****

**İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU**

**BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ**

**BİLİŞİM TEKNOLOJİSİ GÜVENLİĞİ PROGRAMI**

**AĞ ANOMALİ TESPİTİNDE MAKİNE ÖĞRENMESİ ALGORİTMLARININ KULLANILMASI VE SINIFLANDIRILMA İÇİN BİR UYGULAMA ÖRNEĞİ**

**FİNAL PROJE ÖDEVİ**

**Hazırlayan**

**220175094-Mustafa Yurtalan**

**220175078-Mehmet Mert Kılıçarslan**

**220175144-Furkan Yurtseven**

**220175092-Alp Murat Külahçıoğlu**

**230175389-Mehmet Akif Erdener**

**Ödev Danışmanı**

**Ögr.Gör. Sena Nur Benli**

**İSTANBUL-12.16.2023**

**ÖDEV TANITIM FORMU**

**YAZAR ADI SOYADI :** Mustafa Yurtalan, Furkan Yurtseven, Mehmet Akif Erdener, Alp murat Külahçıoğlu, Mehmet Mert Kılıç Arslan

**ÖDEVİN DİLİ :** Türkçe

**ÖDEVİN ADI :** AĞ ANOMALİ TESPİTİNDE MAKİNE ÖĞRENMESİ ALGORİTMLARININ KULLANILMASI VE SINIFLANDIRILMA İÇİN BİR UYGULAMA ÖRNEĞİ

**BÖLÜM :** Bilişim Güvenliği Teknolojisi

**PROGRAM :** Bilgisayar Teknolojisi

**ÖDEVİN TÜRÜ :** Final

**ÖDEVİN TES. TARİHİ :** 28/12/2023

**SAYFA SAYISI :** 13

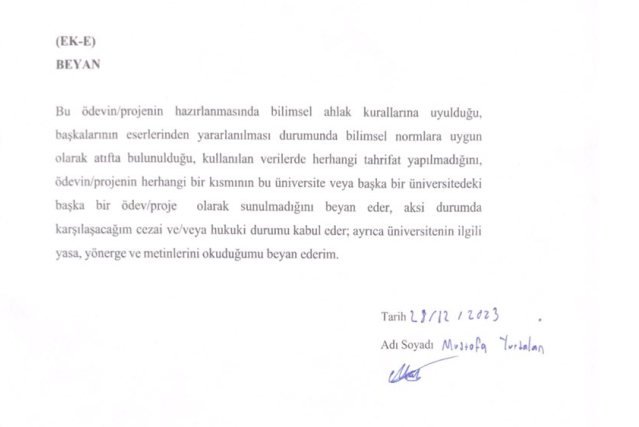
**ÖDEV DANIŞMANI :** Sena Nur Benli

# ÖZET

Ağ anomalisi tespitinde yapay zeka algoritmaları nasıl kullanılır, hangi algoritma neden tercih edilebilir, data set optimizasyonu neden önemlidir v.b konularının incelenip bir bütün halde işlendikten sonra sonuçlarının rapor edilmesi

**Anahtar Kelimeler: Ağ, Anomali, Algoritma, Veri seti, Yapay Zeka**

**Beyan**



İÇİNDEKİLER

ÖDEV TANITIM FORMU [i](#_Toc132112609)

[ÖZET ii](#_Toc132112609)

[İÇİNDEKİLER iii](#_Toc132112610)

[ÖN SÖZ iv](#_Toc132112610)

[GİRİŞ v](#_Toc132112610)

[1.1 Bilgisayar Ağları Ve Yapay Zeka 1](#_Toc132112611)

[1.2 Bilgisayar Ağları 1](#_Toc132112611)

[1.3 LAN (Local Area Network) 1](#_Toc132112611)

[1.4 WAN (Wide Area Network) 1](#_Toc132112611)

[1.5 Yapay Zeka 1](#_Toc132112611)

[1.6 Makine Öğrenimi 1](#_Toc132112611)

[1.7 Derin Öğrenme 1](#_Toc132112611)

[2.1 Yapay Zeka Algoritmaları 2](#_Toc132112611)

[2.2 Karar Ağaçları 2](#_Toc132112611)

[2.3 Navie Bayes 2](#_Toc132112611)

[2.4 Yapay Sinir Ağları 3](#_Toc132112611)

[2.5 Destek Vektör Makineleri 4](#_Toc132112611)

[3.1 Algoritmaların Kullanımı 4](#_Toc132112611)

[3.2 Sonuçlar 6](#_Toc132112611)

[Kaynakça 7](#_Toc132112611)

**ÖN SÖZ**

En başta ödev danışmanımız olan sayın Sena Nur Benli Hocamıza teşekkürlerimizi sunmak istiyoruz. Gerek ders içi gerek ders dışı kattığı vizyon ve verdiği fikirler ile ilerlememiz de çok büyük katkıda bulunmuştur. Bu süreçte yanımızda olan adını veremediğimiz herkese iyi dilekler diliyoruz.

