldırmaktadır. Bu durum kişiler, şirketler, kurumlar ve hatta devletler için büyük bir risk oluşturmaktadır. Ağ trafiğinin analizi ve böylece saldırıların ortaya çıkarılabilmesi için Saldırı Tespit Sistemlerinden yararlanılmaktadır. Saldırı türlerini tanıyacak şekilde oluşturulan bu sistemlerin gelişimleri de artan saldırı tiplerine göre sürekli devam etmektedir. Bu çalışmada makine öğrenmesi teknikleri yardımıyla anormallik tabanlı bir saldırı tespit sistemi oluşturulması amaçlanmıştır. Çalışma sürecinde; Yinelemeli Özellik Elemesi, İleri Yönelimli Seçim, Rastgele Orman, Karar Ağaçları, Naive Bayes, Lojistik Regresyon ve Ekstrem Gradyan Artırma gibi algoritmalardan yararlanılmış ve Doğruluk, Kesinlik, Duyarlılık ve F1 gibi metrikler ile değerlendirmeler yapılmıştır. Ayrıca model değerlendirme için ROC eğrilerinden yararlanılmıştır. Bahsi geçen bu algoritmalardan elde edilen sonuçlar karşılaştırılarak en etkili modelin bulunması için CICIDS 2017 veri seti kullanılmıştır. Çalışma kapsamında Yinelemeli Özellik Elemesi ve İleri Yönelimli Seçim teknikleriyle özellik seçimi yapılmış ve en iyi sınıflandırma sonuçları Rasgele Orman ve Ekstrem Gradyan Artırma algoritmalarından elde edilmiştir.

Bilim Kodu : 10396619
Anahtar Kelimeler : Anomali, Saldırı Tespiti, Makine Öğrenmesi, Bilgi Güvenliği
Sayfa Adedi : 74
Danışman : Doç. Dr. Hidayet TAKCI

INTRUSION DETECTION USING ANOMALY DETECTION APPROACH

(M. Sc. Thesis)

Burak EKİCİ

SİVAS UNIVERSITY OF SCIENCE AND TECHNOLOGY

INSTITUTE OF GRADUATE STUDIES

December 2022

ABSTRACT

Attacks on computer networks are increasing day by day and characteristics of them are changing continuously. Network attacks destroy information security by damaging computer network systems. This situation poses a great risk for individuals, companies, institutions and even governments. To prevent or minimize the damages of network attacks, Intrusion Detection Systems are used. The development of these systems, which are created according to attack characteristics, continues parallelly to increasing attack types. In this study, it is aimed to create an intrusion detection system based on machine learning principles with anomaly detection. Recursive Feature Elimination, Forward Feature Selection, Random Forest, Decision Tree, Naive Bayes, Logistic Regression and Extreme Gradient Boosting algorithms are used during the study and evaluations are made by Accuracy, Precision, Recall and F1 Score metrics. Also, Cross Validation and ROC Curve methods are used for the evaluation. CICIDS2017 data set is used to find the most effective model by comparing the results obtained from the mentioned algorithms. As the result of this study, it is determined that the Intrusion Detection System models, which are created by classifying the features obtained the methods of Forward Feature Selection and Recursive Feature Elimination with Random Forest and Extreme Gradient Boosting algorithms, are successful.

Science Code : 10396619
Key Words : Anomaly, Intrusion Detection, Machine Learning, Information Security
Page Number : 74
Supervisor : Assoc. Prof. Hidayet TAKCI

TEŞEKKÜR

Hazırladığım tez çalışmasında, konu seçiminden çalışma yöntemlerine kadar tüm aşamalarda değerli akademik tecrübeleriyle bana yol gösteren, destekleriyle motivasyonumun her zaman üst seviyede kalmasını sağlayan kıymetli Danışman Hocam Doç. Dr. Hidayet TAKCI'ya çalışmalarım sürecindeki yardımlarından dolayı çok teşekkür ederim.

Çalışma sürecinde bana sabırla destek olan eşim Hilal EKİCİ'ye, bu süreçte dünyaya gelerek bana şans getiren oğlum Ege EKİCİ'ye, hayatımın her anında yanım olan babam Hakkı EKİCİ, annem Fatma EKİCİ ve ablam Ebru EKİCİ KAÇAN'a teşekkür ederim

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

AUC	ROC Eğrisi altında kalan alan
CICIDS 2017	Canadian Institue of Cybersecurity Intrusion Detection System 2017
DT	Karar ağacı
IDE	Tümleşik geliştirme ortamı
LR	Lojistik regresyon
NB	Naive Bayes
RF	Rastgele orman
RFE	Özyinelemeli özellik seçimi
ROC	Alıcı çalışma karakteristiği
SPSS	Statistical Package for the Social Sciences
STS	Saldırı tespit sistemi
XGB	eXtreme gradient boosting

1. GİRİŞ

Günden güne gelişen teknoloji, insanların yaşam kalitesinin yükseltilmesi adına gündelik hayatın merkezinde yerini almıştır. İnsanların konforunun artırılması amacıyla gündelik hayatta ihtiyaç duyulan birçok hizmet internet üzerinden sağlanmaya başlamış ve hatta kullanılan araç gereçler de internet üzerinden kontrol edilmeye başlanmıştır. İnternet üzerinden alışveriş yapmak, sosyal medya araçları ile birçok kişiyle bağlantı kurmak, internet üzerinden gerçek zamanlı görüntülü görüşmeler ve toplantılar yapmak, yemek sipariş etmek ya da yemek yaparken eksik bir ürünü internet üzerinden sipariş vererek kısa süre içerisinde kapıda teslim almak artık çok kolay hale gelmiştir. Ayrıca uzaktan izlenebilen güvenlik kameraları, uzaktan kontrol edilebilen kombiler, uzaktan izlenebilen buzdolapları ve daha sayılamayacak kadar araç gerecin artık internet üzerinden birbiriyle bağlantılı hale gelmesi gündelik hayatta insanların daha az zahmetle daha kısa sürede birçok işi yürütebilmesini sağlamıştır.

Gündelik hayatı kolaylaştıran bu imkânlar, doğal olarak internetin daha fazla kullanıcı tarafından daha yoğun şekilde kullanılması durumunu da ortaya çıkarmıştır. İnternetin yaygınlaşmaya başladığı yıllarda her evde yalnızca bir veya iki internet kullanıcısı varken şu anda hemen hemen herkes, üstelik yalnızca bilgisayarlarından değil, cep telefonlarından, tabletlerinden, akıllı saatlerinden vb. cihazlardan ayrı ayrı birer internet kullanıcısı olarak bu büyük trafiğe katılmıştır. Bununla birlikte evlerde bulunan akıllı süpürgeler, buzdolapları, kombiler, kameralar vb. cihazlar da bu trafiğinin bir parçasını oluşturmaktadırlar.

Oluşan bu devasa boyutlardaki internet trafiği aynı ölçekte veriyi ve verilerin oluşturduğu bilgiyi de bünyesinde barındırmaktadır. Örneğin; internet üzerinden alışveriş yapan bir kişi bu işlem sırasında kullandığı kredi kartı bilgisi gibi hassas verileri internet trafiğine sunmaktadır. Bu örnekteki gibi sadece internet üzerinden alışveriş yapan kişi ile ticaret yapan firma ya da banka arasında gizli kalması gereken verilerin, küresel internet trafiği üzerinde korunması önem arz etmektedir. Sadece bireysel olarak değil daha büyük ölçekte şirketlerin, kurumların ve hatta devletlerin de hassas verilerinin yetkisiz kişilerin eline geçmesi ya da bozulmadan muhafaza edilmesi son derece hayati bir konudur. Bahsi geçen küresel internet trafiği üzerinde bulunan hassas veriler, kötü niyetli insanların iştahlarını

kabartmakta ve hassas verilerin yetkisiz insanların eline geçmesi riskini artırmaktadır. İşte bu noktada “Bilgi Güvenliği” kavramı öne çıkmaktadır.

Bilgi Güvenliğinin sağlanmasında çeşitli araçlar, yöntemler ve sistemler kullanılmaktadır. Farklı koşullara ve ihtiyaçlara göre seçilen bu sistemler günden güne gelişmektedir. Saldırı Tespit Sistemleri (STS) de Bilgi Güvenliğinin sağlanması amacıyla kullanılan ve günden güne geliştirilmeye de devam edilen önemli araçlardan biridir. STS’lerde temel amaç belirli bir bilgisayar ağına odaklanarak, ağda meydana gelen trafiğin incelenip yorumlanması ve şüpheli hareketlerin tanımlanarak bunun bir ağ saldırısı olup olmadığının tespit edilmesidir. Bilgisayar ağlarındaki bahsedilen bu şüpheli hareketler ve oluşan olağan dışı trafik anomali olarak adlandırılır. Anomali tespit yaklaşımındaki temel amaç da bu olağan dışı trafiğin tanımlanarak saldırının tespit edilmesidir.

Yapılan bu çalışmada ağ saldırılarının tespitinde başarı oranının artırılması ve yeni saldırı tiplerinin tespit edilmesi amacıyla Makine Öğrenmesi temeline dayalı bir STS oluşturma amaçlanmıştır. Konuyla ilgili olarak hazır bir veri seti üzerinde özellik seçimi ve sınıflandırma deneyleri yapılmış ve sonuçlar raporlanmıştır.

2. KAYNAK ARAŞTIRMASI

STS, bilgisayar ağlarına yapılan saldırı türlerine göre farklı niteliklere sahip olabilmeleri açısından sürekli değişim ve gelişim halindedir. Saldırı türleri değiştikçe, oluşturulacak olan STS de yeni saldırı türlerini tespit edebilmesi açısından farklı niteliklere gereksinim duyar. Bu nedenle geçmişten beri bu alanda yapılan birçok çalışma mevcut olmakla birlikte yeni çalışmalara ve farklı tekniklere duyulan ihtiyacın da devam etmesi kaçınılmazdır. Bu alanda geçmişte yapılan çalışmalar incelendiğinde;

Jabez ve Muthukumar (2015), yaptıkları çalışmada Aykırılık Tespiti adını verdikleri yeni bir yaklaşım önermektedir. Bu yaklaşıma göre anomali Komşuluğa Aykırı Faktör (Neighborhood Outlier Factor) metriği ile ölçülmektedir. KDD veri setinin kullanıldığı bu çalışmada önerilen yaklaşımın var olan saldırı tespit sistemlerine göre daha az yürütme zamanında çalıştığı ve daha çok anomaliyi tespit edebildiği ortaya konulmuştur.

Aljawarneh, Adlwairi ve Yassein (2017)'e göre etkin bir şekilde ağ saldırılarının tespitinin yapılabilmesi için verilerin son derece hassas bir şekilde toplanması gerekmektedir. Yazarlar, bu çalışmada saldırı kapsamının eşik değerini, ağ işlemlerindeki verilerin eğitim için kullanıma sunulan özelliklerinden en uygun olanlarına göre değerlendirmek için yeni bir hibrit model geliştirmişlerdir. Bu model J48, Rastgele Orman, Naive Bayes, DecisionStump ve AdaBoost sınıflayıcılarını bünyesinde barındırmaktadır. NSL-KDD veri setindeki en anlamlı özelliklerin ortaya çıkarılmasında Bilgi Kazanımı ve Oylama şemaları kullanılarak sonuçta ikili sınıflar için %99,81 ve çoklu sınıflar için ise %98,56'lık oranda saldırıları doğru tespit etme başarısı yakalanmıştır.

Yıldırım, Çavuşoğlu, Şen ve Budak (2014) ise yaptıkları çalışmada KDD Cup 99 veri seti üzerinde çok katmanlı yapay sinir ağı kullanarak bir STS modeli oluşturmuşlardır. Oluşturulan modelin eğitim başarısı %99, test başarısı ise %90,61 olarak ölçülmüştür.

Alamiedy, Anbar, Alqattan ve Alzubi (2019) yaptıkları çalışmada Çok Katmanlı Gri Kurt Optimizasyon Algoritmasını kullanarak NSL-KDD veri setindeki en anlamlı özellikleri seçmiş ve çeşitli sınıflayıcılarla bir STS modeli oluşturmuşlardır. Çalışma sonucunda veri

setindeki özelliklerin en anlamlılarını seçerek, özellik sayısının azaltılmasının başarı oranını artırdığını ortaya koymuşlardır.

Chen, Mei, Kong, Yuan ve Li (2017) ise yeni saldırı tiplerinin daha başarılı olarak tespit edilebilmesi için denetimsiz öğrenme tekniklerine dayalı bir STS yaklaşımını önermişlerdir. Çalışmanın kümeleme aşamasında DBSCAN, One-SVM, Agglomerative Clustering ve Expactation-Maximization modelleri kullanıldıktan sonra oylama modeli ile tutarlı sonuçlar elde etmişlerdir. Çalışma sonucunda False-Positive (FP) metriğine göre geleneksel yöntemlere oranla önerilen sistemin daha başarılı olduğu görülmüştür.

Kumar, Choudhary ve Sahrawat (2020), CICIDS 2017 veri seti üzerinde yaptıkları çalışmada Rastgele Orman algoritmasına göre özellik sayısını düşürerek elde ettikleri anlamlı özellikleri Karar Ağacı, Çok Katmanlı Yapay Sinir Ağları, Naive Bayes ve Topluluk Öğrenmesi algoritmaları ile sınıflandırmışlardır. Çalışma sonucunda elde ettikleri veriler karşılaştırıldığında en başarılı sonuçların Karar Ağacı sınıflandırmasıyla yapıldığı ortaya çıkmıştır.

Ran, Ji ve Tang (2019), Aegean Wi-Fi Intrusion Dataset (AWID) veri seti üzerinde hem denetimli öğrenme hem de denetimsiz öğrenme tekniklerini kullanarak iki aşamalı bir saldırı tespit sistemi önermişlerdir. Çalışmanın ilk aşamasında daha önce etiketlenmiş veriler denetimli öğrenme teknikleri ile ikinci aşamasında ise etiketsiz veriler denetimsiz öğrenme teknikleri ile değerlendirilmiştir. Çalışma sonucunda ortaya çıkan %98,54'lük genel başarı oranı bu karma modelin başarısını ortaya koymuştur.

Satam ve Hariri (2020) yaptıkları çalışmada kablosuz ağlarda saldırı tespiti yaparken anomali davranış analizi yaklaşımıyla yüksek doğruluk oranı elde edebileceklerini göstermişlerdir. İlgili çalışmada Arizona Üniversitesi kablosuz ağlarından alınan yerel veri setleri üzerinde n-gram yöntemini kullanarak yanlış tespit oranını 0,0174 gibi çok düşük bir orana indirmişlerdir.

Abdel-Aziz, Hassanien, Azar ve Hanafi (2013) yaptıkları çalışmada iletişim ağlarındaki anomalilerin tespitinde genetik algoritmaları ve Temel Bileşen Analizi (PCA) yöntemini kullanarak veri setlerindeki en anlamlı özelliklerin ortaya çıkarılması gerektiğini savunmuşlardır. Ortaya çıkarılan özelliklerin de çeşitli algoritmalar ile sınıflandırılmasını

sağladıktan sonra NSL-KDD veri seti üzerinde daha önceden bilinen saldırılarda en etkili sınıflayıcının Naive Bayes, tanımlanmamış saldırıların tespitinde en etkili sınıflayıcının ise J48 olduğunu ortaya koymuşlardır.

Jose, Malathi, Reddy ve Jasseeli (2018) yaptıkları çalışmada saldırı tespit sistemlerinde anomali tespit yaklaşımı ve bu yaklaşımın nasıl uygulanabileceği hususunda çeşitli bilgilere yer vermişlerdir. Mevcut tekniklerin incelendiği çalışmada, saldırı tespit sisteminin kullanım yeri ve sistemden beklentilere göre doğru tekniğin seçilmesinin önemi vurgulanmıştır. Saldırı tespit sistemlerinde anomali tespiti yaklaşımının en büyük avantajının yeni saldırı tiplerinin sisteme tanımlanmasına gerek olmadığı hususu üzerinde durulmuştur.

Karataş ve Şahingöz'ün çalışmasında (2018) ise yazarlar yapay sinir ağları tabanlı, çok katmanlı bir saldırı tespit sistemi oluşturarak KDD Cup 99 veri seti üzerinde "trainc, trainlm, trainbfg, trainscg, traincgp, trainoss, trainbr, trainr" eğitim fonksiyonlarının karşılaştırmasını yapmışlardır. Doğru-Pozitif (TP) metriğinin ölçek olarak kabul edildiği çalışmanın sonucuna göre en hızlı uygulama zamanı "trainscg" fonksiyonu ile en düşük hata oranı ise "trainlm" fonksiyonu ile elde edilmiştir.

Zhou, Cheng, Jiang ve Dai (2020) özellik seçimi ve topluluk öğrenmesine dayalı sınıflayıcıları temel alarak verimli bir saldırı tespit sistemi üzerinde yoğunlaşmışlardır. Çalışmanın özellik seçimi aşamasında Korelasyon Tabanlı Özellik Seçimi (CFS) ve Yarasa Algoritması (BA) beraber kullanılmıştır. CFS, sezgisel değerlendirmelerin sonuçlarına göre özelliklerin seçildiği klasik bir filtreleme algoritması olup, BA ise küçük yarasaların ekolojik konumlanma davranışlarından esinlenerek oluşturulan bir algoritmadır. Sınıflandırma aşamasında ise C4.5, Rastgele Orman ve Cezalandırılan Özellikler ile Karar Ağacı algoritmaları kullanılmıştır. CICIDS 2017 veri seti üzerinde yapılan çalışmada belirtilen algoritmalar ayrı ayrı ve daha sonrasında ise topluluk halinde kullanılarak sonuçlar değerlendirilmiştir. Böylece yapılan çalışmanın en iyi sonucunun topluluk öğrenme algoritmalarıyla sağlandığı ortaya konulmuştur.

Shaukat, Ali, Batool, Alqahtani, Khan ve Ahmad (2020) yaptıkları çalışmada, ağ güvenliği ve saldırı sınıflandırmasında kilit rol oynayan makine öğrenmesi tekniklerinden Naive Bayes ve J48 Karar Ağaçları algoritmalarını karşılaştırmışlardır. CICIDS 2017 veri seti

üzerinde gerçekleştirilen çalışmanın ilk aşamasında, veri setindeki tüm özellikler herhangi bir eleme işlemine tabi tutulmadan kullanılmış, ikinci aşamada ise Sarmalayıcı Özellik Seçimi tekniğine göre özellik seti 8 özelliğe düşürülerek kullanılmıştır.

Fernandez ve Xu (2019), hem denetimli ağ saldırı tespitinde hem de denetimsiz anomali tespitinde derin öğrenmenin kullanılmasıyla ilgili bir çalışma yapmışlardır. Yazarlar öncelikli olarak ileri beslemeli tam bağlı bir derin sinir ağı oluşturarak (DNN) denetimli öğrenme yolu ile ağ saldırı sistemini eğitmeyi daha sonra ise etiketlenmemiş zararlı ağ trafiği verilerini denetimsiz öğrenme yoluyla bir otomatik kodlayıcı ile sınıflandırmayı amaçlamışlardır. CICIDS 2017 veri setinin kullanıldığı çalışmada Derin Sinir Ağının (DNN) saldırı tespitinde diğer makine öğrenmesi tekniklerinden daha iyi performans sağladığı ortaya çıkarılmıştır.

Karataş, Demir ve Şahingöz (2018), yaptıkları çalışmada günden güne artan siber saldırıların sayılarının ve etkilerinin azaltılması hususunda önemli rol oynayan saldırı tespit sistemlerinde derin öğrenme yaklaşımlarının kullanılması ve bu sistemlerin temel yapısı hakkında araştırma yapmışlardır. Yazarlar, saldırı tespit sistemlerinin genel yapısının 3 temel bileşenden oluştuğunu belirtmişlerdir. Çalışmaya göre bunların ilkinin veri toplanması, ikincisinin verilerden özellik vektörü oluşturulması amacıyla vektörize edilmesi ve son olarak da özellik vektörlerine göre sınıflandırma mekanizması olduğu görülmektedir. Çalışmada ayrıca Derin Öğrenmenin, geliştirilmiş bir Makine Öğrenmesi tekniği olarak nitelendirildiği ve STS'lerde Derin Öğrenme ile Makine öğrenmesi arasındaki farklara değinildiği görülmektedir.

Yu, Dong, Chen, Li, Xu, Li, Qiao, Liu, Zhao ve Zhang (2020), mevcutta saldırı tespiti konusunda yapılan çalışmaların çoğunun ağ uzmanlarının bilgi ve tecrübelerine dayalı manuel yöntemlerle tasarlanmış ağırlıklı istatistiksel modellere dayalı olduğunu, bunların da sorunu tam anlamıyla çözemediğini savunmuşlardır. Yazarlar önerdikleri sistemde PBCNN adını verdikleri Paket Byte Tabanlı Evrişimli Sinir Ağı (Packet-Byte Based CNN) yönteminde, ilk aşamada ham pcap dosyalarındaki bir paketteki baytlardan otomatik olarak soyut özellikler çıkarmayı, ikinci aşamada da csv dosyalarındaki hazır özellikler yerine bir akış ve oturumdan çıkarılan paketlerin yeni bir formatta sunumunu oluşturarak orijinal verilerin tam olarak kullanılmasını sağlamışlardır. Son aşamada da yine

Evrişimsel Sinir Ağı ile sınıflandırma yaparak mevcut çalışmalara oranla çok daha başarılı bir modeli ortaya koymayı başarmışlardır.

Kurniabudi, Stiawan, Darmawijoyo, Bin Idris, Bamhdi ve Budiarto (2020), yaptıkları çalışmada veri analizinde özellik seçme işleminin önemini vurgulayarak, saldırı tespit sistemi çalışmalarında özellik seçimi için kullanılan Bilgi Kazanımı (Information Gain) tekniğini derinlemesine incelemişlerdir. Yazarlar öncelikle veri setinde bulunan bazı etiketleri birleştirmiş daha sonrasında ise IG tekniğini CICIDS 2017 veri setine uygulayarak elde ettikleri veriler doğrultusunda özellik seçimi yapmış ve seçilen bu özellikleri de Rastgele Orman, Naive Bayes, Bayes Net ve Rastgele Ağaç algoritmalarıyla sınıflandırmaya tabi tutmuşlardır. Çalışmada elde edilen veriler özellik seçiminde kullanılan Bilgi Kazanımı algoritmasının, sistemin çalışma zamanını ve başarı oranını olumlu yönde etkilediğini göstermiştir.

Li, Yi, Wei, Jiang ve Tian (2021), saldırı tespit sistemlerinde özellik seçimi aşamasının, sistemin performansı açısından kilit rol oynadığını vurgulamışlardır. Yazarlar, yüksek boyutlu veri setlerinin neden olduğu düşük verim ve yüksek FP oranı sorunlarının, özellik seçim aşamasında kullanılacak Linear Nearest Neighbor Lasso Step tekniğine dayalı Kril Herd (LNNLS-KH) algoritmalarıyla aşılabilmesi üzerine çalışmışlardır. Kril Herd algoritması aslında veri madenciliğinde kullanılan verimli bir sürü zekâsı algoritmasıdır. Yazarlar yaptıkları çalışmada bu algoritmayı geliştirerek saldırı tespit sistemlerinin özellik seçim aşamasında sözkonusu algoritmayı kullanmışlardır. CICIDS 2017 veri setindeki bazı sınıf etiketlerini birleştirerek etiketleri “Normal, DoS, DDoS, PortScan ve Web Attack” olarak azaltan yazarlar, daha sonra farklı algoritmalarla özellik seçimi yaparak bu özellikleri sınıflandırmaya tabi tutmuş ve önerdikleri LNNLS-KH algoritmasıyla seçilen özellikle yapılan sınıflandırmaların ortalama olarak doğruluğu %10 artırarak çalışma süresini de %5 düşürdüklerini belirtmişlerdir.

Reis, Maia ve Praça (2020), yaptıkları çalışmada CICIDS 2017 veri seti üzerinde Gini Önemi, Permutasyon Önemi ve Alt Sütün Önemi tekniklerini kullanarak özellik seçim işlemi yaparak veri setindeki özellikleri derecelendirmişlerdir. Bu teknikle özellik seçimi işleminden sonra Rastgele Orman ve Karar Ağaçları algoritmalarıyla da sınıflandırmalar yaparak modelin doğruluğu ve çalışma zamanı gibi metriklerde değerlendirmeler yapmışlardır. Çalışma sonucunda elde edilen verilere göre doğruluk ve çalışma zamanları

da düşünüldüğünde veri setindeki en anlamlı 5 özelliğin Destination Port, Flow IAT Min, Fwd IAT Min, Init Win Bytes Forward, Init Win Bytes Backward olduğu belirtilmiştir.

Gosu, Priyadarsini ve Motupalli (2021), yaptıkları çalışmada anomali tespitinde etkili ve verimli bir sistem geliştirilmesi için seçilmesi gereken öznitelikler konusunda detaylı bir analiz yapmışlardır. Yazarlar , öznitelik seçimi için Bilgi Kazanımı (BA) ve Yarasa Algoritması (BA) 'ndan oluşan hibrit bir yaklaşım kullanmışlar ve farklı parametreler kullanarak farklı öznitelik grupları oluşturmuşlardır. Elde ettikleri öznitelik gruplarını da Rastgele Orman, Naive Bayes, Bayes Network, J48 ve Rastgele Ağaç algoritmalarıyla sınıflandırmışlardır. CICIDS 2017 veri seti üzerinde yapılan çalışma sonucunda genel itibariyle Rastgele Orman algoritması ile yapılan sınıflandırmalar diğer sınıflayıcılara göre daha başarılı olduğu ortaya konmuştur.

3. MATERYAL VE YÖNTEM

3.1. Bilgi Güvenliği

Günümüzün rekabetçi atmosferinde teknolojik açıdan başarılı olabilmenin birinci yolu yeterli bilgiye sahip olmaktır. Teknolojinin temelini oluşturan böylesine önemli bir varlığın korunabilmesi için de ayrı bir disipline ihtiyaç vardır.

Her ne kadar bilginin önemi günümüzde ön plana çıkmış gibi görünse de aslında tarihin en eski dönemlerinden itibaren bilginin korunması için çeşitli yöntemler kullanılmıştır. Çok eski dönemlerde kil tabletler ve taş kitabeler üzerindeki bilgi, zaman geçtikçe hayvan derisi, parşömen, kâğıt, delikli kart, kaset ve manyetik cihazlar üzerinde saklanmaya başlanmıştır. Önceleri bu materyaller üzerinde bilginin güvenliği için sadece duvar örülmesi, nöbetçi bulundurulması vb. fiziksel tedbirler alınmışsa da günden güne gelişen teknoloji nedeniyle bilginin dijital ortamda çok daha pratik şekilde depolanması ve taşınabilmesi bahsedilen fiziksel tedbirlerin artık yetersiz kalmasına ve yeni tedbirlerin alınmasına neden olmuştur.

Literatür incelendiğinde bilgi güvenliği tanımı farklı kaynaklarda sık sık yapılmışsa da içerik itibariyle söz konusu tanımlar birbirine benzerdir. Canbek ve Sağıroğlu (2016), bilgi güvenliğini, “Bir varlık olarak bilginin hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesinin önlenmesi” olarak tanımlar. Pfleeger (1997), ise bilgi güvenliğini “Bilginin içeriğindeki bütünlüğün bozulmadan, herhangi bir değişime uğramadan ve gizliliği korunarak gönderici ve alıcı arasında iletiminin gerçekleştirilmesi ve bilgiye erişimde kesinti olmadan sürekliliğinin sağlanması” olarak ifade eder. Bilgi güvenliği tanımı bu ifadelerden yararlanarak daha genel bir anlamda “verilerin saklanması ve taşınması esnasında bütünlüklerinin bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümü” olarak açıklanabilir.

Günümüzde bilgi güvenliğinin sağlanması hususunda kurumlar, kuruluşlar ve hatta devletler ayrı güvenlik politikaları oluşturmakta bu politikalar doğrultusunda bilgi güvenliği faaliyetlerini sürdürmektedir.

3.1.1. Bilgi güvenliğini oluşturan ilkeler

Bilgi güvenliğinin çatısını oluşturan ve tüm dünyada benimsenen 3 temel ilke vardır. Bu ilkeler; bilginin gizliliği, bütünlüğü ve erişilebilirliğidir. Bu 3 temel ilkeye ilave olarak kayıt tutma, güvenilirlik, kimlik tespiti ve inkâr edememe gibi unsurlara da bilgi güvenliği ilkeleri olarak literatürde rastlanabilmektedir.

Gizlilik: Bilginin izinsiz bir şekilde erişilememesi ve yetkisiz kişilerin bilgiye erişiminin engellenmesi olarak ifade edilebilir. Bu ilke ile saklanan verilerin sadece izin verilen kişilerce elde edilebilmesi sağlanır. Bu ilkeyi sadece depolanan bilginin saklandığı ortamın korunması olarak düşünmek hata olur. Bilginin bir yerden başka yere taşınırken de izinsiz bir biçimde yetkisiz kişilerin eline geçmesinin de önlenmesi gereklidir. Bu nedenle genellikle Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları kullanılmaktadır.

Bütünlük: Bütünlük ilkesi, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standartlarına göre "bilginin doğruluğunun ve tamlığının sağlanması" olarak tanımlanır. Bu ilkeye göre bilginin tam olarak doğru olduğunun, bilginin içeriğinde herhangi bir değişme, bir bölümünde silinme veya fazladan bir kısım eklenme gibi durumların olmaması gerektiği ifade edilir. Bütünlük ilkesinin sağlanabilmesi adına genellikle özetleme (hashing) algoritmaları kullanılmaktadır (Baykız, 2020).

Erişebilirlik: Erişebilirlik ilkesi, bilgiyi talep eden ve aynı zamanda o bilginin elde edilmesi hususunda yetkili olan kullanıcıların bilgiye ve ilişkili varlıklara zamanında ve kesintisiz olarak ulaşabilmelerini ifade eder. Bir başka deyişle yetkili olan kullanıcıların taleplerine zamanında ve kesintisiz cevap verilmesidir. Kötü niyetli insanların bilgi sistemlerine yönelik saldırıları sıklıkla bilgiye erişimi ortadan kaldırmaktır. Bununla birlikte yangın, sel, deprem vb. doğal afetler nedeniyle de bilgiye erişim kısıtlanabilmektedir.

3.1.2. Siber güvenlik kavramı

Siber güvenlik kavramı son yıllarda genellikle Bilgi güvenliği kavramı yerine kullanılsa da bu iki kavram arasında bazı temel farklılıklar bulunmaktadır. Sağıroğlu ve Alkan (2018), Siber güvenlik kavramını "sanal ortamlarda karşılaşılabilecek tehdit ve tehlikelere maruz

kalmamak için saldırganlığı önleme, engelleme ve önlem alma" olarak ifade eder. Bu tanımlayıcı ifadeden de anlaşılacağı gibi Siber güvenlik kavramı aslında dijital ortamlarda bulunan bilginin güvenliğini kasteder. Bilgi güvenliği kavramı ise daha kapsamlı olarak hem fiziksel hem de dijital ortamlardaki bilginin güvenliğini ile ilgilidir. Örneğin, ofiste masamızın üzerinde duran bir evrakın izinsiz olarak yetkisiz kişilerin eline geçmemesi için alacağımız tedbirler yalnızca Bilgi güvenliği kavramının konusuyken, bilgisayar ortamında bulunan bir dosyamızın yine izinsiz olarak yetkisiz kişilerce ele geçirilmesini engellemek için alacağımız önlemler hem Bilgi güvenliğinin hem de Siber güvenliğin konusudur. Bu anlamda Siber güvenlik kavramının Bilgi güvenliğinin bir alt dalı olarak ifade edilmesi yanlış olmaz.

3.1.3. Ülkemizde siber güvenlik

Siber güvenlik kavramının önemi her geçen gün artmaya devam etmektedir. Dijital ortamlarda depolanan ve iletilen hassas verilerin her geçen gün artması ve buna paralel olarak artan dijital dolandırıcılık olayları ile terör faaliyetlerinin dijital dünyaya sıçraması ile kişilerin, şirketlerin, kurumların ve devletin artık dijital ortamda bilgi güvenliğinin yani siber güvenliğin sağlanmasında kendi politikalarını üretmesini zorunlu hale getirmiştir. Bu nedenle 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı dâhilinde hem ulusal hem de uluslararası koordinasyonun sağlanması için Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Bu merkez internet genelinde yer alan aktörler ile kolluk kuvvetleri, uluslararası kuruluşlar, özel sektör ve araştırma merkezleri arasındaki iletişimi yönetmektedir (Sağıroğlu & Alkan, 2018).

USOM ile birlikte yaklaşık sayıları 2000'i bulan ve bir siber tehdit veya saldırı unsuru tespit ettiğinde USOM'a bildirecek olan Siber Olaylara Müdahale Ekipleri (SOME) çeşitli kurum ve kuruluşlarda oluşturulmuştur. Bu ekipler aynı zamanda USOM'dan gelen uyarı ve bildirimlerin yerine getirilmesi için gerçekleştirilmesi istenen görevleri yapabilecek uzmanları bünyesinde barındırmaktadır. Ulusal Siber Güvenlik Stratejisi ve Eylem Planına göre SOME'ler, kurumlarına doğrudan veya dolaylı yollardan yapılan veya yapılması olası görünen siber saldırılara karşı ihtiyaç duyulan tedbirleri alma veya aldırma ve bu tip olaylara müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma ve kurumların bilgi güvenliğini sağlamaya yönelik çalışmaları yaptırmakla görevlendirilmişlerdir.

3.1.4. Siber saldırı türleri

Siber Saldırı en basit ifadeyle dijital ortamların herhangi bir şekilde zafiyete uğratılması amacıyla yapılan eylemlerdir. Bilgisayar korsanları siber saldırıları zarar vermek veya kazanç sağlamak amacıyla tekil veya gruplar halinde düzenlerler. Saldırıların hedefi tekil kullanıcılar olabildiği gibi, şirketler, kuruluşlar ve devlet kurumları da olabilir. Bilgisayarlar, internet siteleri, bilgisayar ağları ve internet üzerindeki her aktör bu saldırılara maruz kalma riskini taşımaktadır.

Siber saldırılar, Bilgi güvenliği ilkelerinin bir ya da birkaçının tahrip edilmesi yoluyla gerçekleştirilirler. Kimi saldırılarda gizli bilgilerin çalınmasını, kimi saldırılarda mevcut bilgilerin değiştirilmesi yoluyla manipülasyonlar yapılmasını, kimi saldırılarda ise hedef sistemlerin erişime kapatılmasını amaçlarlar.

Teknolojinin gelişmesine bağlı ortaya çıkan yeni internet aktörleri, uygulamalar ve sistemler beraberinde yeni saldırı tiplerinin oluşmasına da neden olmuştur. Kötü amaçlı yazılımlar, casus programlar, solucanlar, yığın e-postalar, oltalama saldırıları, sosyal mühendislik saldırıları, hizmet engelleme saldırıları, yapay zekâ araçlarıyla yapılan saldırılar vb. saldırı türleri dijital dünyada kullanıcılar için risk oluşturmaktadır.

Literatür incelendiğinde saldırı türlerinin farklı parametrelere göre sınıflandırılabildiği görülmektedir. Örneğin saldırının taşıdığı risk durumuna göre; kritik riskli, yüksek riskli, orta riskli ve düşük riskli saldırılar olarak sınıflandırılabildiği gibi saldırının yapıldığı ortama göre iç ağdan veya dış ağdan yapılan saldırılar olarak da sınıflandırılabilir. Saldırının hedeflediği işletim sistemlerine göre Windows, Unix, Linux, Ios ve Android saldırıları olarak da sınıflandırılabilir. Benzer şekilde saldırının vereceği etki bakımından ileri düzey kalıcı saldırı veya geçici saldırı olarak da ayrıştırılabilir. Bunun gibi parametre olarak saldırganların, hedef cihazların, verilen zararın, saldırı amacının, altyapının, yazılımların, sistemlerin, faydalanılan araç ve teknolojilerin türlerine göre saldırılar sınıflandırılabilmektedir. Ancak Bilgi güvenliği ilkelerinden yola çıkılarak temelde saldırılar aşağıdaki gibi sınıflandırılabilir;

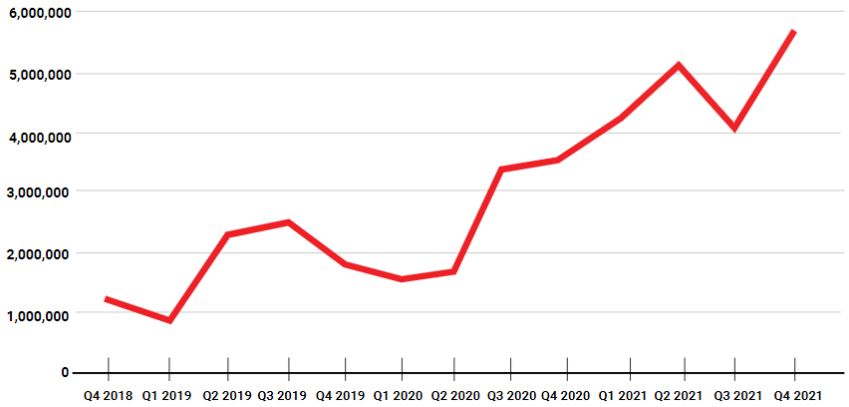
- Hedeflere izinsiz ve yetkisiz erişim,
- Hedefteki verilere zarar verme,
- Hedef veriler üzerinde manipülasyon yapma,

- Kötü amaçlı veri üretimi

3.2. Saldırı Tespit Sistemleri

Günden güne gelişen bilgi teknolojileriyle beraber dijital dünyadaki uygulamaların kullanım oranlarının gün geçtikçe artması, dijital ortamlarda muhafaza edilen bilgilerin güvenliğinin sağlanmasını temel gereksinim haline getirmiştir. Muhafaza edilecek bilginin değerine göre değişiklik gösteren sistemlerin amacı bilginin gereken gizliliğinin korunması ve bu bilginin yasa dışı ve yetkisiz şekilde saldırganların eline geçmesini engelleyebilmek adına gerekli önlemleri almaktır. Dijital dünyada uygulamalar arttıkça, sistemlerin birbirine entegrasyonu hızlandıkça sistemlerdeki güvenlik açıkları da çoğalacak ve bu açıklar sistemlerin güvenlik zafiyetlerini oluşturacaktır. Bilgisayar sistemlerine ait güvenlik zafiyetlerinin hiçbir zaman bitmeyeceği bir dünyada doğal olarak saldırıların tespit edilmesi de bilgi güvenliğinin sağlanmasında önemli bir etken olacaktır (Sağıroğlu, Yolaçan & Yavanoğlu, 2011).

İnternetin yaygınlaşmaya başladığı yıllarda daha çok hobi olarak ortaya çıkan siber saldırı eylemleri, sonraki yıllarda saldırının kapsamı ve verdiği zararlar açısından çok daha hacimli olacak şekilde şirketler, kurumlar ve hatta devletler için çok ciddi birer saldırı aracına dönüşmüşlerdir. Bu durumun oluşmasında hiç şüphesiz internetteki kullanıcı sayısının artması ve internet tabanlı uygulamaların sayısının artması etkili olmaktadır. Bu artışın da yıllara göre sürekli hale gelmesi siber saldırıların her geçen gün daha da artacağını ve saldırı tespit sistemlerinin de bu paralelde önem kazanacağını ortaya koymaktadır. Şekil 3.1'de küresel ölçekli ağ güvenlik teknolojileri ile ilgilenen Watch Guard firmasının Saldırı Önleme Sistemlerinin 2021 yılının 4. Çeyreğine ait raporundaki önlenen siber saldırı sayılarına ilişkin grafiği görülmektedir (WatchGuard, 2021).



Quarter/ Year	IPS Hits
Q4, 2018	1,244,146
Q1, 2019	989,750
Q2, 2019	2,265,425
Q3, 2019	2,398,986
Q4, 2019	1,878,730
Q1, 2020	1,660,904
Q2, 2020	1,752,789
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506
Q3, 2021	4,095,320
Q4 2021	5,686,245

Şekil 3.1. WatchGuard 2021 Yılı 4. Çeyreği İnternet Güvenlik Raporu

3.2.1. Saldırı tespit sistemi kavramı

STS kavramı iz tabanlı saldırı denetimi konseptiyle ilk defa 1980 yılında bilgi güvenliğinde öncü olarak kabul edilen James P. Anderson tarafından ortaya konulmuştur (Spafford, 2008).

Bace ve Mell (2011)'e göre STS, bir ağda veya bilgisayar sisteminde oluşan tüm olayları denetleyen, tespit edilen güvenlik sorunlarını ilgili personele ya da birime rapor ederek oluşabilecek riskleri azaltmak için ihtiyaç duyulan tedbirleri almakla görevleri sistemler olarak ifade edilmiştir.

Saldırı Tespit ve Önleme Raporu'nda ise saldırı tespiti, bir bilgisayar sistemi veya bilgisayar ağında meydana gelen olayların izlenerek bilgisayar güvenlik ilkelerinin, kabul edilebilir kullanım politikalarının veya standart güvenlik uygulamalarının ihlallerine ilişkin muhtemel işaretlerin ve yakın tehditlerin analizlerinin gerçekleştirilmesi ile oluşan vakaların tespit edilmesi olarak ifade edilir (Scarfone & Mell, 2007).

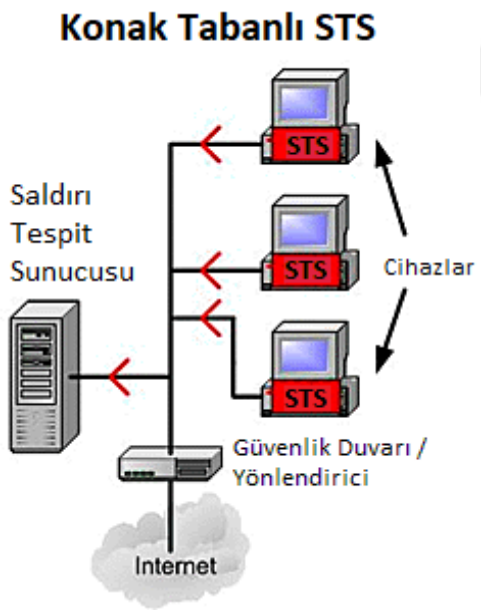
Bu bilgiler ışığında saldırı tespit sistemleri, bir bilgisayarda veya ağda meydana gelen olayları izleyip otomatik olarak analiz ederek olayların saldırı olup olmamasını tanımlayan ve bu tanıma göre alarm üreten yazılımsal veya donanımsal sistemler olarak tanımlanabilir. Tekil bilgisayarlar üzerinde çalışan anti-virüs yazılımlarından, bütün bir omurga ağını dinleyen donanım ve yazılım bileşenlerinin oluşturduğu ileri seviye sistemlere kadar geniş bir yelpazeyi içerir.

STS'ler temel olarak konum bazlı ve analiz bazlı olmak üzere 2 ana grupta incelenebilir.

3.2.2. Konumlarına göre saldırı tespit sistemleri

Konum bazlı sınıflandırmada, sistemin kurulu olduğu yer esas alınır. Buna göre konum bazlı STS'ler, konak (host) tabanlı ve ağ tabanlı olmak üzere iki grupta incelenebilir.

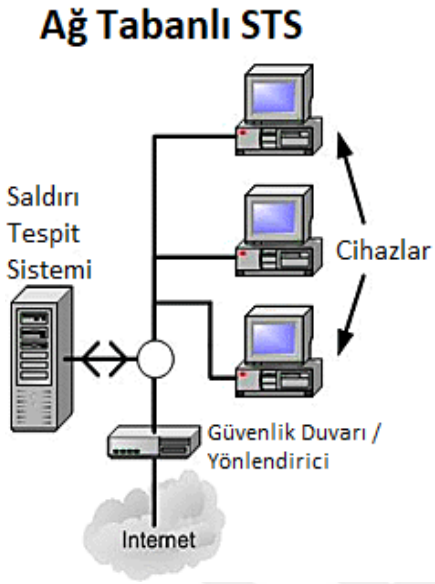
Konak tabanlı saldırı tespit sistemleri: Belirli bir tekil sistemdeki veya cihazdaki hareketlilik hakkında bilgi toplamayı amaçlayan saldırı tespit sistemleridir. Muhtemel saldırıların olacağı cihazlara ya da tekil sistemlere kurulurlar. Kurulu oldukları tekil bir bilgisayar ya da bilgisayar sistemi içerisinde bulunan verileri analiz ederek saldırı tespiti yapmayı amaçlarlar. Şekil 3.2'de Konak Tabanlı STS'lere ilişkin bir model gösterilmektedir.



Şekil 3.2. Konak Tabanlı STS Modeli (InformIt, 2002)

Ağ tabanlı saldırı tespit sistemleri: Ağdaki tüm aygıtlardan gelen trafiği izleyip analiz ederek ağ tabanlı tehditleri tespit eden sistemlerdir. Tek tek cihazları izlemek yerine tüm ağı izlerler. Bu ağ küçük ölçekli bir ev ağı ya da daha büyük ölçekli kurum ve kuruluş ağları olabilir. Ağ tabanlı STS'ler, kurulu oldukları ağı izleyerek lokal ağdan veya internetten gelen, ağdaki sistemlere zarar verme potansiyeli olan verileri analiz edip olası

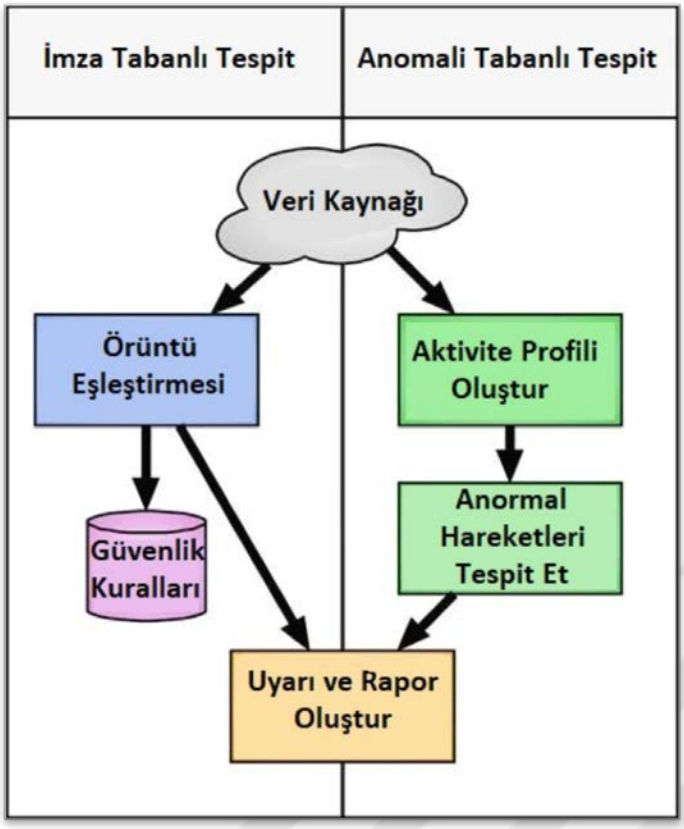
bir saldırı durumunu fark edebilme kabiliyetine sahip olacak şekilde tasarlanmış sistemlerdir. Şekil 3.3'te Ağ Tabanlı STS modeli görülmektedir.



Şekil 3.3. Ağ Tabanlı STS Modeli (InformIt, 2002)

3.2.3. Analiz yöntemlerine göre saldırı tespit sistemleri

Analiz yöntemlerine göre sınıflandırmada temel prensip STS'lerin bulunduğu sistem içerisinde meydana gelen olayları nasıl analiz ettikleri ve saldırıları hangi temel dayanaklara göre algıladıklarıdır. Bu şekilde analiz yöntemlerine göre sınıflandırılan STS'ler Kötüye Kullanım Tespiti Tabanlı STS'ler ve Anomali Tabanlı Saldırı Tespit Sistemleri olarak iki grupta incelenebilir. Şekil 3.4'te analiz yöntemlerine göre olan saldırı tespit süreçleri gösterilmektedir.



Şekil 3.4. Analiz Yöntemlerine Göre STS Süreçleri

Kötüye kullanım tespiti tabanlı saldırı tespit sistemleri: Bu gruptaki STS'lere İmza Tabanlı Sistemler de denilmektedir. Kötüye kullanım tespiti ya da imza tabanlı tespitler, bilinen bir tehdit hakkında benzersiz bir tanımlama oluşturulması ve gelecekteki tehditlerin bu tanımlamaya göre tespit edilebileceği bir süreçtir. Bu konseptte imza kavramı, kötü amaçlı girişimlerin modellenmesini, bıraktığı izi yani örüntüsünü ifade eder. Her saldırıda, saldırıya ilişkin imzalar oluşturulur ve veri tabanında saklanır. Daha sonra sistemde meydana gelen şüpheli olaylar veri tabanına taranarak önceki imzalarla karşılaştırılır ve eşleşme bulunursa şüpheli olay saldırı olarak sınıflandırılır.

Kötüye kullanım tespitinde temel mantık sistemdeki anormal davranışların üzerinden tespit yapmaktır. Bu yaklaşımda daha önce tespit edilememiş bir saldırı türüyle karşılaşıldığında, elde mevcut bir örüntü bulunmadığından bunun bir saldırı olarak tespit edilmesi mümkün olmayacaktır. Yani sıfırıncı gün saldırılarında imza tabanlı yöntem etkisizdir. Bu nedenle böyle sistemlerde imza veya örüntü veri tabanının sık güncellenmesi gerekmektedir. Yeni saldırı türlerinin veri tabanına eklenerek sistemin güncellenmesi de bir sistem yöneticisi vb. dış etkenle yapılacağından dolayı böyle sistemlerin tamamen otonom olmasından söz

edilemez. Klasik yaklaşımdaki antivirüs yazılımları bu gruptaki saldırı tespit sistemlerinin en yaygın örneği olarak gösterilmektedir.

Anomali tespiti tabanlı saldırı tespit sistemleri: İstatistiksel teknikler ve makine öğrenmesi yardımıyla sistemdeki kullanıcılarının normal davranışını öğrenen ve daha sonra yapılan girişimleri normal veya anormal şeklinde sınıflandıran sistemlerdir. Bu gruptaki sistemlerde temel prensip güvenilir bir öğrenme modeli oluşturarak daha sonra oluşan olayların bu modelle karşılaştırılmasıdır. Kötüye kullanım tespiti tabanlı sistemlere göre en büyük farkı da anomali tabanlı sistemlerde izlenen normal aktivitelerin öğrenilmesi üzerinden saldırı tespiti yapılırken, kötüye kullanım tespiti tabanlı sistemlerde anormal aktiviteler üzerinden bu işlemin gerçekleştirilmesidir.

Bu tip saldırı tespit sistemlerinde, sistemin normal aktiviteleri öğrenildiği için anormal aktivitelere genellikle bir saldırı türü eşlik eder. Yeni saldırı tiplerinin tespit edilmesinde kötüye kullanım tabanlı sistemlere göre çok daha başarılıdır. Ancak bu durum beraberinde bir dezavantajı da getirir. Sistemin öğrenme aşamasında olmayan ancak daha sonradan oluşan normal bir aktivite, STS tarafından saldırı olarak algılanıp yanlış alarmlar üretilebilir. STS'nin bir karar destek sistemi olduğu düşünüldüğünde, bu alarmların ilgili sistem yöneticisi veya birimi tarafından gerçekten bir saldırıya ait olması durumunun da yorumlanması gerekebilir.

3.2.4. Saldırı tespit sistemleri (STS) ile saldırı önleme sistemleri (SÖS) arasındaki farklar

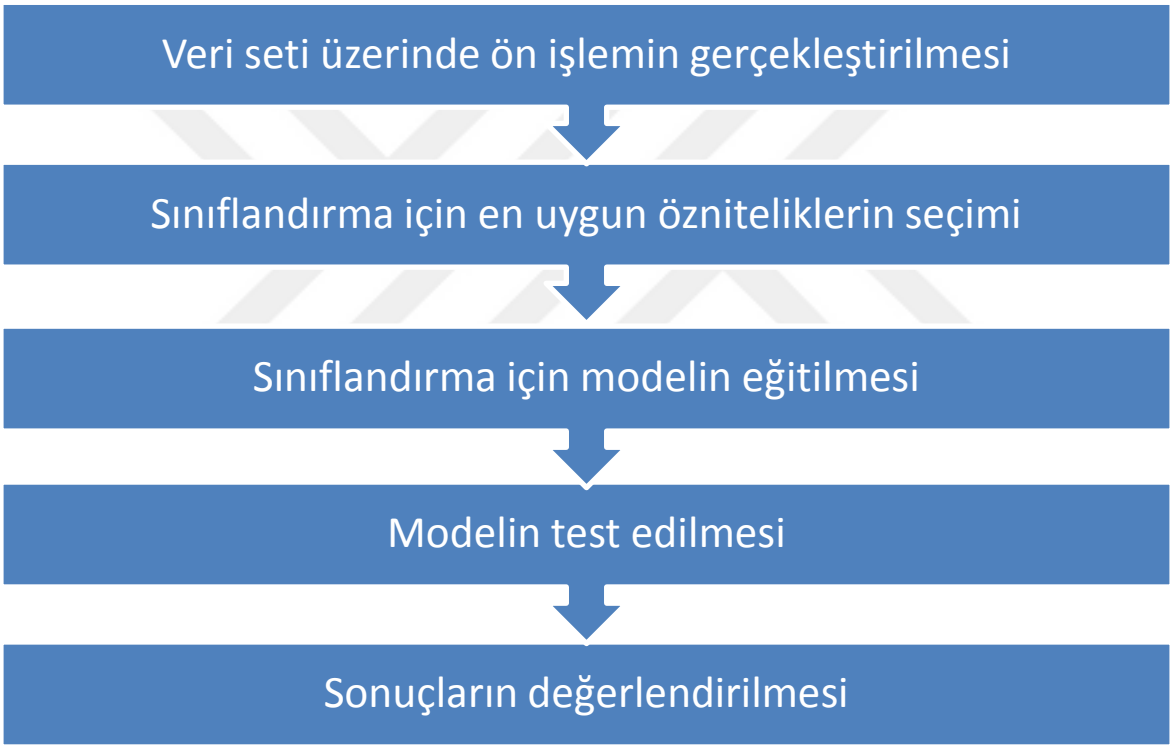
STS, özünde bir karar destek sistemidir. Yani üzerinde kurulu olduğu sistemde bir saldırı durumunun olup olmadığıyla ilgili sistemin yöneticisine bilgi verir. Sisteme yapılan bir saldırı durumunda, STS'nin görevi o olayın doğru şekilde tespit edilmesiyle yani saldırı alarmının üretilmesiyle sona erer. STS'nin oluşturduğu sonuca bakılması için bir insana veya farklı bir sisteme ihtiyaç duyulur.