**GİRİŞ**

Günümüz dünyasında her an etrafımız çeşitli cihazlar ile çevrilidir bu cihazlara okul laboratuvarların da kullandığımız bilgisayarlar, elimizde tutuğumuz telefon, şirkette bulunan yazıcıya kadar çeşitli örnekler verebiliriz bu cihazların ortak noktalarından biri hepsinin ağ ortamında bulunabilme özelliği olmasıdır bu sayede ortak ağda bulunan cihazlar ile haberleşebilirler.

Bu durumun bir dezavantajı bulunmaktadır ağ içindeki cihazların ve ağın kendisinin güvenliğinin sağlanması doğru bir iletişim için kilit rol oynamaktadır çeşitli donanımsal ve yazılımsal önlemler ile bunun önüne geçilebiliyorken günümüzde gelişen yapay zeka teknolojisi ile bu önlemlere yeni bir soluk gelmiştir.

## Bilgisayar Ağları ve Yapay Zeka

Bilgisayar ağları ve yapay zeka, modern teknolojinin temel taşları arasında yer alır. Her iki alan da bilgisayar sistemlerinin işlevselliğini genişleten, iş birliği içinde çalışan ve daha akıllı hale getiren önemli kavramları içermektedir.

## 1.2 Bilgisayar Ağları

Bilgisayar ağları, bilgisayarların birbirleriyle iletişim kurabildiği ve bilgi paylaşabildiği yapıları ifade eder. Temelde, bu ağlar lokal (LAN) veya geniş alan (WAN) ağları olabilir. İnternet, dünya genelindeki bilgisayarları birbirine bağlayan en büyük WAN örneğidir.

Ağ içerisinde iletişim cihazlar üzerindeki IP’adresleri ve çeşitli protokoller ile idare edilir.

## 1.3 LAN (Local Area Network)

LAN, genellikle bir binaya veya bir kuruluşun belirli bir yerine yayılan bir ağdır. Bilgisayarlar, yazıcılar ve diğer cihazlar arasında hızlı veri iletişimini sağlar.

## 1.4 WAN (Wide Area Network)

WAN, coğrafi olarak uzak yerlerde bulunan LAN'ları birbirine bağlayan bir ağ türüdür. Örneğin, bir şirketin farklı şehirlerdeki ofisleri arasında iletişim sağlar.

## 1.5 Yapay Zeka

Yapay zeka, bilgisayar sistemlerine insan benzeri zekâ ve öğrenme yetenekleri kazandırmayı amaçlayan bir disiplindir. Bu alanda öne çıkan önemli kavramlar arasında makine öğrenimi ve derin öğrenme bulunmaktadır.

## 1.6 Makine Öğrenimi

Makine öğrenimi, bilgisayar sistemlerinin belirli bir görevi belirli bir performans düzeyinde gerçekleştirmek için verilerden öğrenmesini sağlayan bir yöntemdir. Örneğin, bir e-posta spam mı yoksa değil mi diye sınıflandırılabilir.

## 1.7 Derin Öğrenme

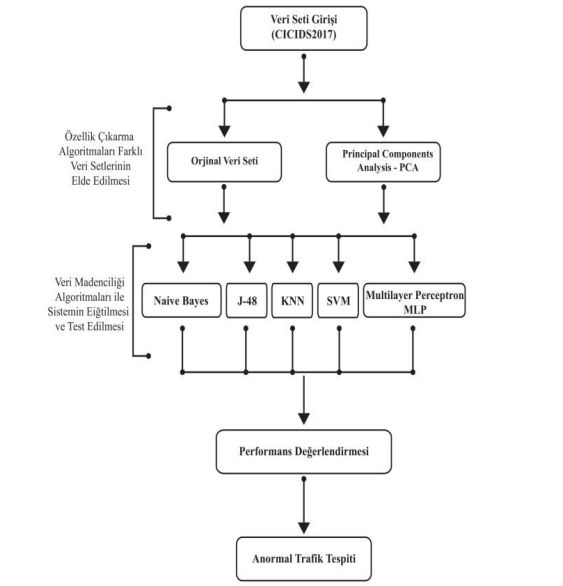
Derin öğrenme, yapay sinir ağları aracılığıyla büyük miktarda veriyi analiz ederek karmaşık görevleri gerçekleştirmek için kullanılan bir makine öğrenimi alt dalıdır. Ses ve görüntü tanıma gibi alanlarda etkili bir şekilde kullanılır.