SÖS ise bir kontrol sistemidir. Saldırının önlenmesini veya en az hasarla bertaraf edilmesini amaçlar. Saldırı olduğu anda herhangi bir insan veya farklı bir sistemin tetiklemesine ihtiyaç duymadan otomatik olarak devreye girer ve görevini yapmaya çalışır.

Bu açılardan STS ile SÖS farklılık gösterse de aslında bu iki sistem birbirini tamamlayan en önemli bilgi güvenliği araçlarındandır.

3.3. Çalışmanın Temel Aşamaları

Yapılan bu çalışmada etkin ve verimli bir saldırı tespit sistemi oluşturmak için, temel olarak ağ trafiğindeki olağan dışı durumların makine öğrenimi tekniklerinden faydalanarak tespit edilmesi, başka bir deyişle anomali tespiti yöntemi benimsenmiştir. Çalışmanın temel aşamaları ise Şekil 3.5'te görülmektedir.



Şekil 3.5. Çalışmanın Temel Aşamaları

3.4. Veri Seti

Çalışmada, Kanada Siber Güvenlik Enstitüsü tarafından oluşturulan ve güncel saldırı senaryolarını bünyesinde barındıran Canadian Institue of Cybersecurity Intrusion Detection System 2017 (CICIDS2017) isimli veri seti kullanılmıştır. CICIDS2017 boyutu ve içeriği ile ağ saldırılarının önlenmesi hususunda oluşturulacak olan yeni modellerin ve algoritmaların analizi açısından önemli bir veri setidir. Veri seti, toplamda 8 ayrı dosyadan oluşmakta ve Kanada Siber Güvenlik Enstitüsünün 5 günlük normal ve saldırı

durumundaki ağ trafiğinin kayıtlarını içermektedir. Çizelge 3.1'de veri setini oluşturan dosyalar hakkında kısa bilgiler gösterilmektedir.

Çizelge 3.1. Veri Setinde Bulunan Dosyalar (Paningrahi & Borah, 2018)

Dosya Adı	Günlük Aktivite	Oluşan Aktivite
Monday-WorkingHours.pcap_ISCX.csv	Pazartesi	Normal ağ trafiği
Tuesday-WorkingHours.pcap_ISCX.csv	Salı	Normal ağ trafiği ve FTP-Patator, SSH-Patator saldırıları
Wednesday-workingHours.pcap_ISCX.csv	Çarşamba	Normal ağ trafiği ve DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed saldırıları
Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv	Perşembe	Normal ağ trafiği ve Web Attack – Brute Force, Web Attack – Sql Injection, Web Attack – XSS saldırıları
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv	Perşembe	Normal ağ trafiği ve Infiltration saldırısı
Friday-WorkingHours-Morning.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve Bot saldırısı
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve PortScan saldırısı
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv	Cuma	Normal ağ trafiği ve DDoS saldırısı

Çizelge 3.1'de gösterilen bu dosyalar birleştirildiğinde 3119345 örnek, 1 tanesi normal ağ trafiğini gösterir şekilde toplam 15 adet sınıf etiketi ve 83 farklı özniteliği bünyesinde barındıran geniş bir veri seti ortaya çıkmaktadır (Paningrahi & Borah, 2018). Etiketlenmiş 15 adet sınıfa ait veri setinde örneği bulunan kayıtların dağılımı da Çizelge 3.2'de görülmektedir.

Çizelge 3.2. Veri Setindeki Örnek Dağılımları (Paningrahi & Borah, 2018)

Sınıf Etiketleri	Veri Setinde Örnek Sayıları
BENIGN	2359087
DoS Hulk	231072
PortScan	158930
DDoS	41835
DoS GoldenEye	10293
FTP-Patator	7938
SSH-Patator	5897
DoS slowloris	5796
DoS Slowhttptest	5499
Bot	1966
Web Attack – Brute Force	1507
Web Attack – XSS	652
Infiltration	36
Web Attack – Sql Injection	21
Heartbleed	11

Çizelge 3.3'te ise veri setinde bulunan tüm öznitelikler ve bu özniteliklere ilişkin kısa açıklamalara yer verilmektedir.

Çizelge 3.3. Veri setinde Bulunan Öznitelikler (Kültür, 2022)

Öznitelik Adı	Açıklaması
Destination Port	Hedef port
Flow Duration	Akış süresi (Mikro-saniye)
Total Fwd Packets	İleri yönde toplam paket sayısı
Total Backward Packets	Geri yönde toplam paket sayısı
Total Length of Fwd Packets	İleri yöndeki paketlerin toplam uzunluğu
Total Length of Bwd Packets	Geri yöndeki paketlerin toplam uzunluğu
Fwd Packet Length Max	İleri yönde paketlerin maksimum uzunluğu
Fwd Packet Length Min	İleri yönde paketlerin minimum uzunluğu
Fwd Packet Length Mean	İleri yönde paketlerin ortalama uzunluğu
Fwd Packet Length Std	İleri yönde paket uzunluklarının standart sapması
Bwd Packet Length Max	Geri yönde paketlerin maksimum uzunluğu
Bwd Packet Length Min	Geri yönde paketlerin minimum uzunluğu
Bwd Packet Length Mean	Geri yönde paketlerin ortalama uzunluğu
Bwd Packet Length Std	Geri yönde paket uzunluklarının standart sapması

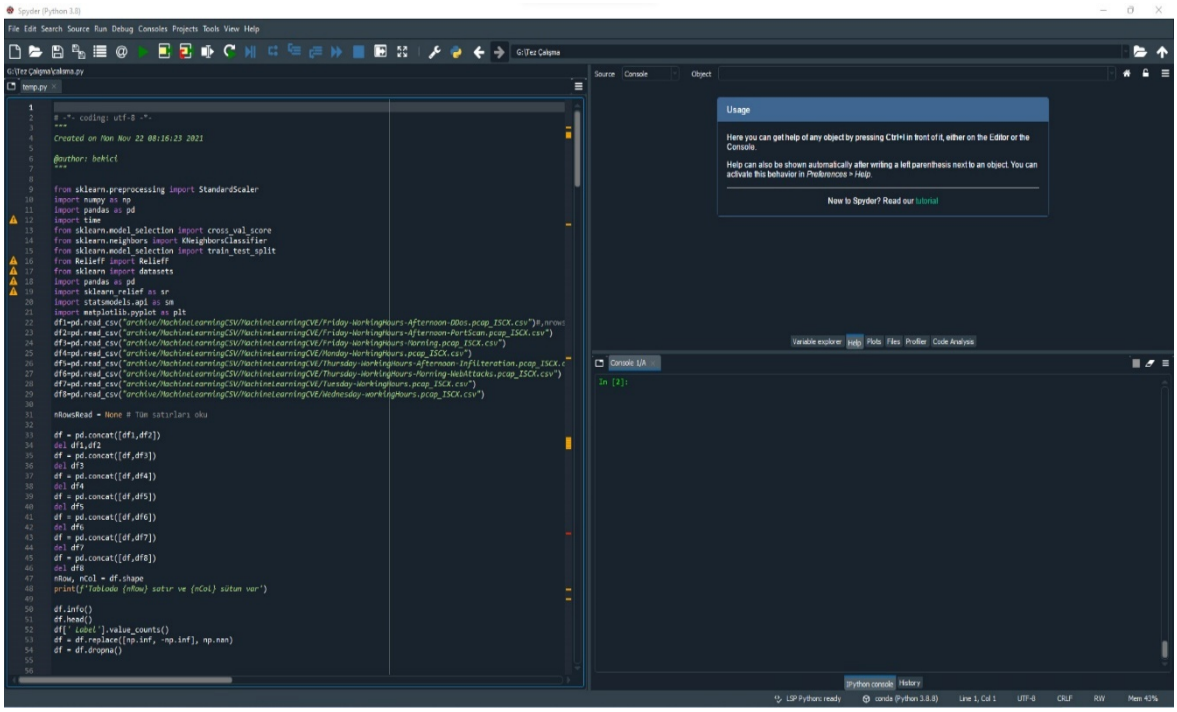
Flow Bytes/s	Saniyede akan byte sayısı
Flow Packets/s	Saniyede akan paket sayısı
Flow IAT Mean	Paketlerin varış zamanı ortalaması
Flow IAT Std	Paketlerin varış zamanlarının standart sapması
Flow IAT Max	Paketlerin maximum varış zamanı
Flow IAT Min	Paketlerin minimum varış zamanı
Fwd IAT Total	İleri yönde gönderilen iki paket arasındaki toplam zaman
Fwd IAT Mean	İleri yönde gönderilen iki paket arasındaki ortalama zaman
Fwd IAT Std	İleri yönde gönderilen iki paket arasındaki zamanın standart sapması
Fwd IAT Max	İleri yönde gönderilen iki paket arasındaki maksimum zaman
Fwd IAT Min	İleri yönde gönderilen iki paket arasındaki minimum zaman
Bwd IAT Total	Geri yönde gönderilen iki paket arasındaki toplam zaman
Bwd IAT Mean	Geri yönde gönderilen iki paket arasındaki ortalama zaman
Bwd IAT Std	Geri yönde gönderilen iki paket arasındaki zamanın standart sapması
Bwd IAT Max	Geri yönde gönderilen iki paket arasındaki maksimum zaman
Bwd IAT Min	Geri yönde gönderilen iki paket arasındaki minimum zaman
Fwd PSH Flags	İleri yönde hareket eden paketlerde PSH bayrağının aktif olma sayısı (UDP için 0)
Bwd PSH Flags	Geri yönde hareket eden paketlerde PSH bayrağının aktif olma sayısı (UDP için 0)
Fwd URG Flags	İleri yönde hareket eden paketlerde URG bayrağının aktif olma sayısı (UDP için 0)
Bwd URG Flags	Geri yönde hareket eden paketlerde URG bayrağının aktif olma sayısı (UDP için 0)
Fwd Header Length	İleri yöndeki başlıklar için kullanılan toplam byte
Bwd Header Length	Geri yöndeki başlıklar için kullanılan toplam byte
Fwd Packets/s	Saniyedeki ileri yön paket sayısı
Bwd Packets/s	Saniyedeki geri yön paket sayısı
Min Packet Length	Bir paketin minimum uzunluğu
Max Packet Length	Bir paketin maksimum uzunluğu
Packet Length Mean	Paketin ortalama uzunluğu
Packet Length Std	Paket standart sapması
Packet Length Variance	Paket uzunluk varyansı
FIN Flag Count	FIN içeren paket sayısı
SYN Flag Count	SYN içeren paket sayısı
RST Flag Count	RST içeren paket sayısı
PSH Flag Count	PUSH içeren paket sayısı
ACK Flag Count	ACK içeren paket sayısı
URG Flag Count	URG içeren paket sayısı
CWE Flag Count	CWE içeren paket sayısı
ECE Flag Count	ECE içeren paket sayısı

Down/Up Ratio	İndirme ve yükleme oranı
Average Packet Size	Ortalama paket boyutu
Avg Fwd Segment Size	İleri yönde gözlenen ortalama segment boyutu
Avg Bwd Segment Size	Geri yönde gözlenen ortalama segment boyutu
Fwd Header Length_1	İleri yönde başlıklar için kullanılan toplam byte
Fwd Avg Bytes/Bulk	İleri yönde byte/kütle oranının ortalama sayısı
Fwd Avg Packets/Bulk	İleri yönde paket/kütle oranının ortalama sayısı
Fwd Avg Bulk Rate	İleri yönde kütle oranının ortalama sayısı
Bwd Avg Bytes/Bulk	Geri yönde byte/kütle oranının ortalama sayısı
Bwd Avg Packets/Bulk	Geri yönde paket/kütle oranının ortalama sayısı
Bwd Avg Bulk Rate	Geri yönde kütle oranının ortalama sayısı
Subflow Fwd Packets	İleri yönde bir alt akıştaki ortalama paket sayısı
Subflow Fwd Bytes	İleri yönde bir alt akıştaki ortalama byte sayısı
Subflow Bwd Packets	Geri yönde bir alt akıştaki ortalama paket sayısı
Subflow Bwd Bytes	Geri yönde bir alt akıştaki ortalama bayt sayısı
Init_Win_bytes_forward	İlk pencere içinde ileri yönde gönderilen byte sayısı
Init_Win_bytes_backward	İlk pencere içinde geri yönde gönderilen bayt sayısı
act_data_pkt_fwd	İleri yönde en az 1 bayt TCP veri yüküne sahip paket sayısı
min_seg_size_forward	İleri yönde gözlenen minimum segment boyutu
Active Mean	Boşta kalmadan önce bir akışın aktif olduğu ortalama zaman
Active Std	Boşta kalmadan önce bir akışın aktif olduğu zamanın standart sapması
Active Max	Boşta kalmadan önce bir akışın aktif olduğu maksimum zaman
Active Min	Boşta kalmadan önce bir akışın aktif olduğu minimum zaman
Idle Mean	Aktif hale gelmeden önce bir akışın boşta olduğu ortalama zaman
Idle Std	Aktif hale gelmeden önce bir akışın boşta olduğu zamanın standart sapması
Idle Max	Aktif hale gelmeden önce bir akışın boşta olduğu maksimum zaman
Idle Min	Aktif hale gelmeden önce bir akışın boşta olduğu minimum zaman
Label	Saldırı etiketi

3.5. Yazılım Geliştirme Ortamı

Çalışmada son yıllarda özellikle veri analizleri ve makine öğrenmesi gibi konularda oldukça popüler olan "Python" yazılım dili kullanılmıştır. Python yazılım dili ile kullanılabilir Makine öğrenmesi ile alakalı birçok kütüphanenin varlığı, bu alanda yapılan çalışmalarda araştırmacılara yardımcı olmaktadır. Ayrıca Python dilinin modüler yapısı ve birçok işletim sisteminde çalışabilir olması gibi etkenler, çalışmada Python dilinin seçilmesinde etkili olmuştur.

Python yazılım dili için piyasada farklı tümleşik geliştirme ortamları (IDE) bulunmaktadır. “Spyder” da Python için veri analistleri, mühendisler ve bilim insanları tarafından sıklıkla tercih edilen, ücretsiz ve açık kaynaklı geliştirme ortamlarından biridir. Çalışmada Spyder’ın 4.2.5 sürümü kullanılmıştır. Resim 3.1’de Spyder çalışma ortamı gösterilmektedir.



Resim 3.1. Spyder Çalıma Ortamı

Çalışma sürecinde faydalanılan bazı Python kütüphaneleri; Sklearn, Numpy, Pandas, Matplotlib’dir.

3.5.1. Sklearn kütüphanesi

Python dilinde “sklearn” olarak yer bulan “Scikit-Learn” kütüphanesi makine öğrenmesi konularında ve veri biliminde sıklıkla kullanılan Python açık kaynaklı kütüphanelerinden biridir. Bu kütüphane ile kümeleme, karar ağaçları ve regresyon gibi yöntemlerin uygulanması sağlanarak veri analizi kolaylaştırılmaktadır. Ayrıca bu yöntemlerin işlevleri ve arka planıyla alakalı dokümantasyonu da sağlamaktadır.

3.5.2. NumPy kütüphanesi

NumPy kütüphanesi ismini “Numerical Python” tanımlamasından almaktadır. Adından da anlaşılacağı üzere bu kütüphane bilimsel hesapların hızlı bir şekilde yapılmasına yarar. Bu kütüphanenin temel dayanağı dizilerdir. Dizi işlemlerinin hızlı şekilde gerçekleştirilmesi için sıklıkla kullanılır. Veri bilimi ve makine öğrenmesinde de büyük boyutlu verilerle çalışıldığı göz önüne alındığında NumPy kütüphanesinin bu alanlarda sıklıkla kullanılmasının nedeni daha net anlaşılmaktadır.

3.5.3. Pandas kütüphanesi

Hızlı ve esnek veri yapıları sağlamak suretiyle, etiketli ve ilişkisel verilerle çalışmayı daha kolay hale getirmek için NumPy kütüphanesinin temelleri üzerine inşa edilerek oluşturulmuş bir Python paketidir. Verilerin temizlenmesi, analizinin yapılması ve model oluşturulması gibi işlevlerin yerine getirilmesi hususunda ideal bir araçtır. Büyük veri kümelerinde eksik verilerin tespitinin yapılması, verilerin dönüştürülmesi, verilerin şekillendirilmesi ve boyutlarının değiştirilmesi gibi işlemlerde de bu kütüphane tercih edilmektedir.

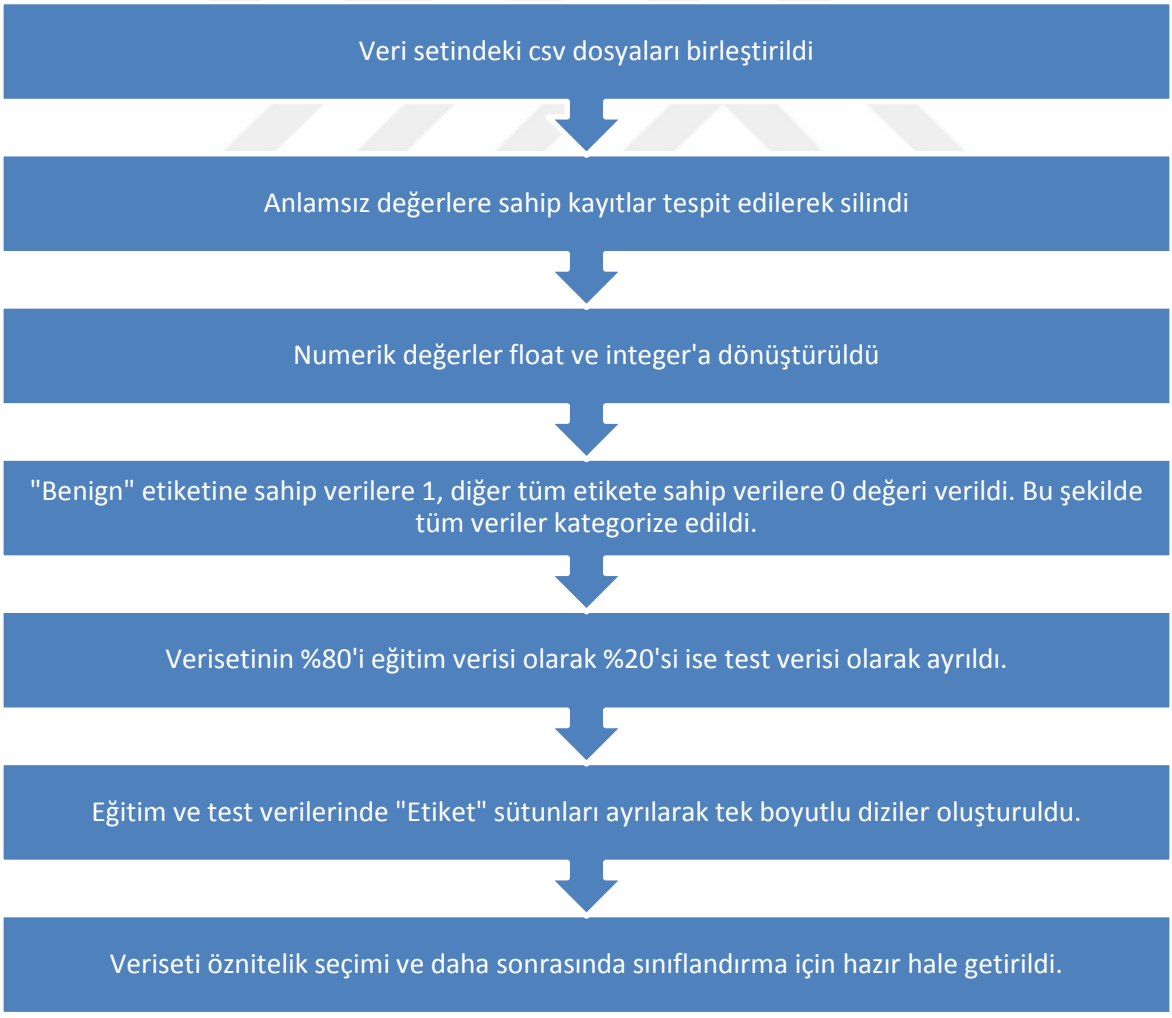
3.5.4. Matplotlib kütüphanesi

Veri biliminde görsellik önemli bir etkendir. Çünkü veriyi analiz ederek bilgi elde etmenin en kolay yolu görselleştirmedir. Matplotlib, Python’da veri görselleştirmek için en kapsamlı işlevleri bünyesinde barındırarak bunların en kolay şekillerde uygulanmasını sağlayan 2 boyutlu çizim kütüphanelerinden biridir. Bu çalışma bünyesinde sunulan grafiklerde Matplotlib kütüphanesinden yararlanılmıştır.

3.6. Veri Ön İşleme

Ön işleme aşamasında, öncelikli olarak orijinal verisetinde ayrık olan csv uzantılı dosyalar, kodlama ortamında Pandas kütüphanesi yardımıyla okunarak tek bir “data frame” nesnesinde birleştirilmiştir. Bu aşamada bundan sonraki tüm işlemler bu obje üzerinden devam ettirilmiştir.

Tek bir nesne üzerinde birleştirilen veri seti bünyesindeki kayıtlardan sonsuz ya da anlamsız değerlere sahip olanlar tespit edilerek silinmiştir. Daha sonra herhangi bir değere sahip olmayan kayıtlar da çalışmada tutarlılığın sağlanması açısından bulunarak kaldırılmıştır. Çalışmanın daha sağlıklı ilerleyebilmesi için numerik değerler float ve integer veri tiplerine dönüştürülmüştür. Bu işlemden sonra çalışmanın temel amacına uygun şekilde, yani saldırının çeşidinden bağımsız olarak saldırının olup olmadığının belirlenebilmesi amacıyla "Benign" etiketine sahip veriler "0", diğer tüm saldırı tipleri ise "1" olarak düzeltilmiştir. Bu şekilde veri seti ikili sınıflandırmaya hazır hale getirilmiştir. Bundan sonra ise eldeki verilerin %80'i modelin eğimi için, kalan %20'si ise oluşturulan modelin test edilmesi için ayrılmıştır. Son olarak veri setindeki "Label" yani etiket sütunu eğitim ve test setleri için tek boyutlu dizilere dönüştürülmüştür. Veri ön işleme aşamasında izlenen metodoloji Şekil 3.6'da görülmektedir.



Şekil 3.6. Veri Ön İşleme Aşamaları

3.7. Öznitelik Seçimi

Öznitelik seçimi, üzerinde çalışılan örneği belirli kriterlere göre en iyi temsil edebilecek özniteliklerin mevcut öznitelik kümesi içerisinden seçilmesi işlemi iken, öznitelik çıkarılması ise yeni bir öznitelik uzayı oluşturmak amacıyla mevcut bilgilere dönüştürme işlemi uygulanmasıdır (Küçüksille & Ateş, 2016).

Çalışmada kullanılan veri setinde 83 farklı öznitelik bulunmaktadır. Oluşturulacak olan saldırı tespit sisteminde ağ trafiğinin izlenerek saldırı tespitinin başarı oranının artırılması ve çalışma zamanının da buna bağlı olarak mümkün olduğunca kısa tutulması amacıyla mevcut 83 farklı özniteliğin sayısının indirgenmesi gerekmektedir. Bu indirgeme işlemi sırasında sınıflandırma işleminde en başarılı sonuçları sağlayacak, sınıflandırma için en anlamlı özniteliklerin korunarak, sınıflandırma sürecinde pek de etkisi olmayan özniteliklerin veri seti dışarısında bırakılmasına dikkat edilmiştir.

Geçmiş çalışmalar, saldırı tiplerine göre veri setinde bulunan farklı öznitelik gruplarının seçilmesinin saldırı tespitinin başarısını olumlu yönde etkilediğini göstermektedir. Örneğin DDoS (Distributed Denial of Service attack) saldırısının belirtileri belirli öznitelikler üzerinde görülürken, Brute Force saldırı tipine ait belirtiler de farklı öznitelik gruplarında görülmektedir. Ancak bu çalışmada, saldırı tipinden ziyade saldırının olup olmadığıyla ilgilenildiğinden dolayı, veri setindeki tüm saldırı tiplerinde mümkün olduğunca ortak belirti gösteren veya saldırı tiplerinin çoğunda belirti gösteren özniteliklerin ortaya çıkarılması planlanmıştır. Bu plan doğrultusunda hem makine öğrenmesi teknikleriyle hem de manuel olarak çeşitli öznitelik grupları seçilmiş ve sınıflandırma çalışmaları yapılmıştır.

3.7.1. Özyinelemeli özellik seçimi (RFE)

Saldırı tespitinde en anlamlı özniteliklerin seçilmesi adına çalışma boyunca farklı teknikler uygulanıp sonuçları değerlendirilmiştir. Öncelikle öznitelik seçim tekniklerinden biri olan Özyinelemeli Özellik Seçimi (RFE)(Recursive Feature Elemination) tekniği kullanılmıştır. Bu teknikte veri seti alt kümeler halinde istenilen bir denetimli öğrenme tekniği ile değerlendirilerek her alt kümenin en az değerli özelliği bulunarak küme dışına itilir ve bu işlem özyinelemeli olarak istenilen sayıda özellik kalana kadar devam eder (Scikit Learn, 2022).

Bu tekniğin arkasında yatan temel mantık, öne çıkarılmak istenilen n tane en anlamlı özniteliğin bulunabilmesi için veri setinde bulunan tüm özniteliklerin alt kümelere bölünerek, bu alt kümelerde bulunan özniteliklerin önem derecelere göre puanlanması ve önem derecesi en az özniteliklerin alt kümelerden elenerek bu işlemin n tane en çok öneme sahip öznitelik kalana kadar öz yinelemeli olarak devam etmesidir. Önem derecesinin belirlenmesinde denetimli bir öğrenme algoritması kullanılır.

Li ve diğerleri (2021), yaptıkları çalışmada CICIDS 2017 veri setinde en başarılı sınıflandırmayı yapabilmek için ortalama 10,2 tane öznitelik kullanılması gerektiğini savunmuşlardır. Bu çalışmada da öznitelik seçilmesi aşamasında 2 farklı teknik kullanılacağı için ilk aşamada bu sayının 2 katı olan 20 özniteliğin öne çıkarılması amaçlanmıştır. Bu amaç doğrultusunda, çalışmada Rastgele Orman (RF) denetimli öğrenme tekniği kullanılarak oluşturulan RFE modeli ile öznitelik sayısının 20'ye indirgenmesi sağlanmıştır.

3.7.2. İleri yönelimli seçim (FS)

İleri Yönelimli Seçim (Forward Selection) tekniğinde belirlenen bir p eşik değeri baz alınarak en başta boş küme olan seçilen özellikler kümesine adım adım özellik seçilir (Vikas Verma, 2020). Özelliklerin değerlerinin hesaplanmasında ise Sıradan En Küçük Kareler (Ordinary Least-Squares Model)(OLS) modeli kullanılır. Bu hesaplama tekniği bir veya daha fazla açıklayıcı değişken ile karesel hataların toplamını (buradaki hata kavramı sonuç değişkeninin tahmin edilen değeri ile gerçek değeri arasındaki farktır) en aza indiren sürekli veya en azından aralıklı sonuç değişkeni arasındaki ilişkiyi modeller (Zdaniuk, 2014). Bu şekilde eşik değer altında kalan özellik kalmayana kadar adım adım devam eden işlemler sonucunda elde edilen özellikler veri setindeki en anlamlı öznitelikler olarak öne çıkar.

FS tekniği daha yakından incelenecek olursa, en başta seçilecek öznitelik kümesini bir boş küme olarak düşünmek daha doğru olur. Bahsedilen boş kümenin ilk elemanı, tüm öznitelikler ile hedef değişken yani sınıf etiketi arasındaki ilişkiye bakılarak en fazla hedef değişkeni etkileyen ya da daha kapsamlı olarak hedef değişkeni en iyi tarif eden öznitelik seçilerek belirlenir. Daha sonra ise seçilen bu öznitelik yanına hangi diğer öznitelik eklenirse, seçilecek öznitelik kümesinde oluşacak 2'li öznitelik hedef değişkeni en iyi tarif

eder sorusuna cevap aranır. Tüm öznitelikler bu şekilde taranarak en iyi performans gösterecek öznitelik aranır ve öznitelik kümesine eklenir. Sonrasında ise aynı işlem öznitelik kümesine eklenecek 3. Eleman için tekrarlanır ve birlikte hedef değişkeni tasvir eden en iyi 3'lü öznitelik grubu belirlenir. Bu işlem belirlenen "p" eşik değeri altında öznitelik kalmayana kadar devam eder.

Bahsedilen eşik değeri "p" ise kullanıcının tanımladığı bir değişkendir. Ancak eşik değerinin belirlenmesi hususunda kesin bir kanı olmamakla beraber bu değer istatistiksel hesaplamaların göz önüne alınması neticesinde genellikle 0,05 olarak belirlenir. SPSS (Statistical Package for the Social Sciences) yazılımında bağlantılı ihtimalin ayarlanması için kullanılan normal ölçüt de 0,05'tir. Bu değerin üstünde kalanlar değişkenler istatistiksel olarak anlamsız, bu değer ile 0,01 arasında kalan değerler ise istatiksel olarak anlamlı kabul edilir (Alfa İstatistik, 2018).

Elde edilen 20 öznitelik İleri Yönelimli Seçim (Forward Selection, FS) tekniği kullanılarak tekrar öznitelik seçim işlemine tabi tutulmuştur. Eşik değeri p'nin 0,05 seçilmesiyle yapılan işlemde 20 olan öznitelik sayısı 16'ya düşürülmüştür.

3.7.3 Manuel seçim yöntemi

Çalışmada önerilen hibrit yaklaşımlı öznitelik seçim yöntemi dışında deney sayısını artırarak farklı öznitelik gruplarının seçilmesinin ortaya çıkacak sınıflandırma başarısına etkisini gözlemleyebilmek için makine öğrenmesi teknikleri haricinde manuel seçim yöntemiyle de belirli öznitelik grupları seçilerek sınıflandırma testlerine tabi tutulmuştur. Manuel öznitelik seçimlerinde literatürde bulunan çalışmalarda kullanılan öznitelikler, network bilgisine dayalı olarak daha fazla öne çıktığı düşünülen öznitelikler, ön çalışma sürecinde deneme-yanılma yoluyla elde edilen verilerde nispeten daha başarılı bulunan öznitelikler ve CICIDS 2017 veri seti üzerinde öznitelik önem dereceleri üzerinde yapılan çalışmalarda öne çıkan özniteliklerin kombinasyonuyla oluşan gruplar dikkate alınmıştır.

Gosu ve diğerleri (2021) çalışmalarında CICIDS 2017 veri seti üzerinde farklı parametrelerle 4 farklı öznitelik grubu oluşturmuştur. 4 farklı öznitelik gurubundan ilkinde 8 öznitelik, ikincisinde 13 öznitelik, üçüncüsünde 21 öznitelik ve dördüncüsünde 34

öznitelik bulunmaktadır. Bu çalışmayla beraber, Shams (2020)'ın çalışmasında da CICIDS 2017 veri seti üzerinde sınıf etiketlerine göre en belirgin öznitelikler belirtilmiştir.

Çizelge 3.4. Sınıflara göre en önemli öznitelikler (Shams, 2020)

Sınıf	Öznitelik
DoS Hulk	Bwd Packet Length Std, Fwd Packet Length Std, Fwd Packet Length Max, Flow Duration
PortScan	Flow Bytes/s, Total Length of Fwd Packets, Fwd Packet Length Max, Flow IAT Mean
DDoS	Bwd Packet Length Std, Total Backward Packets, Fwd IAT Total, Total Length of Fwd Packets
DoS GoldenEye	Flow IAT Max, Bwd Packet Length Std, Flow IAT Min, Total Backward Packets
FTP-Patator	Fwd Packet Length Max, Fwd Packet Length Std, Fwd Packet Length Mean, Bwd Packet Length Std
SSH-Patator	Fwd Packet Length Max, Flow IAT Mean, Flow IAT Max, Total Length of Fwd Packets
DoS slowloris	Flow IAT Mean, Total Length of Bwd Packets, Bwd Packet Length Mean, Total Fwd Packets
DoS Slowhttptest	Flow IAT Mean, Fwd Packet Length Std, Fwd Packet Length Mean, Fwd Packet Length Min
Bot	Bwd Packet Length Mean, Flow Duration, Flow IAT Std, Flow IAT Min
Web Attacks	Bwd Packet Length Std, Flow IAT Min, Total Length of Fwd Packets, Bwd Packet Length Max
Infiltration	Fwd Packet Length Mean, Total Backward Packets, Total Length of Fwd Packets, Flow Duration
Heartbleed	Bwd Packet Length Mean, Bwd Packet Length Max, Total Length of Fwd Packets, Fwd Packet Length Max

İlgili çalışmalar sonucu ortaya çıkan veriler, manuel seçimli öznitelik grupları oluşturulurken dikkate alınmıştır. Çalışmada asıl odaklanılan konu ikili sınıflandırma olduğu için, oluşturulan manuel seçimli öznitelik gruplarında bu çalışmalarda belirtilen öznitelik grupları birebir aynısı olacak şekilde kullanılmamıştır. Ancak bu bilgiler ışığında mümkün olacak şekilde gruplarda ortak olarak yer alan öznitelikler ve yapılan deneylerde de iyi sonuç verdiği gözlemlenen öznitelikler manuel öznitelik gruplarının belirlenmesinde etken olmuştur.

3.8. Sınıflandırma

3.8.1. XGB algoritması

XGB, karar ağacı temelli gradyan yükseltme (boosting) algoritmasının etkili ve ölçeklenebilir bir versiyonudur. 2016 yılında Tianqi Chen ve Carlos Guestrin tarafından makale olarak sunulduktan sonra sadece akademik olarak değil çeşitli platformlardaki makine öğrenmesi sistemleriyle alakalı yarışmalarda da veri analizcileri tarafından sıklıkla kullanılmaktadır. XGB algoritmasının elde ettiği başarının arkasındaki en önemli faktör kullanılacağı tüm senaryolar için ölçeklenebilir olmasıdır (Chen & Guestrin, 2016).

XGB algoritması, zayıf öğrenici olarak da adlandırılan nispeten güçsüz olan karar ağaçlarının bir araya getirilerek topluluk öğrenmesi yoluyla çok daha güçlü bir ağaç ortaya konulması mantığına dayanır. Diğer yükseltme algoritmalarında olduğu gibi zayıf algoritmayı sıralı ve yinelemeli eğiterek güçlendirir. Algoritmanın içerisinde oluşturulan her ağaç kayıp fonksiyonunu azaltmak için eklenir ve eklenen her ağaç bir önceki ağacın modeli ile beslendiği için bu kayıp oranını azaltır. Bu yapıyla birlikte çeşitli optimizasyonlar yapılarak performans iyileştirilmesi sağlanmış ve XBG algoritması ortaya çıkarılmıştır.

XGB algoritmasını daha iyi anlayabilmek için topluluk öğrenme algoritmalarının temel mantığını incelemek gerekir. Topluluk öğrenmesinde model tek bir öğrenici yerine birden fazla öğrenici ile eğitilir. Daha yalın bir ifadeyle birkaç modelden gelen tahminler tek bir modelde toplanır. Birden fazla eğitici kullanılarak modelin daha doğru karar vermesi ve başarısının artması sağlanır.

Topluluk öğrenmesinde bahsedilen farklı modellerin bir araya getirilmesi için bazı yöntemler kullanılır. Yaygın olarak Torbalama (Bagging) ve Yükseltme (Boosting) yöntemleri kullanılsa da bunların dışında da farklı yöntemler kullanılabilmektedir.

Torbalama yönteminde model içinde kullanılan eğiticiler paralel olarak çalışır. Model içerisinde kullanılan eğiticiler birbirinden bağımsız çalışır. Dolayısıyla ortaya birden fazla sonuç çıkar. Birden fazla modelin ortaya koyduğu bu farklı sonuçlar oylama, ağırlıklı ortalama vb. yöntemlerle tek bir sonuç çatısı altında birleştirilir ve modelin son kararı olur.

Yükseltme yönteminde ise topluluk öğrenmesi içerisinde bulunan birden fazla farklı eğitici sıralı olarak çalışır. Yani her bir eğitici sırayla alınarak bir önceki eğiticinin hatasına göre modelleme işlemi devam eder. Daha iyi performans gösteren eğiticilere daha çok ağırlık verilir. Böylece her eğitici kendisinden önceki eğiticilerin hatasından ders alarak sonuçta çok daha başarılı bir modelin oluşturulmasına katkı yapar.

XGB algoritmasının temelini oluşturan Gradyan Yükseltme algoritması da bu şekilde bir yükseltme algoritmasıdır. Gradyan Yükseltmede temel öğrenici olarak kullanılan tahmin ağaçları, sıralı olarak her bir ağacın hesapladığı hatalar üzerine set halinde kurulur. Amaç hatayı en aza indirgemektir. Burada hata olarak bahsedilen kayıp fonksiyonudur ve 1. dereceden denklemlerle hesaplanır.

XGB algoritması, geleneksel gradyan yükseltme algoritmalarının optimize edilmiş bir türüdür. XGB algoritmasının geleneksel gradyan yükseltme algoritmalarına göre en büyük avantajlarından biri aşırı öğrenmeyi engellemek üzerine daha düzgün biri yapıyı bünyesinde barındırmasıdır. XGB'de ağaçların derinliği için bir sınır kullanılır ve ağaç bu sınır değeri aştığında budama işlemi yapılarak aşırı öğrenmenin önüne geçilir. Bununla birlikte Gradyan yükseltmede kayıp fonksiyonu 1. dereceden denklemlerle hesaplanırken XGB'de bu fonksiyon 2. Dereceden denklemlerle hesaplanır. Ayrıca diğer makine öğrenme algoritmalarına oranla hesaplanabilirliğinin çok daha kolay olması nedeniyle çok boyutlu büyük verilerin analizinde verimli bir şekilde kullanılabilmektedir.

3.8.2. Naive bayes algoritması

Thomas Bayes'in 1812 yılında ortaya koyduğu teoreme dayanan Naive Bayes algoritması olasılık tabanlı bir sınıflandırma yöntemidir. Basitçe ifade etmek gerekirse bu algoritma, gelecekteki olayların tahminini gerçekleştirmek için önceki olaylara ait verileri kullanır.

Naive Bayes algoritmasında öğrenilecek kavrama ait tüm öznitelikler birbirinden bağımsız olarak değerlendirilir ve ilgili kavramın bu özniteliklerin tümüne bağlı olduğu bir ağ düşünülür. Her bir özniteliğin bağımsız olarak ele alınması ve bu özniteliklere ait olasılıkların en yüksek olana göre sınıflandırılması bu algoritmanın uygulanabilirliğini kolaylaştırır. Dolayısıyla daha az eğitim verisiyle çok daha başarılı sınıflandırma sonuçları

elde edilebilir. Bu etmenler, Naive Bayes algoritmasının veri madenciliğinde, sinyal ve görüntü işleme alanlarında en çok kullanılan sınıflandırma ve tahmin algoritmalarından biri olmasında önemli rol oynar.

Naive Bayes algoritması sahip olduğu bu avantajların yanında bazı dezavantajlara da sahiptir. Şüphesiz bu dezavantajların en önemlisi, algoritma içerisinde koşulsal olarak birbirinden bağımsız olarak değerlendirilen özniteliklerin arasındaki ilişkiler hiçbir zaman modellenemez.

3.8.3. Karar ağacı algoritması

Karar ağacı (DT) algoritması sınıflandırma problemlerinde sıklıkla kullanılan denetimli öğrenme algoritmalarından biridir. Kategorik ve sürekli değerlerle çalışabilen bu algoritmada karar ağacı, bir ağaç şeklinde sınıflandırma ve regresyon modelleri oluşturur. Üzerinde çalışılan veri seti kendinden daha küçük alt veri setlerine bölünerek ortaya ilişkili bir karar ağacı ortaya çıkarılır. Sonuçta, karar düğümleri ve yaprak düğümleri olan bir ağaç yapısı oluşur.

DT algoritmasıyla oluşturulan modellerin okunması ve anlaşılması basittir. Ayrıca bu algoritmanın hızlı bir şekilde ağaç yapısının oluşturabilmesi algoritmanın yaygın bir şekilde kullanılmasını sağlamıştır. Bu gibi avantajlarının yanında, algoritmanın kısmen tutarsız sonuçlar üretmesi, nümerik verilerde karmaşayı artırması, birden fazla öznitelik içeren çıktıları mümkün kılmaması gibi dezavantajları da bulunmaktadır.

DT algoritmasından daha fazla verim elde edebilmek için torbalama (bagging) ve artırma (boosting) teknikleriyle topluluk öğrenmesi algoritmaları geliştirilmiştir.

3.8.4. Rastgele orman algoritması

Rastgele Orman (RF) algoritması torbalama yöntemiyle birden fazla karar ağacı oluşturan ve oylama yöntemiyle en iyi tahmini oluşturan bir denetimli öğrenme algoritmasıdır. Zaten torbalama yönteminin temel özelliği öğrenme modellerinin kombinasyonlarıyla başarı oranını artırmaktır. RF algoritması adından da anlaşılacağı gibi torbalama yöntemine rassallık eklenmesi suretiyle oluşturulan gelişmiş bir algoritmadır.

RF algoritması, mevcut değişkenler içinden en iyi dalın üzerinden her bir düğümü dallara ayırmak yerine, rassal olarak her düğümde seçilen değişkenler arasından en iyisini kullanarak düğümleri dallara ayırır. Her veri seti yer değiştirmeli olarak orijinal veri setinden üretilir. Bunu takiben rastgele özellik seçimi kullanılarak ağaçlar geliştirilir. Geliştirilen ağaçlar budanmaz. Bu strateji RF algoritmasının doğruluğunu eşsiz yapar. (Akar, Ö. & Güngör, O)

Günümüzde RF algoritması hızı, basitliği ve esnekliği ile görüntü işleme, e-ticaret, bankacılık, tıp gibi birçok farklı alanlarda başarıyla kullanılmaktadır.

3.8.5. Lojistik regresyon algoritması

Logistic Regresyon (LR) analizinin amacı, en az değişkeni kullanarak en iyi uyuma sahip olacak şekilde bağımlı ve bağımsız değişkenler arasındaki ilişkiyi tanımlayabilen kabul edilebilir bir model kurmaktır (Bircan, 2004).

Makine öğrenmesinde LR algoritması genelde ikili sınıflandırma problemlerinde kullanılan istatistik tabanlı, denetimli bir öğrenme algoritmasıdır. LR'de hedef değişken kategorik ve çoğunlukla ikilidir. Hedef değişkenin ikiden fazla olduğu durumlarda ise çok terimli lojistik regresyon kullanılabilmektedir.

LR algoritmasının yorumlanması ve uygulanması kolay olmakla birlikte üzerinde çalışılan veri seti doğrusal olarak ayrılabilirse, bu durum algoritmanın başarı oranına olumlu şekilde katkı yapar.

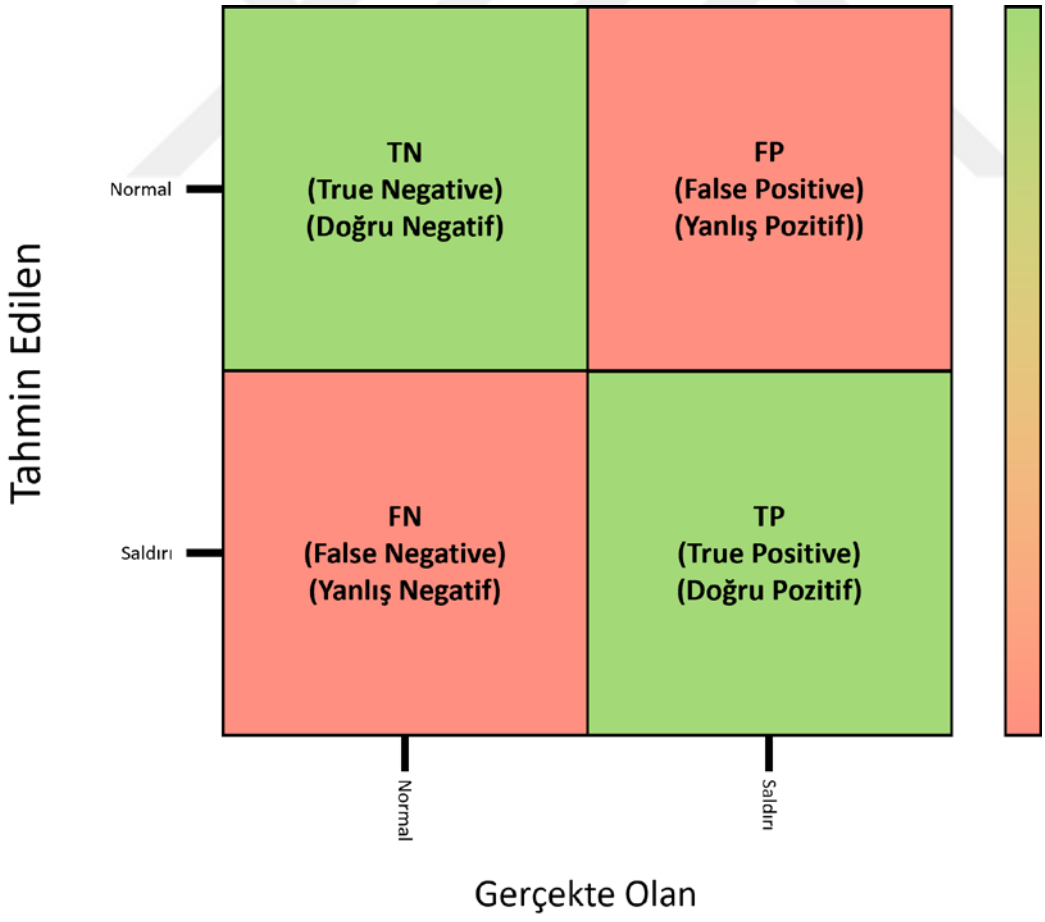
3.9. Değerlendirme

Makine öğrenmesi alanlında oluşturulan modellerin başarı oranının tespit edilmesi kritik derecede öneme sahiptir. Başarı oranı tespit edilerek oluşturulan modellerde iyileştirme yapılıp yapılmayacağının kararı verilir, model başarısız bulunursa hatalar düzeltilir ve modelin geliştirme sürecinin devam edilmesi sağlanır. Başarı oranı yeterliyse çalışmanın amacına göre gerçeğe en yakın şekilde tahminler üretilip sınıflandırmalar yapılır. İşte bu şekilde oluşturulan modellerin değerlendirilmesi için farklı araçlara başvurulur.

Bu çalışma kapsamında yapılan deneylerden elde edilen sonuçların değerlendirilmesi için Karmaşıklık Matrisi, Çapraz Doğrulama ve ROC Eğrisi yöntemleri Doğruluk (Accuracy), Kesinlik (Precision), Duyarlılık (Recall) ve F1 metriklerinden yararlanılmıştır.

3.9.1. Karmaşıklık Matrisi

Karmaşıklık matrisi en yalın şekilde veri setindeki mevcut durum ile modelin ürettiği doğru ve yanlış sayılarını göstererek modelin başarı oranı hakkında fikir veren tablo olarak ifade edilebilir. Karmaşıklık matrisinin boyutu, yapılan sınıflandırmadaki sınıf sayısı büyüklüğüne göre belirlenir. Bu çalışmada ağda belirtilen normal trafik verileri ve saldırı içeren trafik verileri olduğu için iki sınıflı bir karmaşıklık matrisiyle değerlendirme yapılmıştır. İki sınıflı veri seti için 4 farklı olasılık söz konusudur. Şekil 3.7'de çalışmada kullanılan karmaşıklık matrisi gösterilmektedir.



Şekil 3.7. Karmaşıklık Matrisi

TP (True Positive): Doğru pozitif olarak adlandırılır. Bu çalışmada saldırı içeren ağ trafiği olarak tahmin edilen verilerin gerçekte de saldırı içeren veriler olduğu durumdur.

FP (False Positive): Yanlış pozitif olarak adlandırılır. Bu çalışma için gerçekte normal olan ağ trafiği verisinin sistem tarafından saldırı içerikli veri olarak tahmin edildiği durumdur.

TN (True Negative): Doğru negatif olarak adlandırılır. Bu çalışma için gerçekte normal olarak nitelendirilen ağ trafiğinin sistem tarafından da normal ağ trafiği olarak tahmin edildiği durumu belirtir.

FN (False Negative): Yanlış negatif olarak adlandırılır. Bu çalışmada, gerçekte saldırı içeren ağ trafiği verisinin sistem tarafından normal olarak tahmin edildiği durumdur.

3.9.2. ROC eğrisi

ROC (Receiver Operating Characteristics) analizi ilk defa 1940'lı yıllarda gürültüye maruz kalan sinyallerin doğru bir şekilde algılanarak tanınması amacıyla kullanılmaya başladı. Zaten terimin açılımında var olan ve Türkçe karşılığı "alıcı" olan ifade radar alıcılarına yapılan bir atıftı (Karcı, Z, 2017). Bu analizin kullanılmaya başlanmasında 2. Dünya Savaşında radarların kullanılması dost kuvvetlerin yanlış bir şekilde tanımlanmasından kaçınarak ve düşman hava araçlarının doğru şekilde ayırt edilmesi fikri yatmaktaydı. Daha sonraları psikolojik analizlerde, verem hastalığının tespiti için farklı göğüs filmlerinin karşılaştırılması için radyolojide ve 1980'li yılların son zamanlarında ise Makine Öğrenmesinde kullanılmaya başlandı. Veri madenciliğinde de kullanılan ROC analizi, karar destek sistemleri arasındaki farkları değişik yöntemlerle değerlendirmektedir.

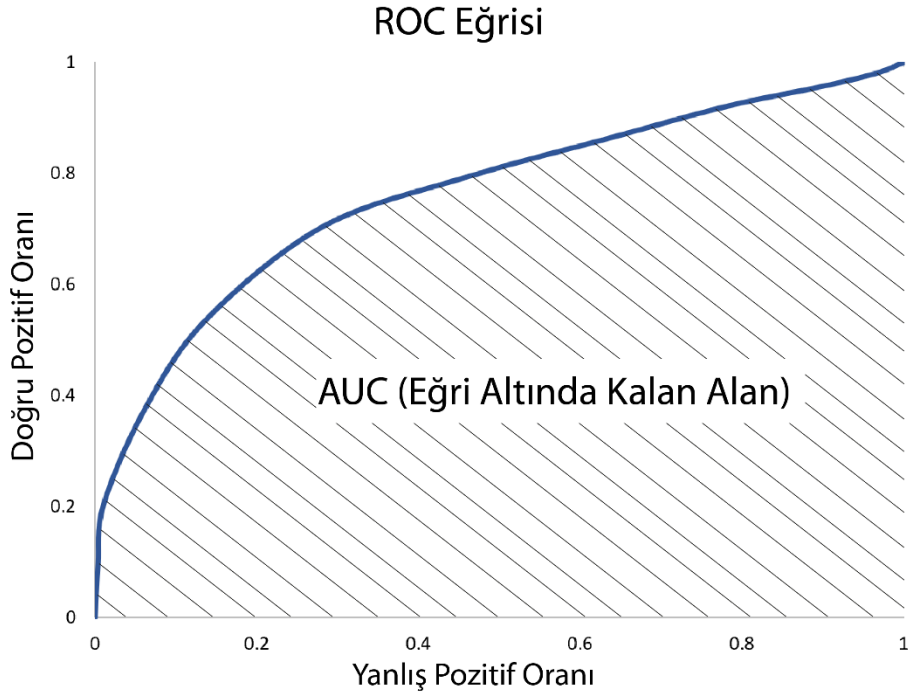
Daha özel bir perspektiften bakılacak olursa, ROC eğrisi temelinde sınıflandırma problemi olan olayların çözümü için oluşturulan modellerin ne kadar iyi çalıştığının anlaşılması amacıyla kullanılmaktadır.

ROC eğrisinde değişik eşik değerlerine göre yatay eksende yanlış pozitiflik (özgüllük) oranı bulunurken, dikey eksende doğru pozitiflik (duyarlılık) oranı yer alır. ROC eğrisi üzerindeki her nokta, farklı eşik değerlerine karşılık gelen duyarlılık ve özgüllük

değerlerini ortaya koyar. Genelde düşük yanlış pozitiflik oranlarını veren eşik değerleri, düşük doğru pozitiflik oranına da sahiptir. Doğru pozitiflik oranı arttıkça, yanlış pozitiflik oranı da artar (Tomak & Bek, 2011).

ROC eğrisinin veriminin ölçülmesinde en sık kullanılan yöntemlerden biri AUC (Area Under Curve – Eğri Altında Kalan Alan) yöntemidir. Bu yöntemde adından da anlaşılacağı gibi ROC eğrisinin altında kalan alanı esas alır. Bu metot ile testin pozitif ve negatif değerlerini ayırmasındaki doğruluk oranı tespit edilir. ROC eğrisi altında kalan alan büyüdükçe AUC değeri büyür. AUC değeri 0 ve 1 değerleri arasında yer alır ve bu değer 1'e yakınlaştıkça testin doğruluğu artmaktadır.

Şekil 3.8'de ROC Eğrisinde AUC değeri gösterilmektedir. Bu çalışmada gösterilen ROC Eğrisi grafiklerinde de AUC değerlerine yer verilmiştir.



Şekil 3.8. ROC Eğrisi ve AUC

3.9.3. Çapraz doğrulama

Makine öğrenmesi teknikleri kullanılırken eğitim ve test veri setlerine rastgele eleman atanır. Bazı durumlarda bu atama sonucunda veri ve eğitim setlerinin dengesiz dağılımdan kaynaklı yanıltıcı durumlar ortaya çıkabilir. Örneğin, test için ayrılan verilerin karakteristiği birbirine çok benzeyerek oluşturulan modelin çok başarılı olduğuna dair

veriler ortaya çıkabilir. Bu şekilde veri setinin dağılımı veya parçalanması nedeniyle ortaya çıkan yanılsama, sapma ve hataları en asgari düzeye indirebilmek için Çapraz Doğrulama (Cross Validation) kullanılarak modelin değerlendirilmesi yapılabilir.

En yaygın kullanılan çapraz doğrulama yöntemi ise K-Katlamalı Çapraz Doğrulama (K-Fold Cross Validation)'dur. Bu yöntemde K sayısı aslında tekrarlama sayısını belirtir. Veri seti bu sayıya bölünerek elde edilen alt setler eğitim ve test veri setleri olarak ayrılır. Her alt veri seti için eğitim ve test yapılarak hata oranları alınır. Bu işlem K sayısı kadar tekrar eder ve ortaya çıkan hata oranlarının ortalaması alınarak çapraz doğrulama değerleri belirlenir.

Bu çalışmada da 10 katlamalı çapraz doğrulama yöntemi kullanılarak sınıflandırma işlemlerinin doğrulamaları gerçekleştirilmiştir.

3.9.4. Doğruluk Metriği (Accuracy)

Doğruluk metriği (A), test aşamasında yapılan doğru tahminlerin sayısının toplam tahmin sayısına oranını ifade eder.

$$A=(TP+TN)/(TP+TN+FP+FN)$$

3.9.5. Kesinlik Metriği (Precision)

Kesinlik metriği (P), doğru tahmin edilen pozitif gözlem sayısının, pozitif olarak nitelendirilen tüm gözlem sayısına oranını gösterir. Yani bir başka deyişle pozitif olarak tahmin edilen verilerin içinde gerçekte kaç tanesinin pozitif olduğunu ifade eder.

$$P=TP/(TP+FP)$$

3.9.6. Duyarlılık Metriği (Recall)

Duyarlılık metriği (R), doğru tahmin edilen pozitif veri sayısının gerçekte ne kadar pozitif veri olarak tahmin edilmesi gereken veri sayısına oranıdır.

$$R=TP/(TP+FN)$$

3.9.7. F1 Metriği

F1 metriği (F1 Score) ise Kesinlik ve Duyarlılık metriklerinin harmonik ortalamasını gösterir.

F1= 2PR/(P+R)

4. BULGULAR VE TARTIŞMA

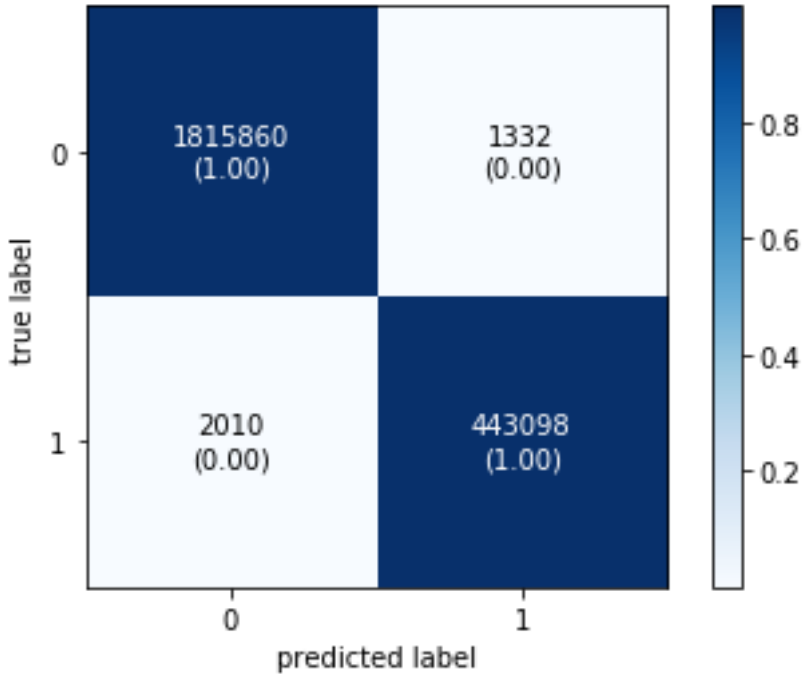
4.1. Birinci Öznitelik Grubu İle Yapılan Sınıflandırma Çalışmaları

Çalışmada öncelikli olarak iki aşamalı seçimle elde edilen 16 adet özniteliğe (Paketlere ait ortalama varış zamanı, Paketin ortalama uzunluğu, İlk pencere içinde ileri yönde gönderilen byte sayısı, İleri yönde gönderilen paketlerin toplam uzunluğu, Geri yönde gözlenen ortalama segment boyutu, Paket uzunluk varyansı, İlk pencere içinde geri yönde gönderilen byte sayısı, Paketin standart sapması, Paketin maksimum uzunluğu, Ortalama paket boyutu, Geri yönde paketlerin maksimum uzunluğu, Hedef port, Geri yönde paketlerin standart sapması, Geri yönde alt akıştaki byte sayısı, Geri yöndeki paketlerin toplam uzunluğu, Geri yönde paketlerin ortalama uzunluğu) dayalı sınıflandırma işlemleri uygulanmıştır. Sınıflayıcılara göre elde edilen eğitim sonuçları Çizelge 4.1'de gösterilmektedir.

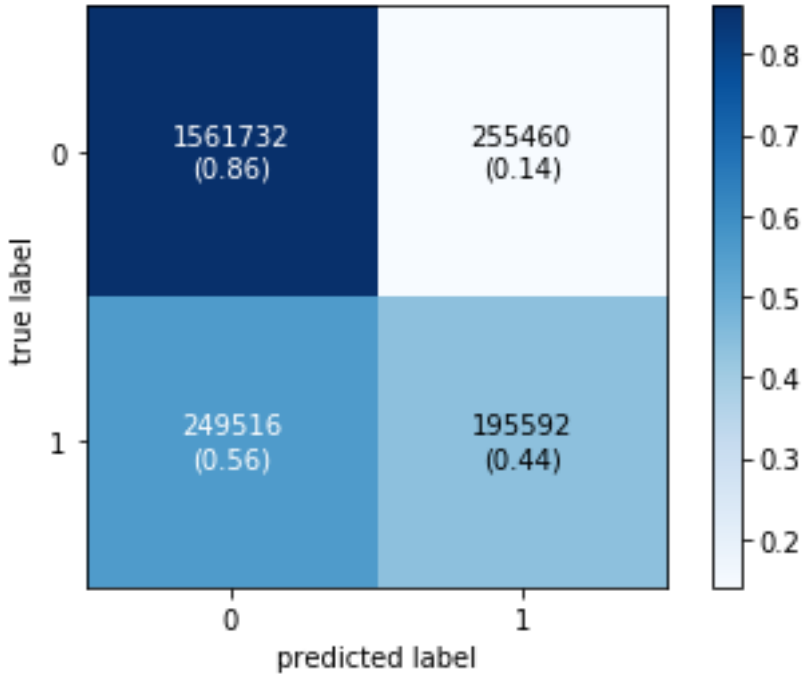
Çizelge 4.1. Birinci Sınıflandırma Uygulamasına Ait Eğitim Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,99	1	1	1	0,99
NB	0,78	0,78	0,78	0,78	0,78
LR	0,90	0,90	0,90	0,88	0,89
DT	0,99	0,99	0,99	0,99	0,99
RF	0,98	0,98	0,96	0,98	0,98

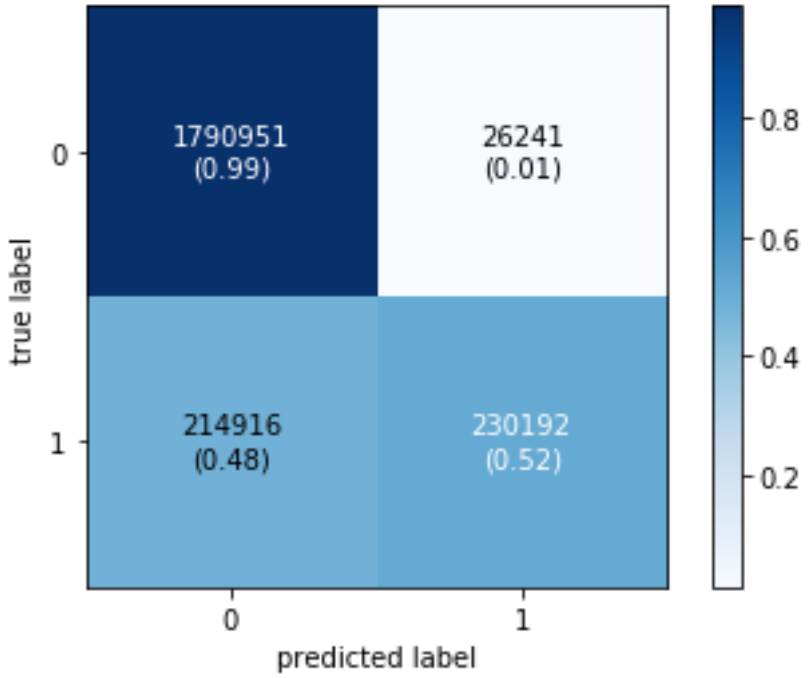
Birinci sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan eğitim sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.1, Şekil 4.2, Şekil 4.3, Şekil 4.4 ve Şekil 4.5'te gösterilmiştir.



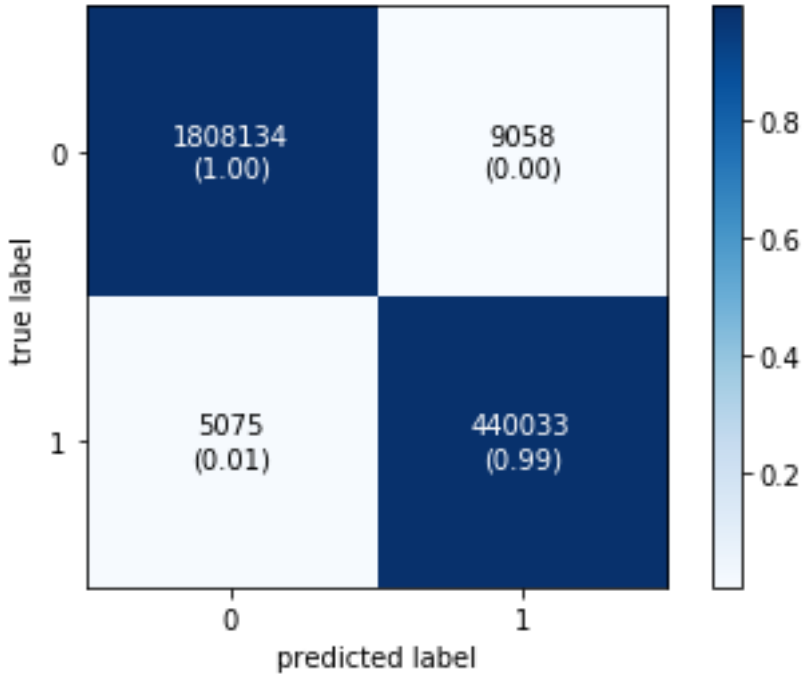
Şekil 4.1. Birinci Deneyde XGB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



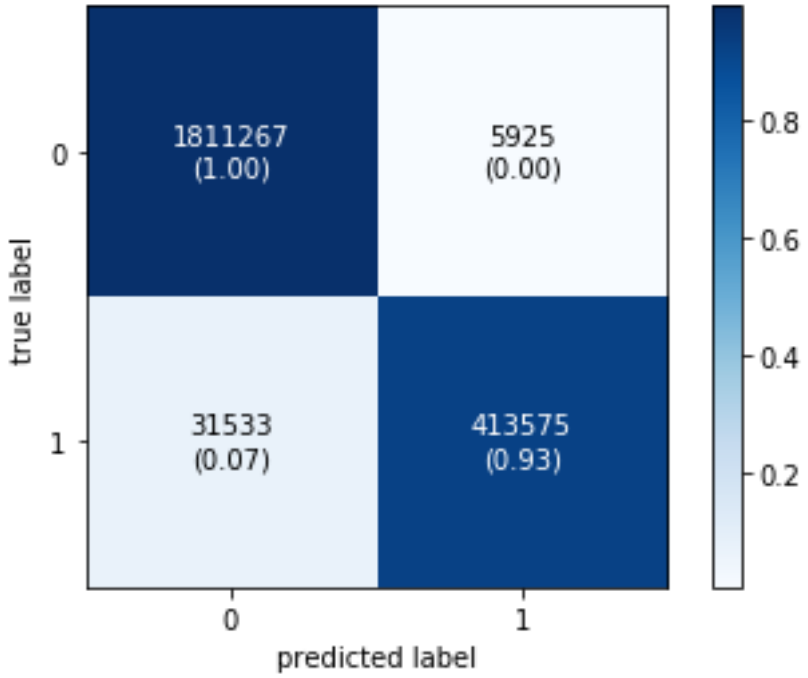
Şekil 4.2. Birinci Deneyde NB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.3. Birinci Deneyde LR Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.4. Birinci Deneyde DT Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



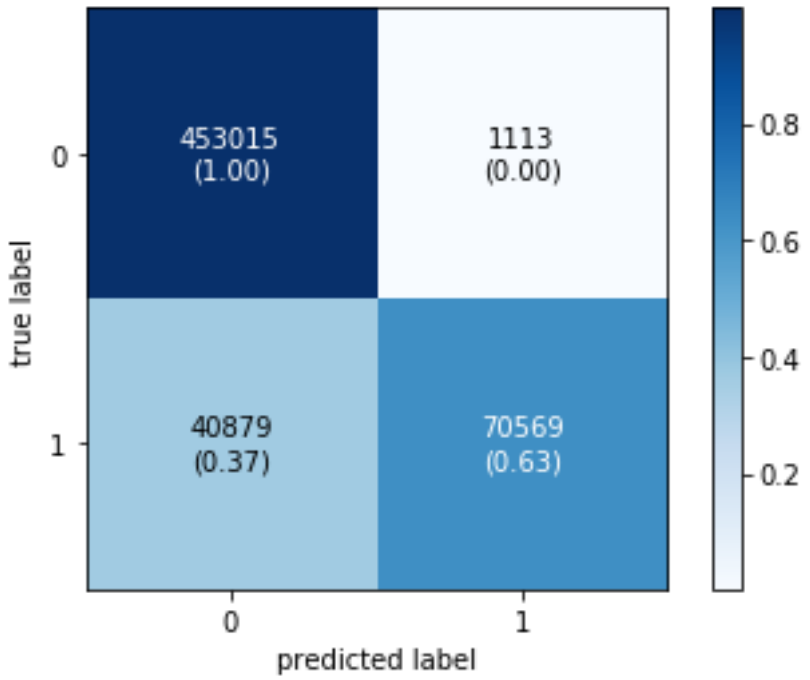
Şekil 4.5. Birinci Deneyde RF Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi

Hibrit yaklaşımla gerçekleşen birinci sınıflandırma uygulamasına ilişkin test sonuçları Çizelge 4.2'de gösterilmektedir.

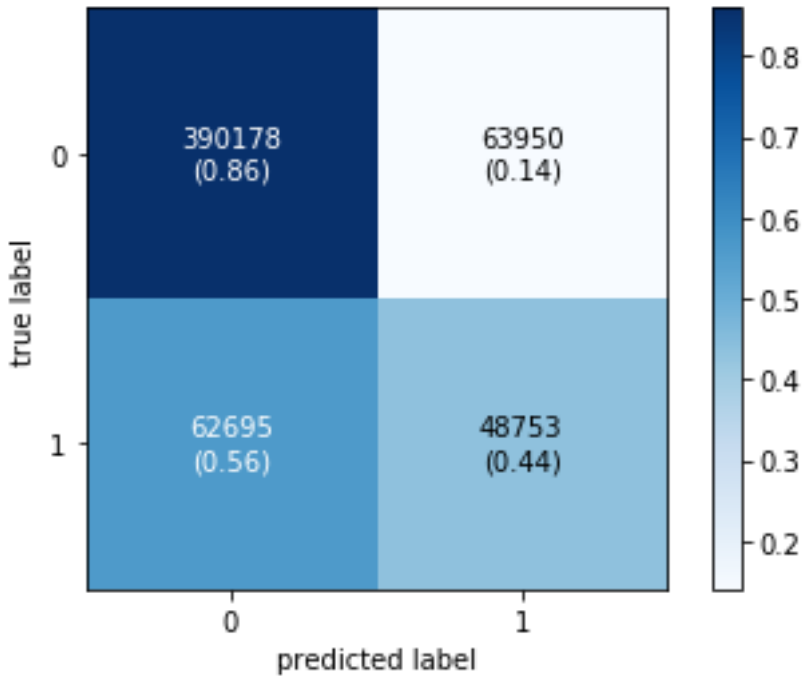
Çizelge 4.2. Birinci Sınıflandırma Uygulamasına Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,93	0,93	0,93	0,92	0,99
NB	0,78	0,78	0,78	0,78	0,78
LR	0,89	0,89	0,89	0,88	0,89
DT	0,84	0,84	0,84	0,81	0,99
RF	0,94	0,93	0,93	0,93	0,98

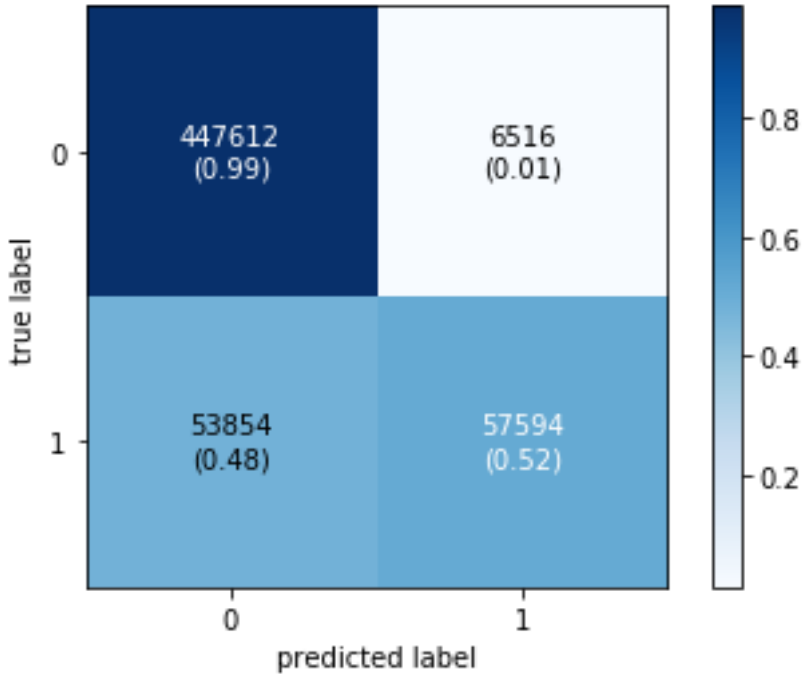
Birinci sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan test sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.6, Şekil 4.7, Şekil 4.8, Şekil 4.9 ve Şekil 4.10'da gösterilmektedir.



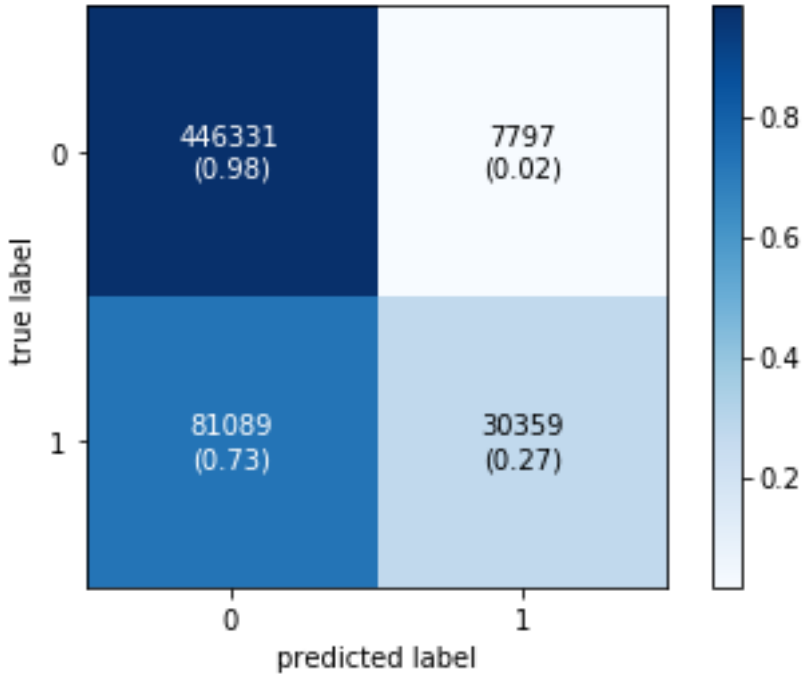
Şekil 4.6. Birinci Deneyde XGB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



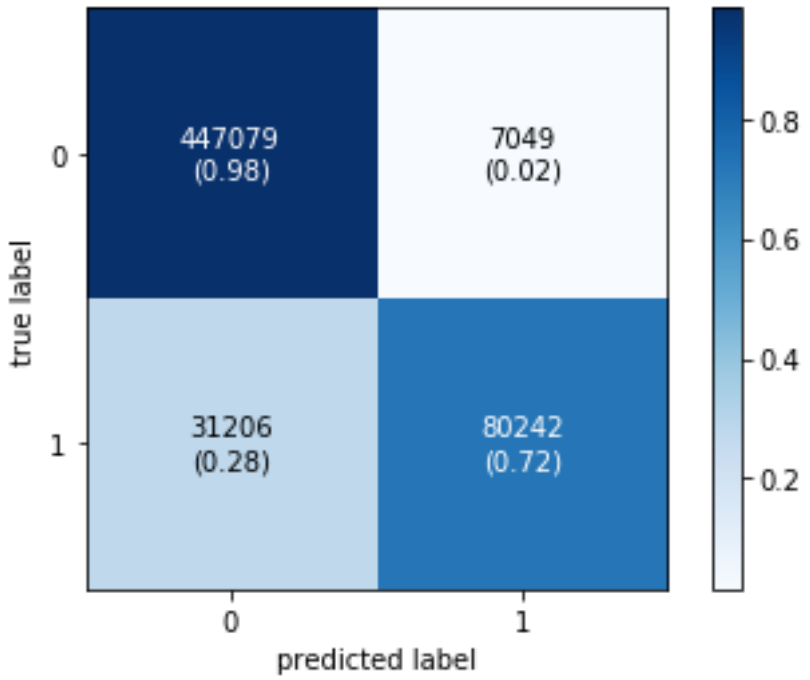
Şekil 4.7. Birinci Deneyde NB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



Şekil 4.8. Birinci Deneyde LR Sınıflayıcısına Ait Test Karmaşıklık Matrisi

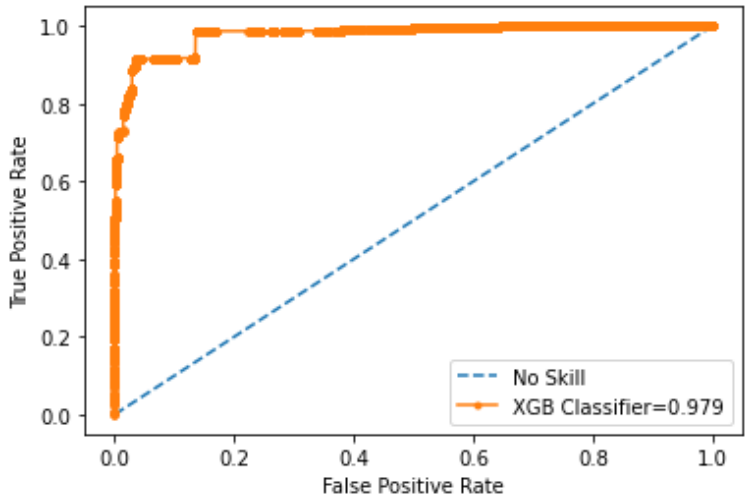


Şekil 4.9. Birinci Deneyde DT Sınıflayıcısına Ait Test Karmaşıklık Matrisi

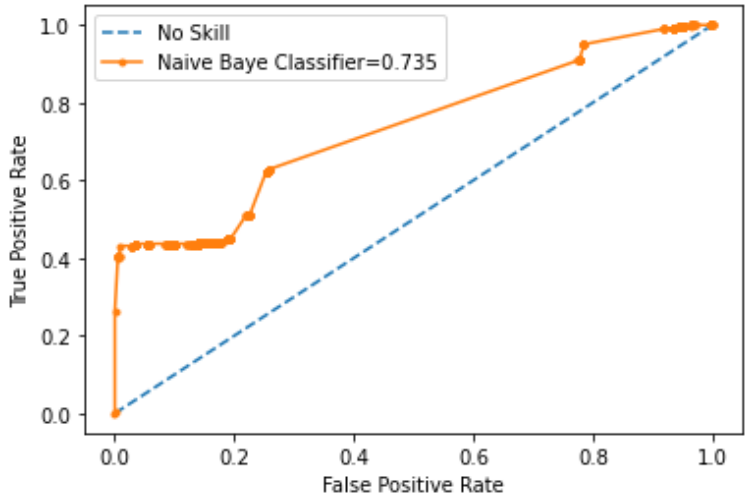


Şekil 4.10. Birinci Deneyde RF Sınıflayıcısına Ait Test Karmaşıklık Matrisi

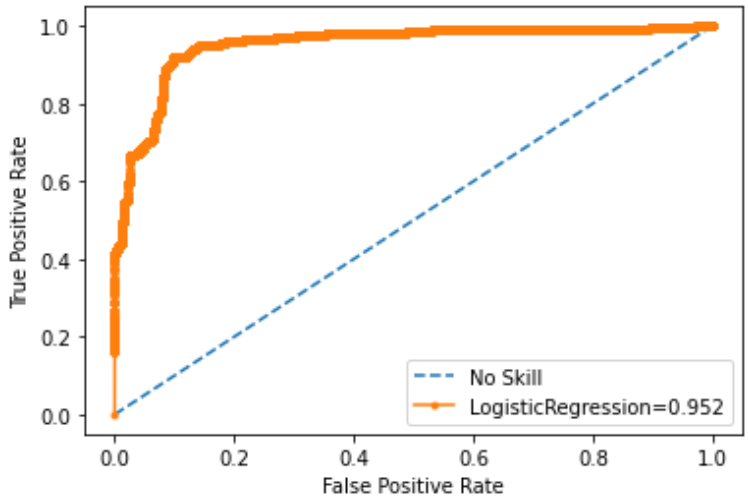
İki aşamalı öznitelik seçiminden sonra farklı sınıflayıcılarla yapılan sınıflandırma işlemlerine ait ROC eğrileri ise Şekil 4.11, Şekil 4.12, Şekil 4.13, Şekil 4.14 ve Şekil 4.15'te gösterilmektedir.



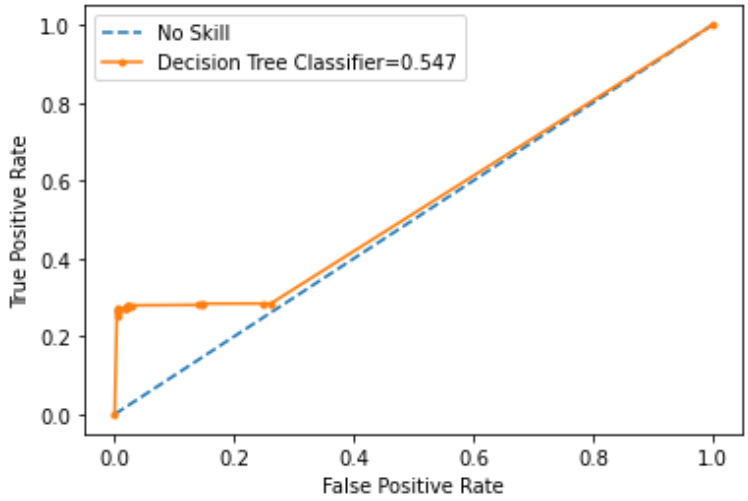
Şekil 4.11. Birinci Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



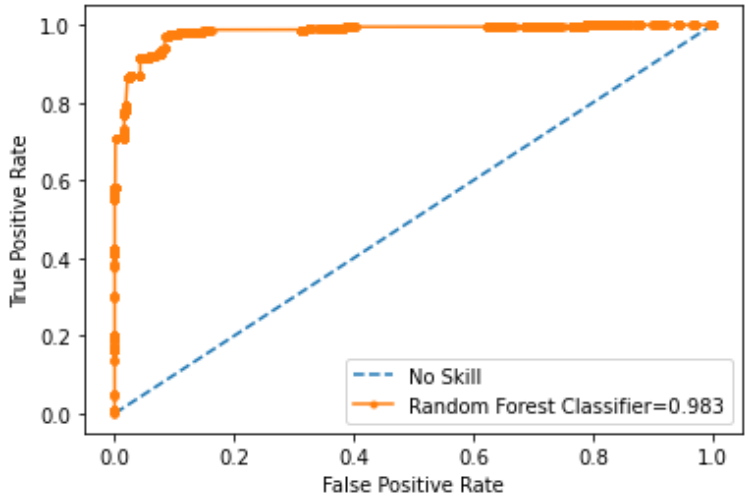
Şekil 4.12. Birinci Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.13. Birinci Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.14. Birinci Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.15. Birinci Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

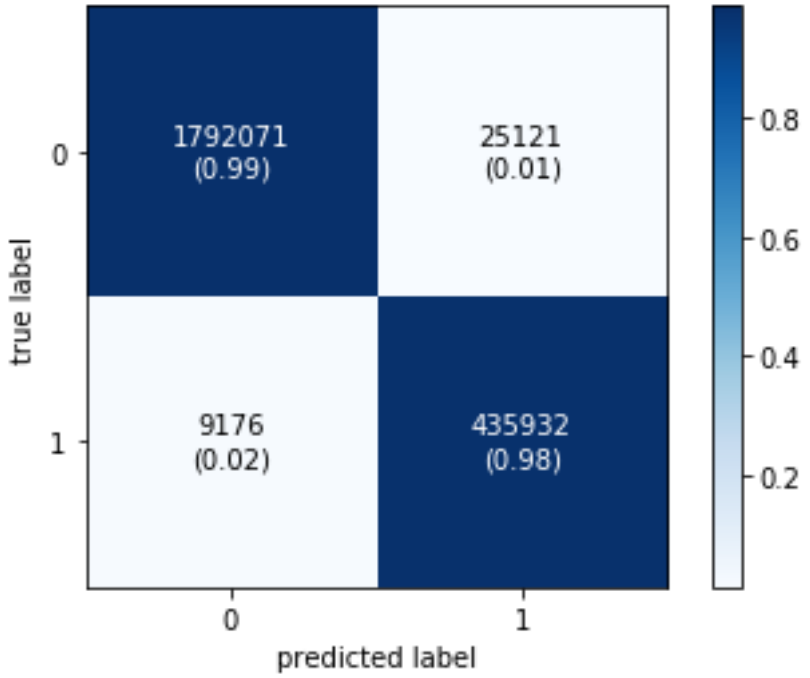
4.2. İkinci Öznitelik Grubu İle Yapılan Sınıflandırma Çalışmaları

Bir diğer deneyde ise manuel olarak seçilen 14 adet özniteliğe (İleri yönde maksimum paket uzunluğu, İleri yönde paketlerin uzunluklarının standart sapması, Paketlerin en uzun varış zamanı, Paketlerin en kısa varış zamanı, Paketlerin ortalama varış zamanı, İleri yönde gönderilen iki paket arasındaki maksimum zaman, İleri yönde gönderilen iki paket arasındaki minimum zaman, İleri yönde gönderilen iki paket arasındaki ortalama zaman, Maksimum paket uzunluğu, Paket ortalama uzunluğu, Bir paketin uzunluk varyansı, İndirme/yükleme oranı, Ortalama paket boyutu, Paketin aktif hale gelmeden önce boşta kaldığı zaman) göre sınıflandırma işlemleri yapılmıştır. Sınıflandırma işlemlerine ait eğitim sonuçları Çizelge 4.3'te gösterilmektedir.

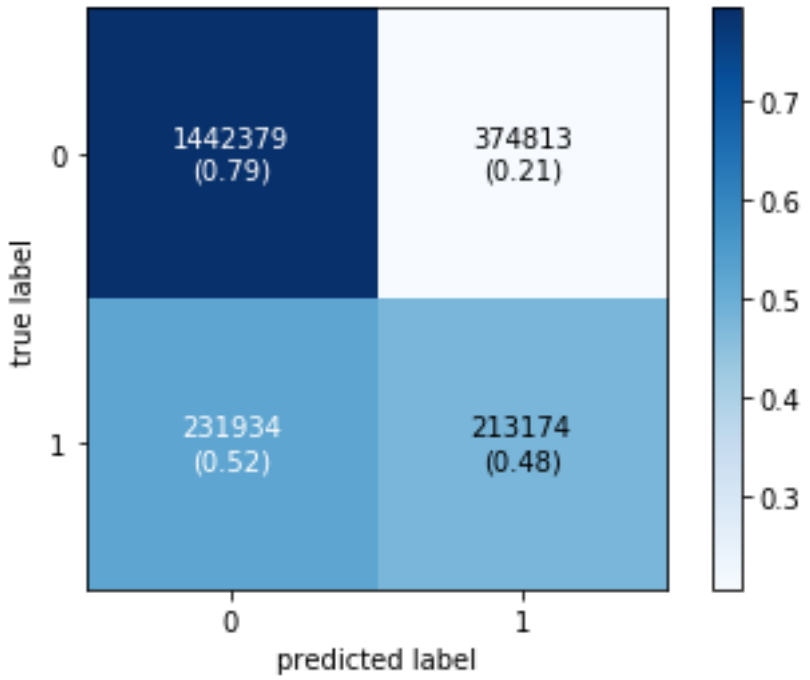
Çizelge 4.3. İkinci Sınıflandırma Uygulamasına Ait Eğitim Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,98	0,97	0,98	0,98	0,98
NB	0,73	0,76	0,73	0,74	0,73
LR	0,89	0,89	0,89	0,87	0,89
DT	0,98	0,90	0,98	0,98	0,98
RF	0,96	0,96	0,96	0,96	0,96

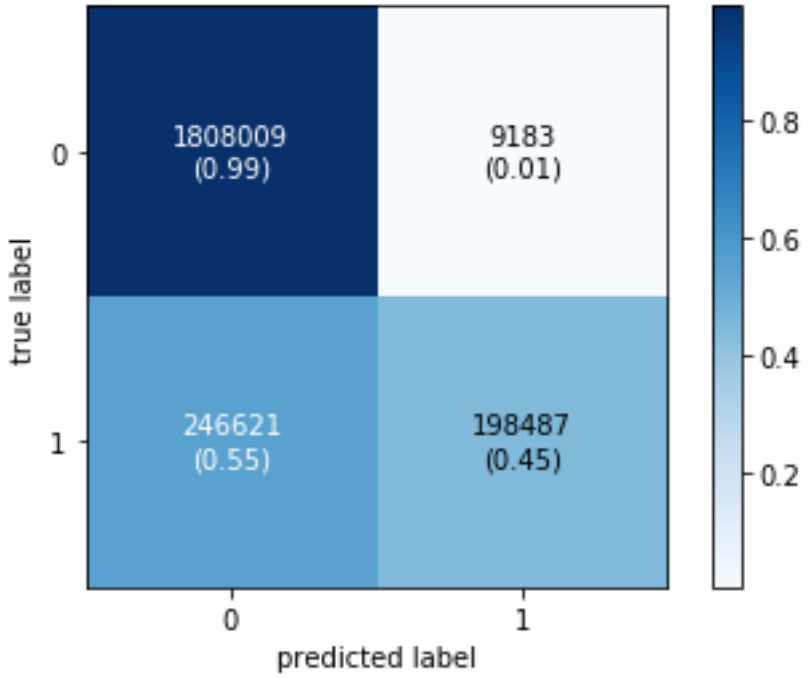
İkinci sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan eğitim sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.16, Şekil 4.17, Şekil 4.18, Şekil 4.19 ve Şekil 4.20'de gösterilmektedir.



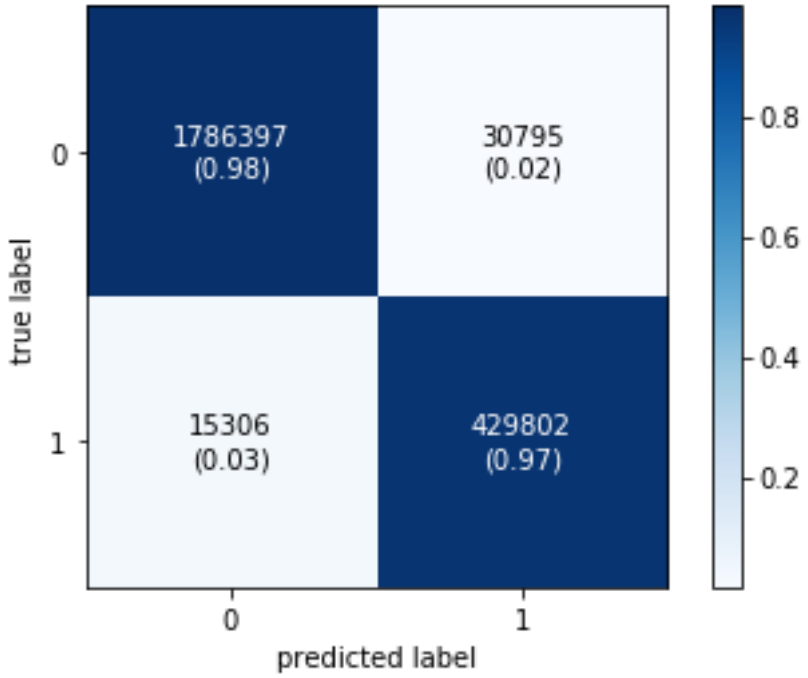
Şekil 4.16. İkinci Deneyde XGB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



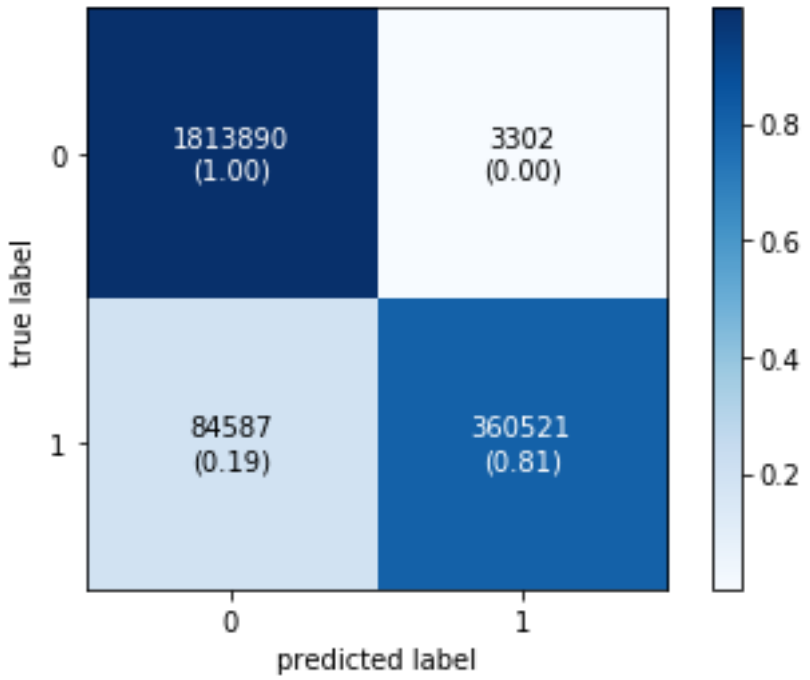
Şekil 4.17. İkinci Deneyde NB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.18. İkinci Deneyde LR Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.19. İkinci Deneyde DT Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



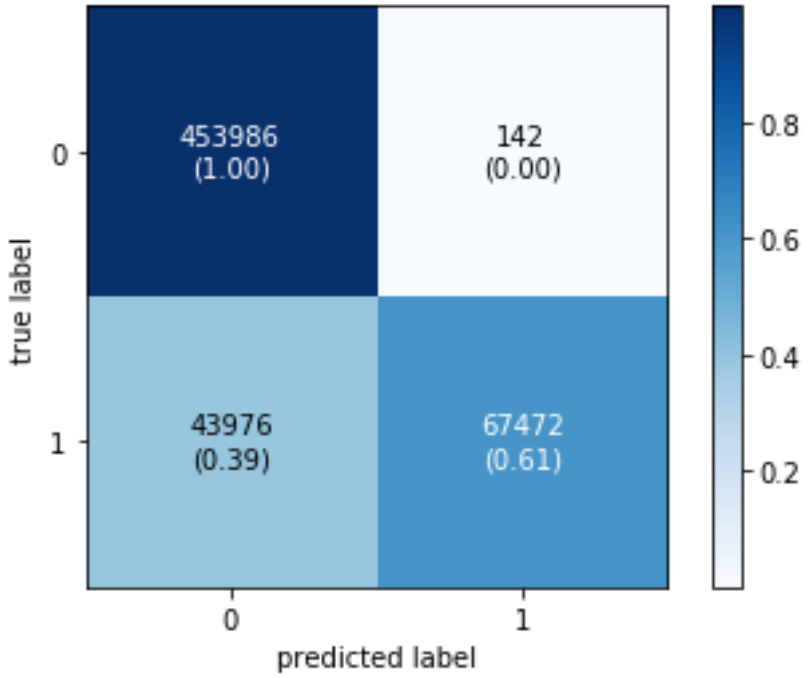
Şekil 4.20. İkinci Deneyde RF Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi

İkinci deneyde yapılan test sınıflandırmasına ilişkin sonuçlar ise Çizelge 4.4'te verilmiştir.

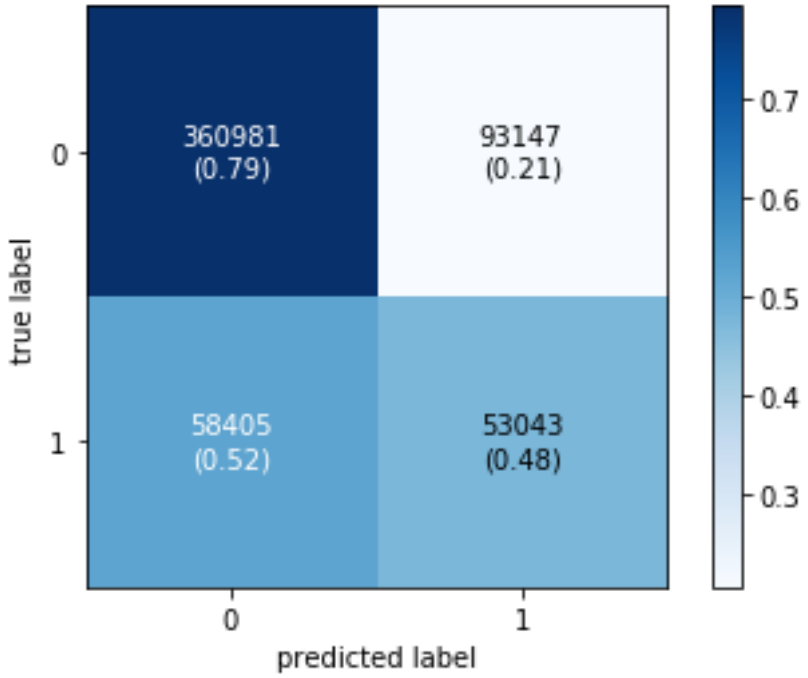
Çizelge 4.4. İkinci Sınıflandırma Uygulamasına Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,92	0,93	0,92	0,91	0,98
NB	0,73	0,76	0,73	0,74	0,73
LR	0,88	0,89	0,89	0,87	0,88
DT	0,89	0,90	0,89	0,88	0,98
RF	0,92	0,93	0,92	0,92	0,96

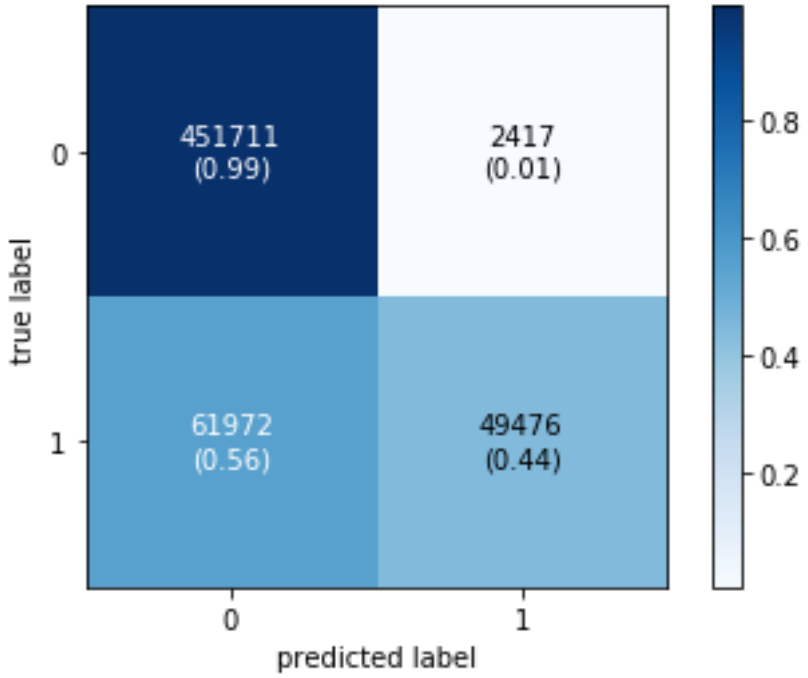
İkinci sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan test sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.21, Şekil 4.22, Şekil 4.23, Şekil 4.24 ve Şekil 4.25'te gösterilmektedir.



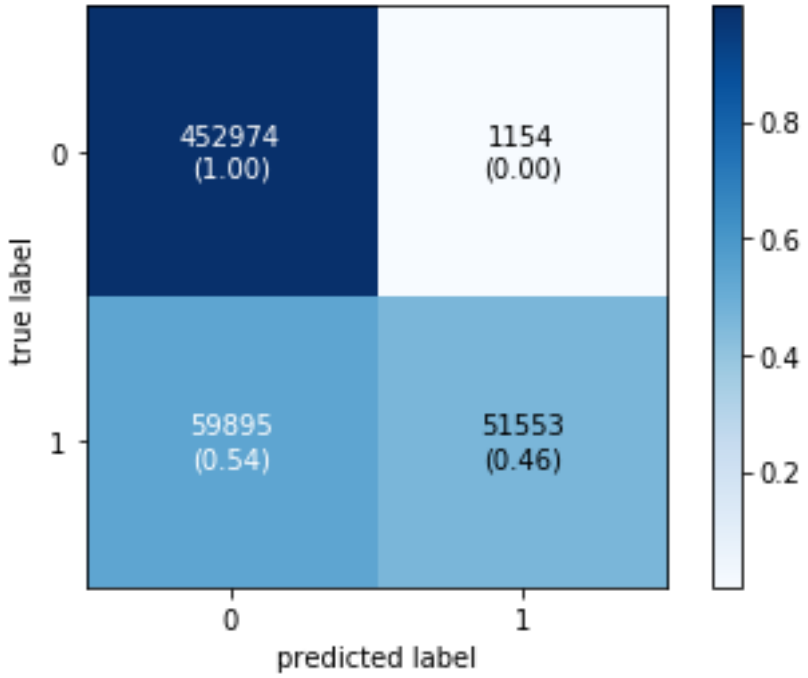
Şekil 4.21. İkinci Deneyde XGB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



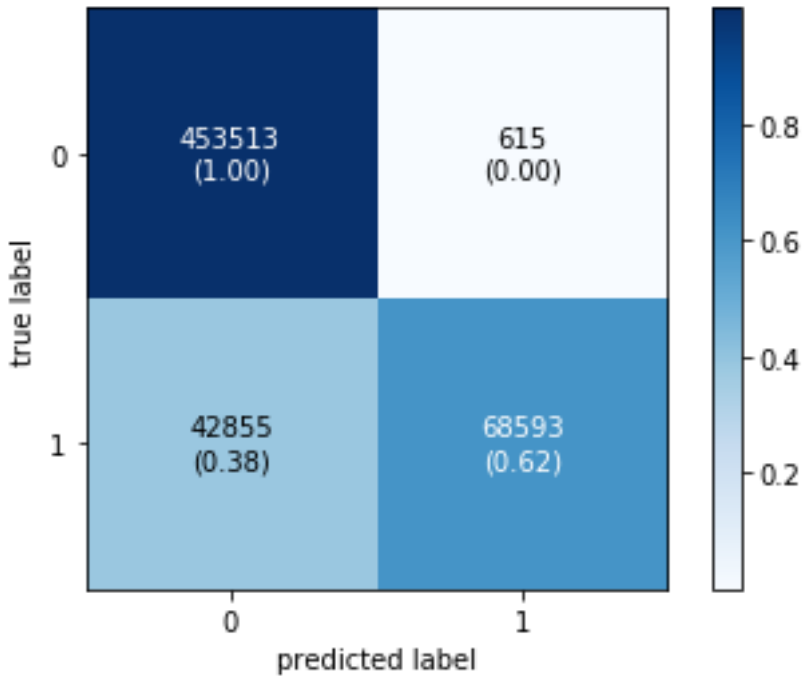
Şekil 4.22. İkinci Deneyde NB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



Şekil 4.23. İkinci Deneyde LR Sınıflayıcısına Ait Test Karmaşıklık Matrisi

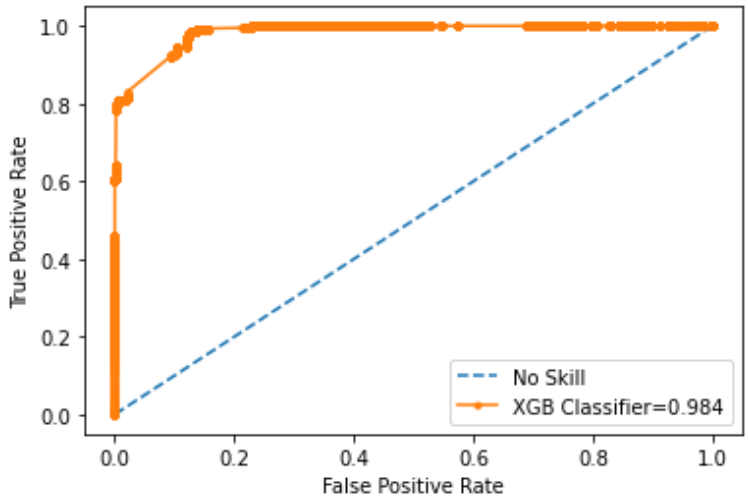


Şekil 4.24. İkinci Deneyde DT Sınıflayıcısına Ait Test Karmaşıklık Matrisi

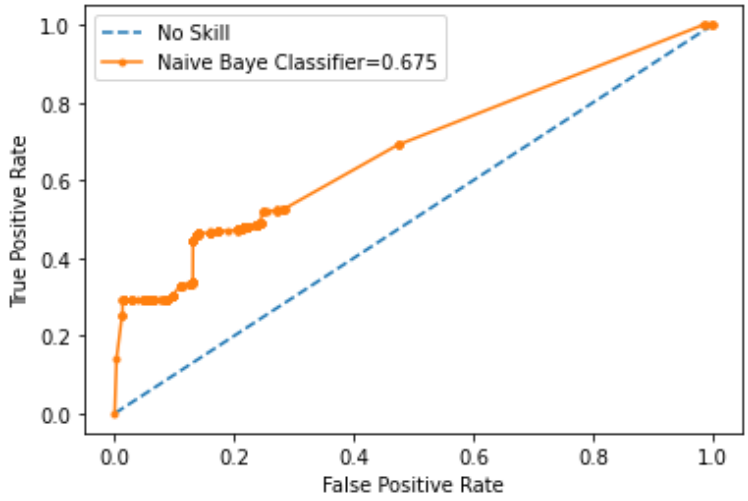


Şekil 4.25. İkinci Deneyde RF Sınıflayıcısına Ait Test Karmaşıklık Matrisi

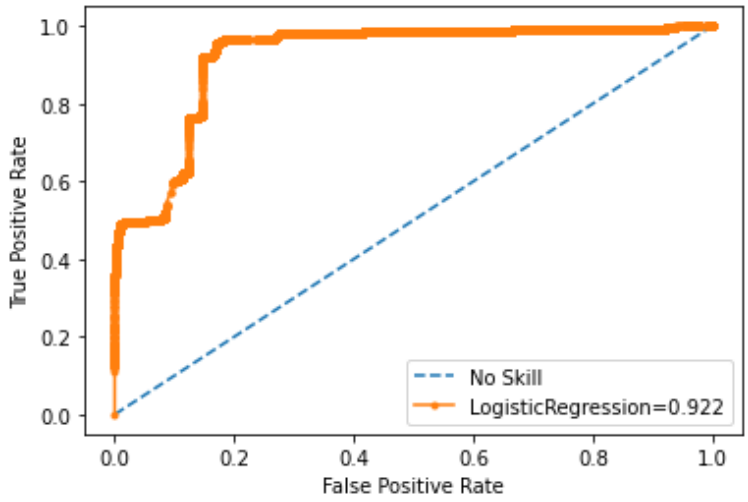
Manuel olarak seçilen 14 özniteliğin farklı sınıflayıcılarla sınıflandırma işlemlerine ait ROC eğrileri Şekil 4.26, Şekil 4.27, Şekil 4.28, Şekil 4.29 ve Şekil 4.30'da gösterilmektedir.



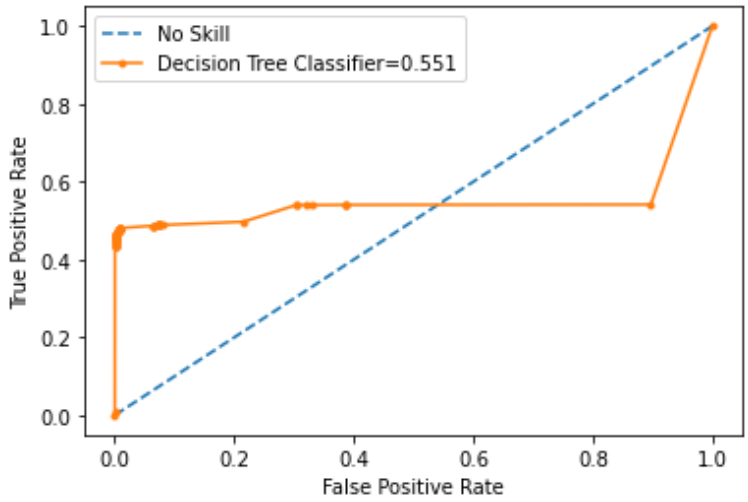
Şekil 4.26. İkinci Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



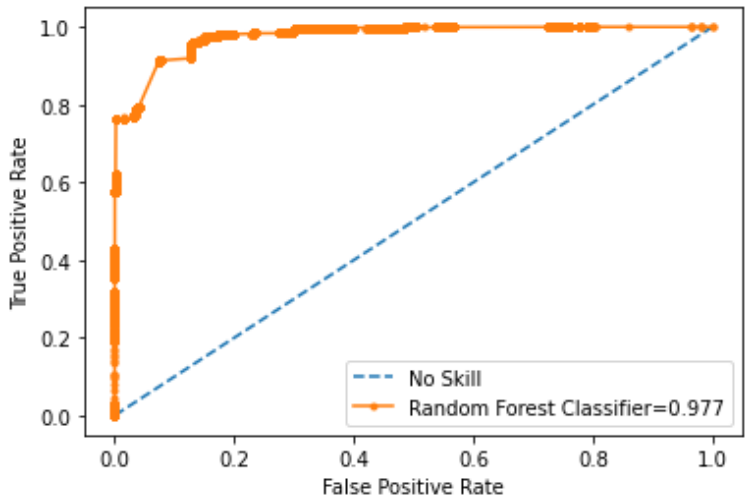
Şekil 4.27. İkinci Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.28. İkinci Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.29. İkinci Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.30. İkinci Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

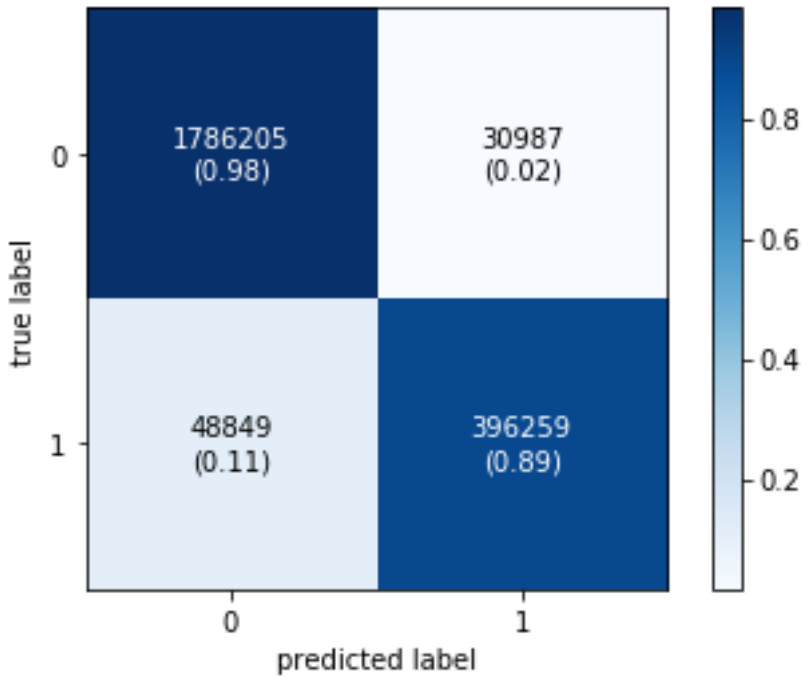
4.3. Üçüncü Öznitelik Grubu İle Yapılan Sınıflandırma Çalışmaları

Son deneyde ise yine manuel olarak daha az sayıda öznitelik seçilmiştir. Seçilen 8 adet özniteliğe (Akış süresi mikrosaniye, Geri yöndeki paketlerin maksimum uzunluğu, Geri yöndeki paketlerin minimum uzunluğu, Geri yöndeki paketlerin ortalama uzunluğu, Minimum paket uzunluğu, PUSH bulunan paket sayısı, URG içeren paket sayısı, Geri yönde gözlenen ortalama segment boyutu) göre yapılan sınıflandırma işleminin eğitim sonuçları Çizelge 4.5'te verilmiştir.

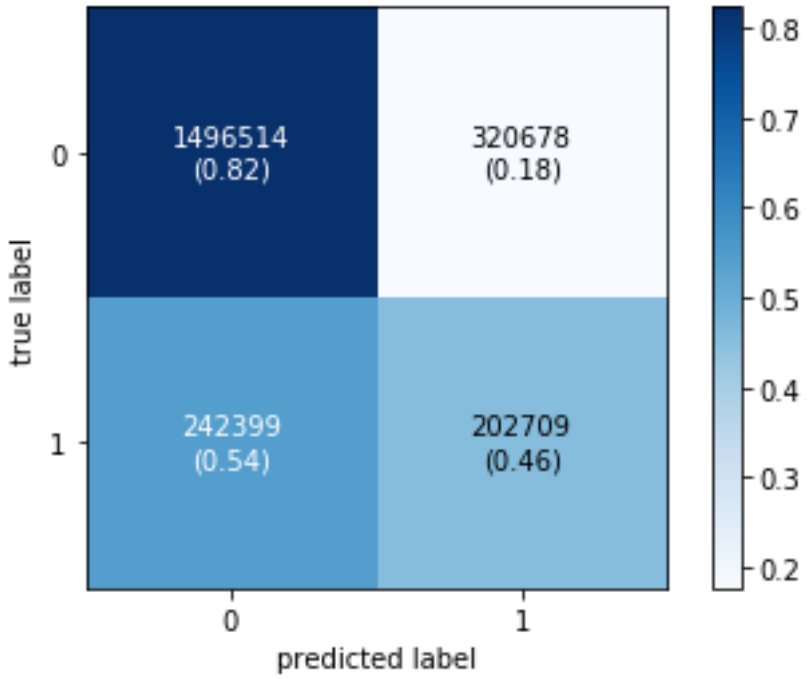
Çizelge 4.5. Üçüncü Sınıflandırma Uygulamasına Ait Eğitim Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,96	0,96	0,96	0,96	0,96
NB	0,75	0,77	0,75	0,76	0,75
LR	0,88	0,88	0,88	0,86	0,88
DT	0,96	0,95	0,96	0,95	0,96
RF	0,93	0,93	0,93	0,93	0,93

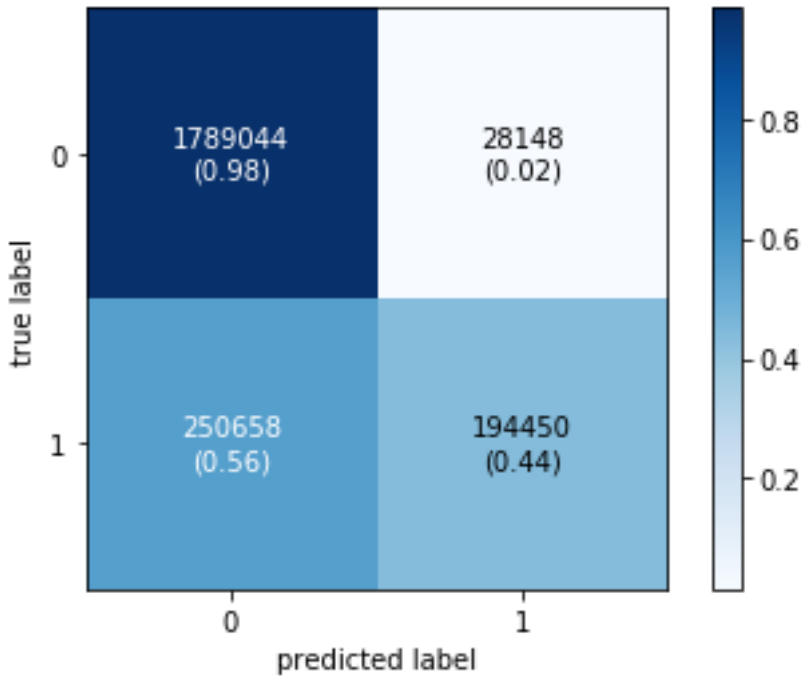
Üçüncü sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan eğitim sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.31, Şekil 4.32, Şekil 4.33, Şekil 4.34 ve Şekil 4.35'te gösterilmektedir.



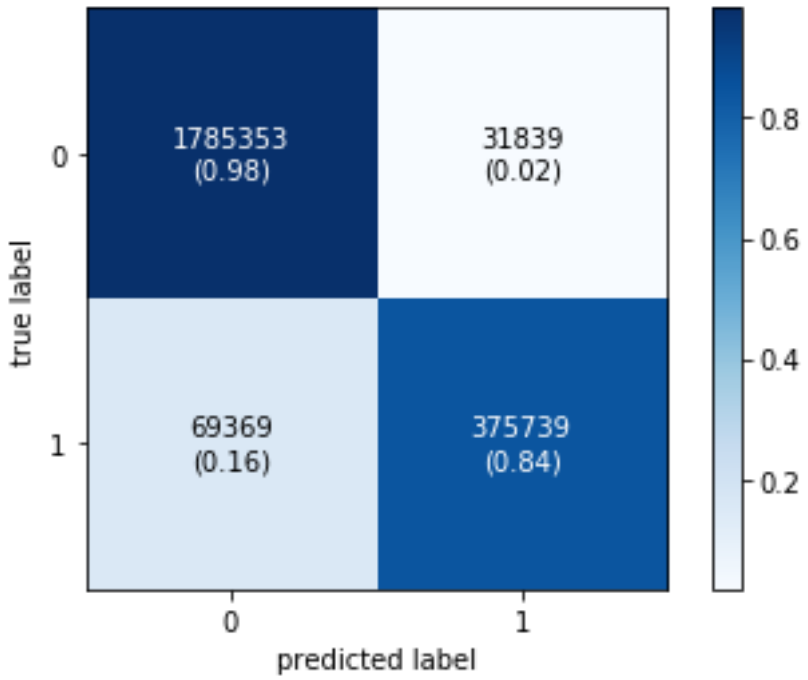
Şekil 4.31. Üçüncü Deneyde XGB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



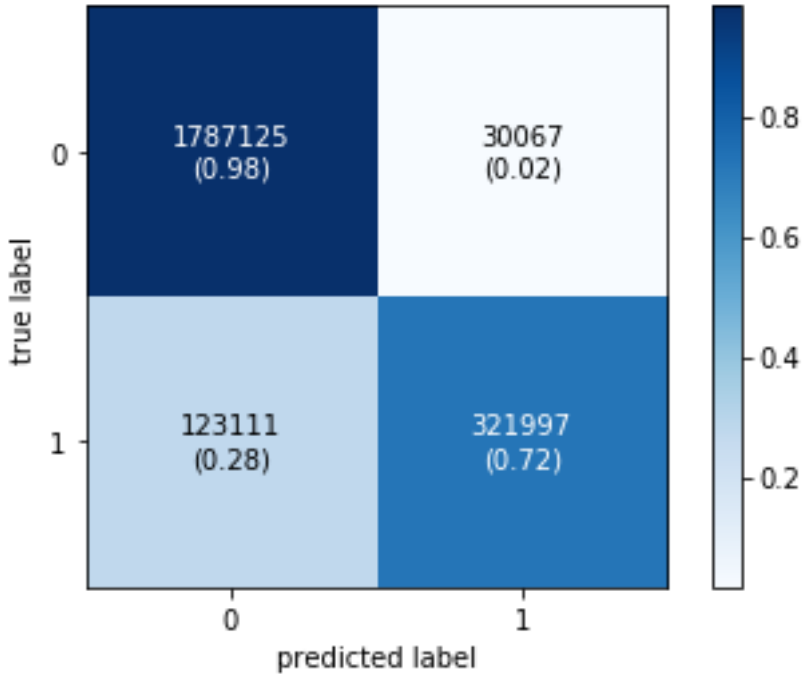
Şekil 4.32. Üçüncü Deneyde NB Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.33. Üçüncü Deneyde LR Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



Şekil 4.34. Üçüncü Deneyde DT Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi



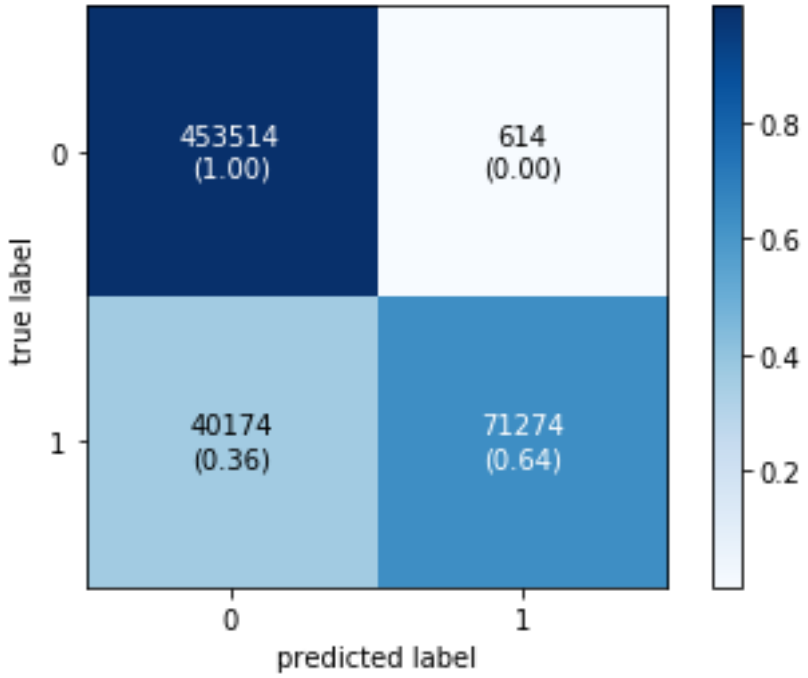
Şekil 4.35. Üçüncü Deneyde RF Sınıflayıcısına Ait Eğitim Karmaşıklık Matrisi

Çizelge 4.6'da ise üçüncü sınıflandırma çalışmasında elde edilen sonuçlar gösterilmektedir.

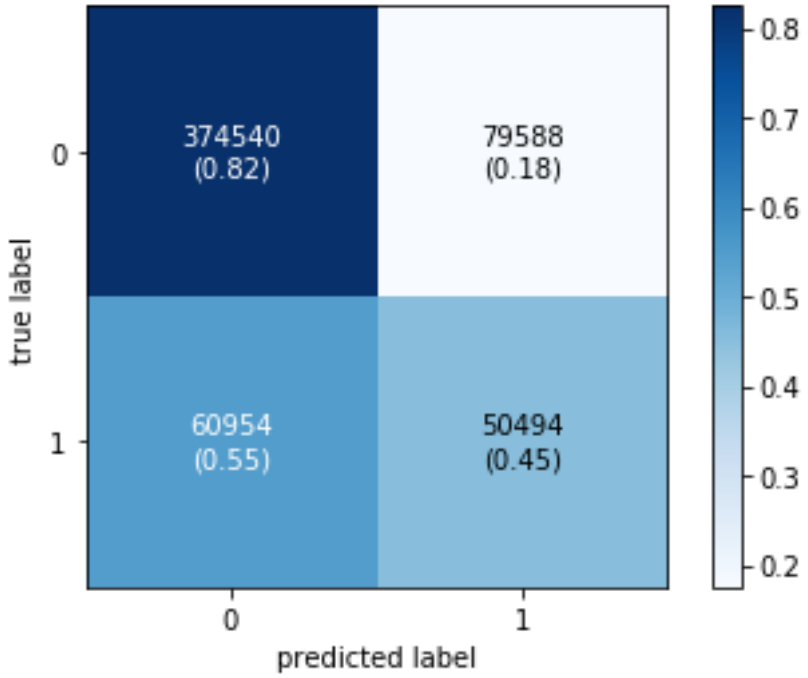
Çizelge 4.6. Üçüncü Sınıflandırma Uygulamasına Ait Test Sonuçları

Sınıflayıcı	Doğruluk (Accuracy Score)	Kesinlik (Precision Score)	Duyarlılık (Recall Score)	F1 Score	Çapraz Doğrulama
XGB	0,93	0,93	0,93	0,92	0,96
NB	0,75	0,77	0,75	0,76	0,75
LR	0,88	0,88	0,88	0,86	0,87
DT	0,94	0,94	0,94	0,94	0,95
RF	0,93	0,93	0,93	0,93	0,93

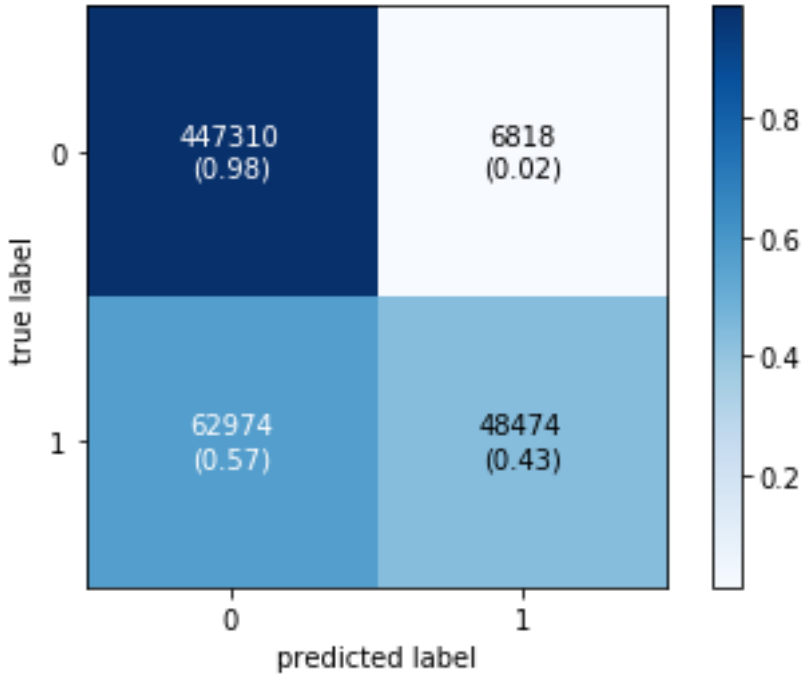
Üçüncü sınıflandırma çalışmasında, her bir sınıflandırıcıya göre yapılan test sonuçlarına göre oluşturulan karmaşıklık matrisleri Şekil 4.36, Şekil 4.37, Şekil 4.38, Şekil 4.39 ve Şekil 4.40'ta gösterilmektedir.



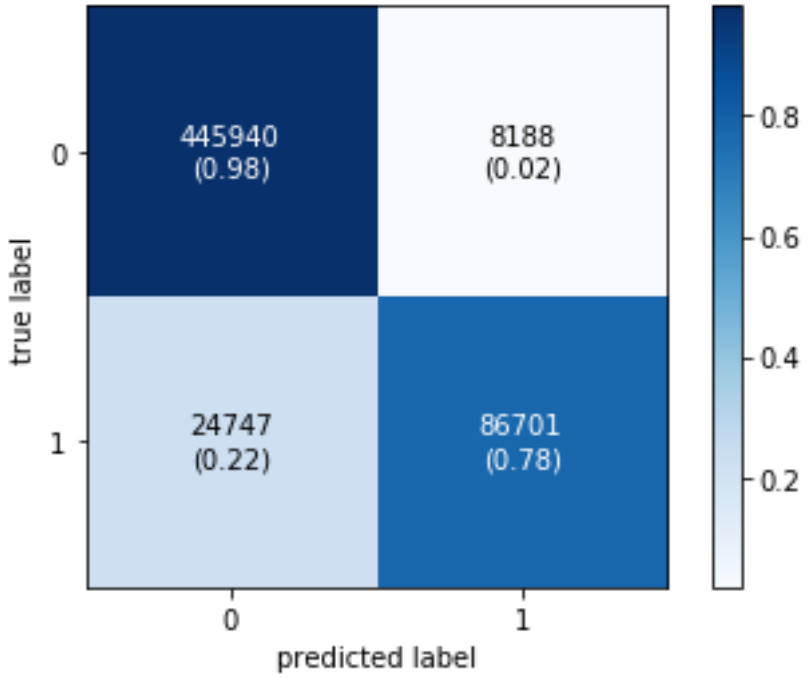
Şekil 4.36. Üçüncü Deneyde XGB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



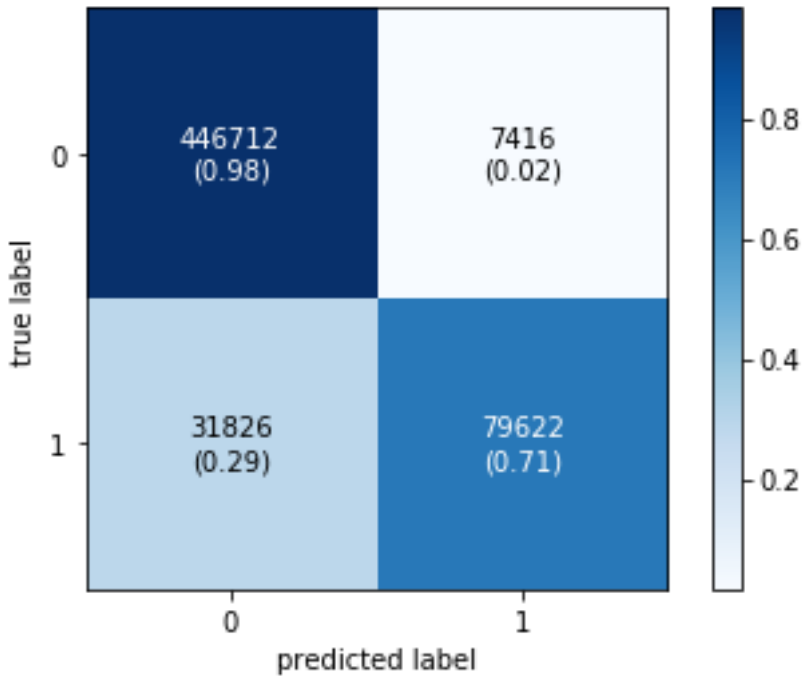
Şekil 4.37. Üçüncü Deneyde NB Sınıflayıcısına Ait Test Karmaşıklık Matrisi



Şekil 4.38. Üçüncü Deneyde LR Sınıflayıcısına Ait Test Karmaşıklık Matrisi

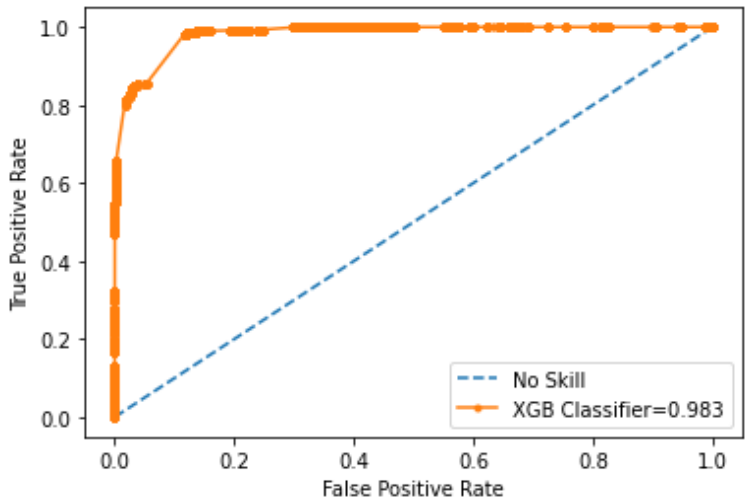


Şekil 4.39. Üçüncü Deneyde DT Sınıflayıcısına Ait Test Karmaşıklık Matrisi

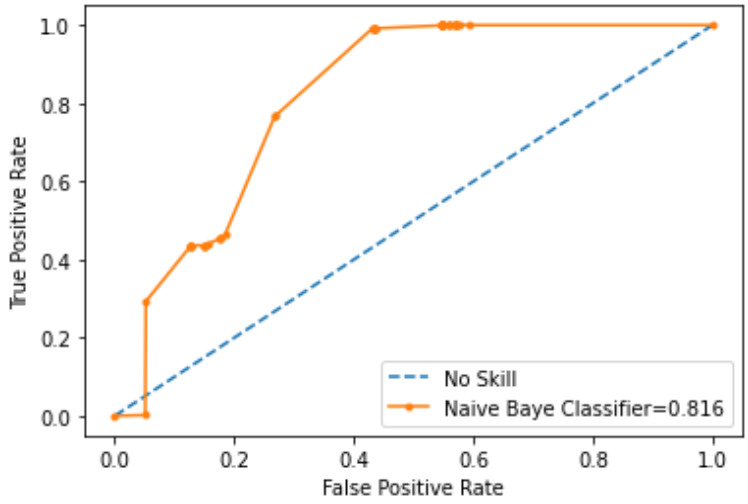


Şekil 4.40. Üçüncü Deneyde RF Sınıflayıcısına Ait Test Karmaşıklık Matrisi

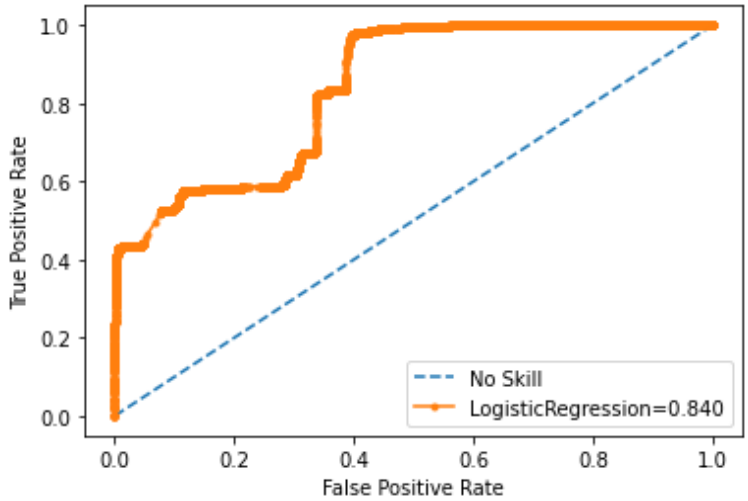
Manuel olarak seçilen 8 özniteliğin farklı sınıflayıcılarla sınıflandırma işlemlerine ait ROC eğrileri Şekil 4.41, Şekil 4.42, Şekil 4.43, Şekil 4.44 ve Şekil 4.45'te gösterilmektedir.



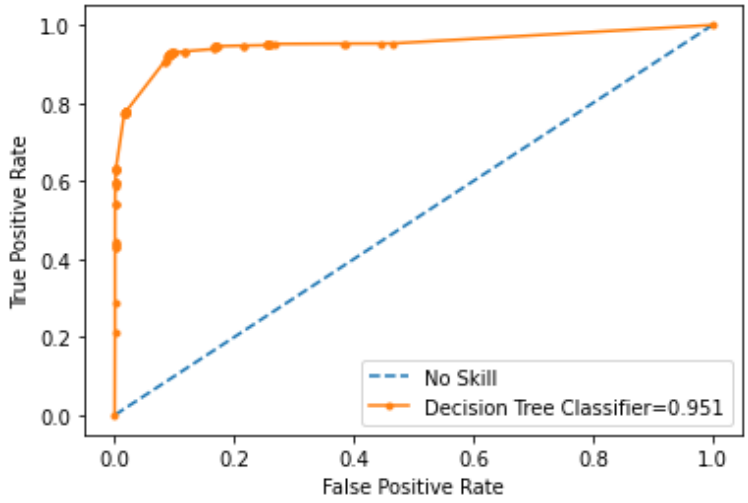
Şekil 4.41. Üçüncü Deneyde XGB Sınıflayıcısına Ait ROC Eğrisi



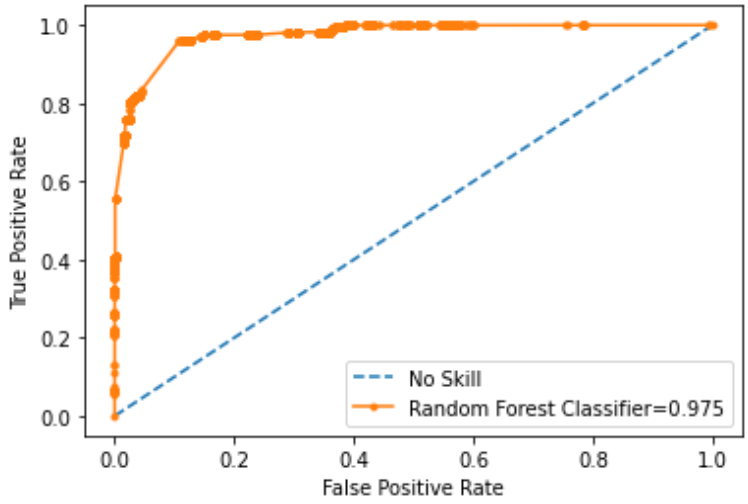
Şekil 4.42. Üçüncü Deneyde NB Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.43. Üçüncü Deneyde LR Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.44. Üçüncü Deneyde DT Sınıflayıcısına Ait ROC Eğrisi



Şekil 4.45. Üçüncü Deneyde RF Sınıflayıcısına Ait ROC Eğrisi

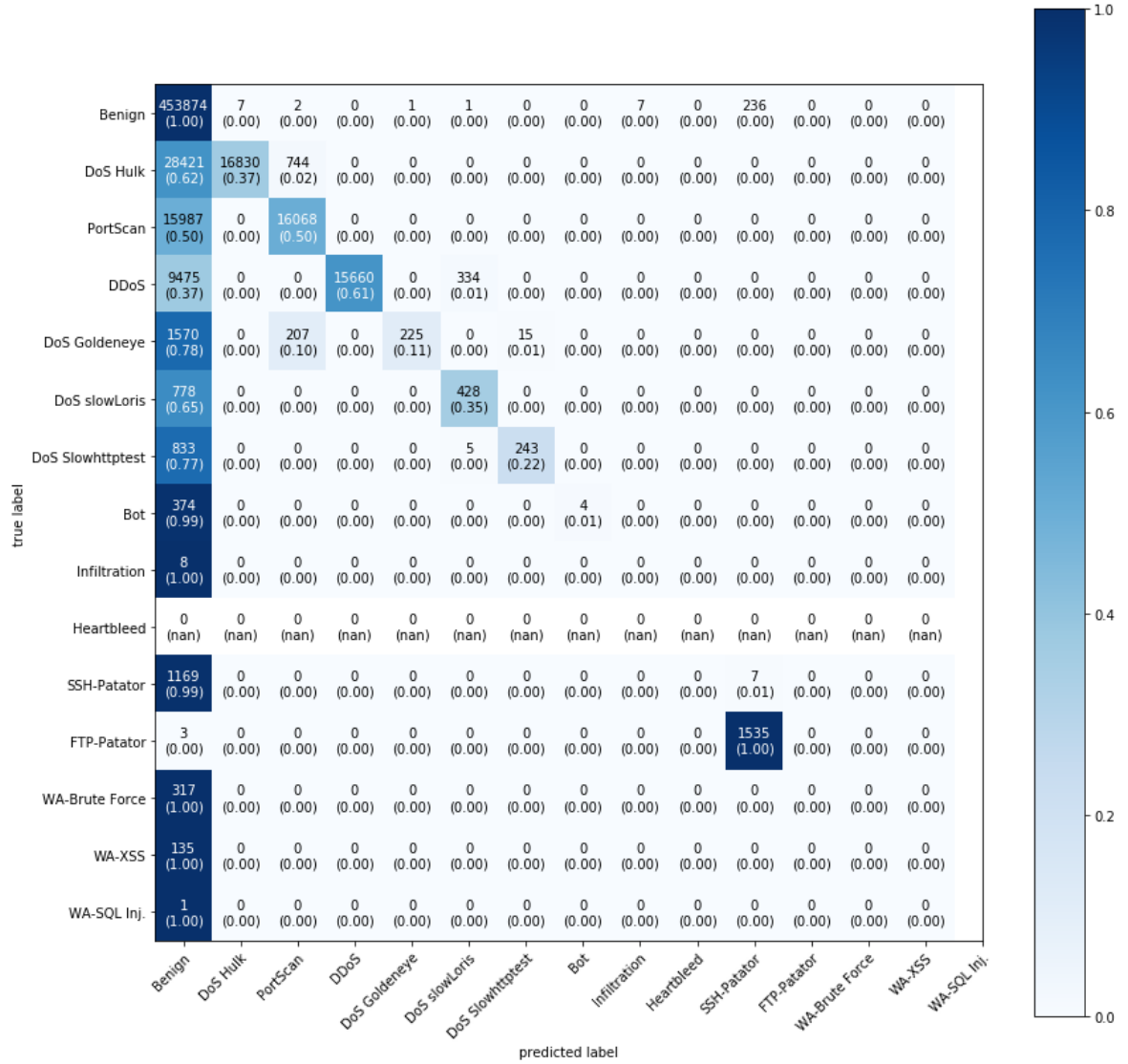
4.4. Çoklu Sınıflandırma

Çalışmanın son bölümünde ise hibrit özellik seçiminden sonra ikili sınıflandırma yerine CICIDS 2017 veri setinde bulunan toplam 15 adet hedef etiketinin tamamının yer aldığı sınıflandırma deneyi yapılmış. Bu son deneyde sınıflayıcı olarak XGB algoritması kullanılmıştır. Deneyde sonucunda Doğruluk (A) metriğinde genel sonuç 0,89 olarak ölçülmüştür. Kesinlik, Duyarlılık ve F1 Skor metriklerinde her sınıfa ait elde edilen detaylı sonuçlar Çizelge 4.7'de sunulmuştur.

Çizelge 4.7. Çoklu Sınıflandırma Sonuçları

Sınıf Etiketi	Kesinlik (P)	Duyarlılık (R)	F1 Skor	Örnek Sayısı
Normal	0,88	1,00	0,94	454128
Dos Hulk	1,00	0,37	0,54	45995
PortScan	0,94	0,50	0,65	32055
DDoS	1,00	0,61	0,76	25541
DoS GoldenEye	1,00	0,11	0,20	2017
DoS SlowLoris	0,56	0,35	0,43	1206
DoS Slowhttptest	0,94	0,22	0,36	1081
Bot	1,00	0,01	0,02	378
Infiltration	0,00	0,00	0,00	8
Heartbleed	0,00	0,00	0,00	0
SSH-Patator	0,00	0,00	0,00	1176
FTP-Patator	0,86	1,00	0,93	1538
Web Attack - Brute Force	0,00	0,00	0,00	317
Web Attack - XSS	0,00	0,00	0,00	135
Web Attack - Sql Injection	0,00	0,00	0,00	1

Bu deneye ait olan karmaşıklık matrisi de Şekil 4.46’da gösterilmektedir.



Şekil 4.46. Çoklu Sınıflandırma Karmaşıklık Matrisi

4.5. Çalışmanın Literatürdeki Benzer Çalışmalarla Kıyaslanması

Literatür incelendiğinde saldırı tespiti konusunda CICIDS 2017 veri seti üzerinde yapılan çalışmalarda öznitelik seçim işleminin sistemin doğruluğu ve yanıt süresi açısından önemli olduğu görülmüştür. Çizelge 4.8'de daha önce yapılan bazı çalışmalarda öznitelik seçimi ve sınıflandırma aşamalarında kullanılan algoritmalarla elde edilen sonuçlara ilişkin kısa bilgiler verilmektedir.

Çizelge 4.8. Literatür Özeti

Çalışma ve Yıl	Öznitelik Seçim Teknikleri	Sınıflandırma Teknikleri	Sonuç
Kumar ve diğerleri, 2020	RF	ID3(DT), MLP, NB, Topluluk Öğrenmesi	Doğruluk, Kesinlik, Duyarlılık ve F1 metriklerinde 0,95 ve üzeri sonuçlar alınan ve bir tür karar ağacı algoritması olan ID3 başarılı olmuştur.
Zhou ve diğerleri, 2020	Korelasyon Tabanlı Öznitelik Seçimi (CFS) ve Yarasa Algoritması (BA)	C4.5, RF, Cezalandırılan Özellikler ile Karar Ağacı algoritmalarının birleşimi ile oluşturulan Topluluk Öğrenmesi	Oluşturulan Topluluk Öğrenmesi metodu ile Doğruluk, Kesinlik ve F metriklerinde 0,99'luk değerlere ulaşılmıştır.
Shoukat ve diğerleri, 2020	Sarmalayıcı Öznitelik Seçimi	J48, NB	J48 algoritması ile Doğruluk Kesinlik ve Duyarlılık metriklerinde 0,999 ve F1 metriğinde 0,996'lık değerler elde edilmiştir. NB ile yapılan sınıflandırma bu sonuçların oldukça altında kalmıştır.
Fernandez ve Xu, 2019	Öznitelik seçimi yok	7 katmanlı DNN	IP adresleri dahil edildiğinde TPR (True Positive Rate): 0,99, IP adresleri dahil edilmediğinde 0,96
Farahani, 2020	Çapraz Korelasyon Tabanlı Öznitelik Seçimi (CCFS)	SVM, NB, DT, KNN	DT algoritması Doğruluk:97,91 – Kesinlik:99,42 – Duyarlılık: 99,07 ve F1 Skor:99,24
Yu ve diğerleri, 2021	Hiyerarşik Paket Byte Tabanlı CNN Öznitelik Seçimi	Hiyerarşik Paket Byte Tabanlı CNN Sınıflandırma	Doğruluk:0,99 – Kesinlik:0,98 – Duyarlılık:0,98 ve F1 Skor:0,98
Kurniabudi ve diğerleri, 2020	Sınıf etiketlerinin azaltılması ve Bilgi Kazanımı	RF, NB, Bayes Net, Random Tree, J48	22 özellik ile RF algoritması Doğruluk:0,9986; 52 özellik ile J48 algoritması Doğruluk:0,9987
Li ve diğerleri, 2021	Sınıf etiketlerinin azaltılması ve LNNLS-KH	KNN	Normal sınıfı doğruluğu: 0,94; DoS sınıfı doğruluğu :0,94; DDoS sınıfı doğruluğu: 0,95; PortScan sınıfı doğruluğu:0,97, Web Attack sınıfı doğruluğu: 0,96

Çizelge 4.8'de belirtilen önceki çalışmalarda görüldüğü üzere genellikle Rastgele Orman ve Karar Ağaçları algoritmalarının saldırı tespiti ve sınıflandırılmasında başarılı olduğu görülmektedir. Ancak sınıflandırma aşamasından önce öznitelik seçimi yapılmadan, veri setindeki tüm özelliklerin kullanıldığı çalışmalarda başarı oranı yüksek olmasına rağmen sistemin cevap süresinin uzun olduğu ve donanımsal gereksinimlerin de buna paralel olarak arttığı anlaşılmaktadır. Buna karşın farklı öznitelik seçimi yöntemlerinin saldırı tespit sistemlerinin uygulanabilirliği açısından olumlu etkiler yaptığı, öznitelik seçimi kullanmadan yapılan çalışmalarda elde edilen başarı oranlarına yakın elde edilen sonuçlara sistemin daha kısa süreli eğitim aşamalarıyla ulaştığı görülmüştür. Ayrıca CICIDS 2017 veri setinin hedef etiketlere göre örnek sayıları açısından dengesiz olduğu, birçok çalışmada bu dengesizliğin hedef etiketlerin ortak gruplarda toplanması suretiyle giderilmesine çalışılmıştır. Bu şekilde sistemin daha başarılı sonuçlar ortaya çıkardığı da anlaşılmıştır.

Bu çalışmada ise hibrit yaklaşımla yapılan öznitelik seçimi sonrasında gerçekleştirilen sınıflandırma işlemlerinde Doğruluk metriğine göre en başarılı sonuç (0,94) RF sınıflayıcısı ile Kesinlik, Duyarlılık ve F1 metriklerine göre en başarılı sonuçlar ise (0,93) hem RF hem de XGB sınıflayıcıları ile elde edilmiştir.

Çalışmada manuel olarak seçilen ilk öznitelik grubu ile gerçekleştirilen sınıflandırma sonuçlarına göre ise Doğruluk, Kesinlik ve Duyarlılık metriklerinde en başarılı sınıflayıcılar (0,93) XGB ve RF olurken, F1 metriğine göre ise en başarılı sonuçlar (0,92) RF sınıflayıcısı ile elde edilmiştir.

Çalışmanın manuel olarak seçilen son öznitelik grubu ile yapılan testlerde ise Doğruluk, Kesinlik, Duyarlılık ve F1 metriklerinin tamamında en başarılı sonuçlara (0,94) DT sınıflayıcısı ile ulaşılmıştır.

Oluşturulan modellerin ne kadar iyi çalıştığını görmek için Çapraz Doğrulama (Cross Validation) işlemi uygulanmış ve ROC eğrileri oluşturulmuştur. Deneylerde öne çıkan XGB, RF ve DT sınıflayıcıları ile oluşturulan modellerin Çapraz Doğrulama sonuçları incelendiğinde, bu sonuçların başarılı olduğu gözlemlenmektedir.

Deney sürecinde yapılan sınıflandırmalara ait ROC Eğrileri incelendiğinde ise XGB, LR ve RF sınıflayıcıları ile yapılan çalışmaların daha doğru sonuçlar verdiği görülmektedir.

Deneylere ait Çapraz Doğrulama ve ROC Eğrileri birlikte incelendiğinde XGB ve RF sınıflayıcılarının bahsedilen her iki analize göre çok başarılı sonuçlar ortaya koyduğu görülmektedir. Bu da modellerin gösterdiği sınıflandırma sonuçlarının rastlantısal olarak değil gerçekten stabil bir modele göre tutarlı sonuçlar ortaya koyduğunu göstermektedir.

Çalışmanın sonunda yapılan aynı veri setinin tüm etiketlerini içeren çoklu sınıflandırma uygulaması sonuçları da veri setindeki örnek dağılımının dengesiz olduğunu göstermiştir. Her ne kadar diğer etiketlere oranla çok daha fazla olan “Normal” ağ hareketlerini doğru sınıflandırılmış olsa da diğer etiketlere ait örnekler test veri seti içerisinde dengeli dağılamamış ve bu durumun sınıflandırma başarısına olumsuz yönde etki ettiği görülmüştür.

5. SONUÇ VE ÖNERİLER

Bilgisayar ağlarına yönelik saldırıların önlenebilmesi, ilgili ağlarda ortaya çıkabilecek güvenlik zafiyetlerine tedbir alınması ve daha çok kullanıcının oluşturduğu güvenlik açıklarının kapatılmasıyla mümkün olabilecektir. Bununla birlikte teknolojinin gelişimine paralel olarak artan kullanıcı sayıları ve uygulama çeşitliliği bu durumu zorlaştırmakta ve yapılan saldırı türlerini artırmaktadır. Sürekli gelişim ve değişim içinde olan bu konsept nedeniyle saldırı tespit ve önleme sistemleri de günden güne değişmekte ve gelişmektedir.

Yapılan bu çalışmayla ağlara nüfuz eden saldırıların tespiti ve saldırı nedeniyle oluşabilecek her türlü zararın minimize edilebilmesi için ağ yönetimiyle ilgili ve yetkili kişilerin uyarılmasını sağlayacak olan bir karar destek modelinin oluşturulması üzerine bir araştırma yapılmıştır. Saldırı tespit sürecinde insan müdahalesinin olabildiğince az, makine öğrenmesi esaslarına dayanan ve ağ trafiğindeki olağan dışı hareketleri önceden tanımlanması gerek kalmadan yorumlayabilen bir sistem hedeflenmiştir.

Çalışma sonucunda elde edilen veriler ışığında saldırı tespitinde kullanılacak olan özniteliklerin en iyi şekilde seçilmesi gerektiği görülmüştür. Çalışmada önerilen iki aşamalı hibrit öznitelik seçim yönteminin XGB ve RF algoritmalarıyla birlikte saldırı tespitinde başarı oranını artırdığı görülmektedir. Daha çok deney tecrübesi ile manuel olarak seçilen daha az üyeye sahip öznitelik gruplarında ise DT algoritmasının öne çıktığı görülse de hedeflenen modelde insan müdahalesinin minimize edilebilmesi için önerilen hibrit öznitelik seçim tekniği ve XGB, RF algoritmalarıyla yapılan saldırı tespitinin daha uygun olduğu tavsiye edilmektedir. Ayrıca CICIDS 2017 veri setindeki örnek dağılımının dengesizliğinin sınıflandırma başarısına olumsuz etkisi görülmüş ve bu dengesizliğin giderilmesi için hedef etiketlerin belirli kriterlere göre birleştirilmesinin daha başarılı sonuçlar ortaya çıkaracağı tavsiye edilmektedir.

Gelecek çalışmalarda aynı veri seti üzerinde mevcut olan farklı saldırı tiplerine göre sınıflandırmaların yapılabileceği düşünülmektedir. Ayrıca çalışma sürecinde, üzerinde çalışılan CICIDS2017 veri seti her ne kadar geniş ve kapsamlı olsa da gelecekte daha nitelikli dengeli şekilde oluşturulacak olan veri setleri üzerinde seçilen öznitelikler ve eğitilen modeller ile daha etkili sonuçlar alınacağı öngörülmektedir.

KAYNAKLAR

Abar, H. (2020). XGBoost ve Mars Yöntemleriyle Altın Fiyatlarının Kestrimi. *EKEV Akademi Dergisi*, 24 (83), 427-446.

Abdel-Aziz, A.S., Hassanien, A.E., Azar, A.T. & Hanafi, S.E. (2013, September). Machine Learning Techniques for Anomalies Detection and Classification. *In Proceedings of SecNet*, 219-229.

Akar, Ö. & Güngör, O. (2012). Rastgele Orman Algoritması Kullanılarak Çok Bantlı Görüntülerin Sınıflandırılması. *Jeodezi ve Jeoinformasyon Dergisi*, (106), 139-146.

Aksu, M. & Karaman, E. (2017). Link Analysis and Detection in a Web Site With Decision Trees. Acta Infologica, 1(2), 84-91.

Alamiedy, T.A., Anbar, M., Alqattan, Z.N.M. & Alzubi, Q.M. (2019). Anomaly-Based Intrusion Detection System Using Multi-Objective Grey Wolf Optimisation Algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 11, 3735–3756.

Aljawarneh, S., Adlwairi, M. & Yassein, M.B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, 25, 152–160.

Bace, R. & Mell, P. (2011). NIST Special Publication on Intrusion Detection Systems. Gaithersburg: Publications of National Institute of Standards and Technology, 1-53.

Baykız, M.S. (2020). Elektronik Finans Kullanan Küçük ve Orta Büyüklükteki İşletmelerde (KOBİ) Bilgi Güvenliği Risklerine Karşı Alınabilecek Tedbirler Üzerine Bir Öneri: Bilgi Güvenliği Odaklı İç Kontrol ve Risk Profiline Uygun Kontrol Seçimi, Yayınlanmış Doktora Tezi, Gazi Üniversitesi Yönetim Bilişim Sistemleri Ana Bilim Dalı, Ankara.

Bircan, H. (2004). Lojistik Regresyon Analizi: Tıp Verileri Üzerine Bir Uygulama. *Kocaeli Üniversitesi Sosyal Bilimler Dergisi*, (8), 185-208.

Canbek, G. & Sağıroğlu, Ş. (2006) Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9 (3), 165-174.

Chen, T., & Guestrin, C. (2016). XGBoost: A Scalable Tree Boosting System, In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 785-794.

Chen, W., Kong, F., Mei, F., Yuan, G., & Li, B. (2017, May). A novel unsupervised anomaly detection approach for intrusion detection system. IEEE 3rd International Conference On Big Data Security On Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), And IEEE International Conference On Intelligent Data And Security (IDS). Beijing: IEEE.

Farahani, G. (2020). Feature Selection Based on Cross-Correlation of the Intrusion Detection System. *Hindawi Security and Communicaiton Networks*, 2020(6), 1-17.

Fernandez, G.C. ve Xu, S. (2019, November). A Case Study on Using Deep Learning for Network Intrusion Detection. *2019 IEEE* Military Communications Conference. Norfolk: IEEE, 12-14.

Gosu, J.S., Priyadarsini, P & Motupalli, R.K. (2021). A Hybrid Approach fort he Analysis of Feature Selection using Information Gain and BAT Techniques on The Anomaly Detection. *Turkish Journal of Computer and Mathematics Education,* 12(5), 656-666.

İnternet: A comprehensive guide to Feature Selection using Wrapper methods in Python. Analytics Vidhya (2020). Vikas Verma. Web: https://www.analyticsvidhya. com/blog/2020/10/a-comprehensive-guide-to-feature-selection-using-wrapper-methods-in-python/ adresinden 19 Şubat 2022'de alınmıştır.

İnternet: SPSS'te İlişki ve Anlamlılık. Alfa İstatistik (2018). Web: https://alfaistatistik.com/blog/16/spss-te-iliski-ve-anlamlilik adresinden 21 Eylül 2022'de alınmıştır.

Internet: Going on the Defensive: Intrusion Detection System (2002). InformIt, Web: https://www.informit.com/articles/article.aspx?p=29601 adresinden 19 Ocak 2022'de alınmıştır.

İnternet: Internet Security Report (2021). Watch Guard, Web: https://www.watchguard.com/wgrd-resource-center/security-report-q4-2021. adresinden 2 Şubat 2022'de alınmıştır.

İnternet: Sklearn Feature Selection RFE (2022). Scikit Learn, Web: https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.RFE.html adresinden 18 Şubat 2022'de alınmıştır.

Jabez, J. & Muthukumar, B. (2015). Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach. *Procedia Computer Science*, 48, 338-346.

Jose, S., Malathi, D., Reddy, B. & Jayasseeli, D. (2018). A Survey on Anomaly Based Host Intrusion Detection System. *Journal of Physics: Conference Series* 1000 (1), 12-49.

Karataş, G. & Şahingöz, Ö.K. (2018, March). Neural Network Based Intrusion Detection Systems with Different Training Functions. 2018 6th International Symposium on Digital Forensic and Security. Antalya: IEEE, 1-6.

Karataş, G., Demir, Ö. ve Şahingöz, Ö.K. (2018, December). Deep Learning in Intrusion Detection Systems. International Congress on Big Data Deep Learning and Fighting Cyber Terrorism. Ankara: IEEE, 113-116.

Karcı, Z. (2017). Lojistik Regresyon Modeli İle Elde Edilen Tahminlerin ROC Eğrisi Yardımıyla Değerlendirilmesi: Türkiye'de Hanehalkı Yoksulluğu Üzerine Bir Araştırma, Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Ekonometri Anabilim Dalı, Isparta.

Karniabudi, Stiawan, D., Darmawijoyo, Bin Idris, M.Y., Bamhdi, A.M. & Budiarto, R. (2020). CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection. IEEE Access, 2020(8), 132911-132921.

Keserwani, P.K., Govil, M.C., Pilli, E.S. & Govil, P. (2021). A Smart Anomaly-Based Intrusion Detection System For The Internet of Things (IoT) Network Using GW0-PSO-RF Model. *Journal of Reliable Intelligent Environments,* 7, 3-21.

Kishore, P.J., Raman, C.R., Raja, J.K. ve Rao, R.V. (2021). A Multi Approach For The Analysis of Feature Selection Using Data Gain and BAT Techniques On The Anomaly Detection. *Turkish Journal of Computer and Mathematics Education*, 12 (11), 4708-4718.

Kültür, E. (2022). Network Intrusion Detection With A Deep Learning Approach, Unpublished Master's Thesis, Middle East Technical University Cyber Security Department, Ankara.

Kumar, V., Choudhary, V., Sahrawat, V. & Kumar, V. (2020, June). Detecting Intrusions and Attacks in the Network Traffic using Anomaly based Techniques. Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020) Coimbatore: ICCESS, 554-560.

Küçüksille, E.U. & Ateş, N. (2016). Destek Vektör Makineleri ile Yaramaz Elektronik Postaların Filtrelenmesi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 6 (1).

Özekes, S. & Karakoç, E.N. (2019). Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7, 566-576.

Paigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Kumar, Y. & Jhaveri, R.H. (2021). A Consolidated Decision Tree-Based Intrusion Detection System for Binary and Multiclass Imbalanced Datasets. *Mathematics MDPI*, 9 (7), 1-35.

Panigrahi, R. & Borah, S. (2018). A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. *International Journal of Engineering & Technology*, 7, 479-482.

Pfleeger, C.P. (1997). The Fundamentals of Information Security. *IEEE Software*, 14 (1), 15 – 16.

Ran, J., Ji, Y. & Tang, B. (2019, April). A Semi-Supervised Learning Approach to IEEE 802.11 Network Anomaly Detection. Proceedings of 2019 IEEE 89th Vehicular Technology Conference. Kuala Lumpur: IEEE, 1-5.

Reis, B., Maia, E. & Praça, I. (2020). Selection and Performance Analysis of CICIDS2017 Features Importance. In: Benzekri, A., Barbeau, M., Gong, G., Laborde, R., Garcia-Alfaro, J. (Eds.), *Foundations and Practice of Security*. Springer, Cham, pp. 56-71.

Sağıroğlu, Ş. & Alkan, M. (2018). Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık, Ankara: Grafiker Yayınları, 26-34.

Sağıroğlu, Ş., Yolaçan, E.N. & Yavanoğlu, U. (2011). Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi. *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi*, 26 (2), 325-340.

Satam, P. & Hariri, S. (2020). WIDS: An Anomaly Based Intrusion Detection System for Wi-Fi (IEEE 802.11) Protocol. *IEEE Transactions on Network and Service Management*, 18(1), 1077-1091.

Scarfone K. & P. Mell (2007). Guide to Intrusion Detection And Prevention Systems (IDPS), NIST Special Publication. Gaithersburg: Publications of National Institute of Standards and Technology, 94.

Shams, M. (2020). Ağ Anomalisi Tespitinde Makine Öğrenmesi Algoritmalarının Kullanımı ve Karşılaştırmalı Analizi, Yayınlanmış Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.

Shaukat, S., Ali, A., Batool, A., Alqahtani, F., Khan, J.S. & Ahmad, J. (2020, November). Intrusion Detection and Attack Classsification Leveraging Machine Learning Technique. 14th International Conference on Innovations in Information Technology. Al Ain: IEEE. 198-202.

Spafford, E. (2008). James P. Anderson: An Information Security Pioneer. *IEEE Security and Privacy Magazine* 6(1), 9.

Tomak, L. & Bek, Y. (2011). İşlem Karakteristik Eğrisi Analizi ve Eğri Altında Kalan Alanların Karşılaştırılması. *Ondokuz Mayıs Üniversitesi Deneysel ve Klinik Tıp Dergisi*, 27 (2).

Yıldırım, M. Z., Çavuşoğlu, A., Şen, B., & Budak, İ. (2014, Şubat). Yapay Sinir Ağları ile Ağ Üzerinde Saldırı Tespiti ve Paralel Optimizasyonu. XVI, Akademik Bilişim. Mersin: Mersin Üniversitesi, 671-677.

Yu, L., Dong, J., Chen, L., Li, M., Xu, B., Li, Z., Qiao, L., Liu, L., Zhao, B. & Zhang, C. (2021). PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection. Computer Networks, 194.

Zdaniuk, B. (2014). Ordinary Least-Squares (OLS) Model, In Michalos, A.C. (Eds.), *Encyclopedia of Quality of Life and Well-Being Research*. Dorddrecth: Springer, pp. 4515–4517.

Zhou, Y., Cheng, G., Jiang, S. ve Dai, M. (2020). Building An Efficient Intrusion Detection System Based On Feature Selection And Ensemble Classifier. Computer Networks, 174.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: E**** B****
Uyruğu	: T.C.
Doğum tarihi ve yeri	:
Medeni hali	:
Telefon	:
e-mail	:

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek lisans	SBTÜ/ Savunma Teknolojileri	Devam ediyor
Lisans	Ankara Üniversitesi / Bilgisayar Mühendisliği	2011
Lise	Selçuk Anadolu Lisesi	2006

İş Deneyimi

Yıl	**Yer**	**Görev**
2011-Halen	Karayolları 16. Bölge Müdürlüğü	Bilgi Teknolojileri Başmühendisi

Yabancı Dil

İngilizce

Yayınlar

Ekici, B. & Takcı, H. (2022). Bilgisayar Ağlarında Anomali Tespiti Yaklaşımı ile Saldırı Tespiti. Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi, 22 (5), 1016-1027.

Ekici, B. & Takcı, H. (2021). Spam Tespitinde Word2Vec ve TF-IDF Yöntemlerinin Karşılaştırılması ve Başarı Oranının Artırılması Üzerine Bir Çalışma. Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi, 8 (2), 646-655.

Hobiler

Yüzme, Tarih, Futbol

KÖKLERDEN GÖKLERE…