Bilgisayar ağları ve yapay zeka, bir araya geldiğinde, veri paylaşımını hızlandırabilir, otomatik karar alma süreçlerini optimize edebilir ve daha akıllı sistemlerin geliştirilmesine olanak tanır. Bu entegrasyon, birçok sektördeki iş süreçlerini ve günlük yaşantımızı önemli ölçüde etkileme potansiyeline sahiptir.

## 2.1 Yapay Zeka Algoritmaları

## 2.2 Karar Ağaçları

Karar ağacı algoritmaları, makine öğrenimi ve veri madenciliği alanlarında geniş bir uygulama yelpazesine sahip olan etkili ve yaygın bir modelleme tekniğidir. Bu algoritmalar, karmaşık karar yapılarını anlamak ve öğrenmek için kullanılır. Temel kavramlar arasında, her iç düğümün bir özellik veya öznitelik üzerinde bir testi temsil ettiği bir ağaç yapısı, özellik seçimi ve bölünme kriterleri bulunur. Algoritmalar, Gini impurity, bilgi kazancı veya hata oranı gibi farklı bölünme kriterlerini kullanarak en iyi bölünmeyi belirler. Ağaç, veri setine adapte olmak ve karmaşıklığı kontrol etmek için büyütülür ve ardından gerektiğinde budanır. Sınıflandırma ve regresyon görevlerinde etkili bir şekilde kullanılan bu algoritmalar, tıp alanında hastalıkları sınıflandırmaktan, ev fiyatlarını tahmin etmeye kadar birçok uygulama alanında değerli çözümler sunar. Ayrıca, müşteri davranışlarını analiz etmek ve hedefli pazarlama stratejileri geliştirmek gibi işletmelerde de kullanılarak geniş bir etki alanına sahiptirler.



Şekil 1Performans testi diyagramı

## 2.3 Navie Bayes

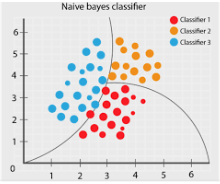
Naive Bayes sınıflandırma algoritmaları, makine öğrenimi alanında önemli bir role sahip olan bir grup olasılık temelli modellendirme yöntemidir. Bu algoritmalar, basit ancak etkili bir şekilde çalışabilme yetenekleri ile öne çıkarlar. Temel kavramlar arasında Bayes teoremi, olasılık hesaplamaları ve özellik bağımsızlık varsayımı bulunmaktadır.

Naive Bayes algoritmalarının temelinde Bayes teoremi yer alır, bu teorem bir olayın gerçekleşme olasılığını, bu olayın gerçekleştiği koşulları bilerek hesaplamayı sağlar. Naive Bayes'in "naive" (saf) olarak adlandırılmasının nedeni, bu algoritmanın özellikler arasındaki bağımsızlık varsayımını yapmasıdır; yani, her özellik diğer özelliklerden bağımsızdır.

Algoritmanın çalışma prensibi, bir veri noktasını bir sınıfa sınıflandırmak için özniteliklerin birleşik olasılığını kullanmaktır. Bu, her sınıf için olasılıkları karşılaştırarak en yüksek olasılığa sahip sınıfı seçmek şeklinde gerçekleşir.

Uygulama alanlarına gelince, Naive Bayes sınıflandırıcıları genellikle metin madenciliği ve spam filtreleme gibi doğal dil işleme görevlerinde kullanılır. Ayrıca, tıp alanında hastalık teşhisi ve finansal analiz gibi birçok alanda da etkili bir şekilde kullanılmaktadır.

Sonuç olarak, Naive Bayes algoritmaları, basit yapısı, hızlı eğitim ve tahmin yetenekleri ile öne çıkan, özellikle büyük veri setleri üzerinde etkili çalışabilen bir sınıflandırma yöntemidir.

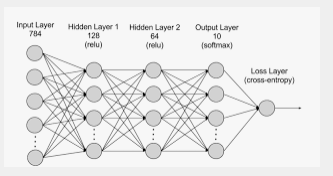


Şekil 2 Navie Bayes Sınıflandırması

## 2.4 Yapay Sinir Ağları

Yapay Sinir Ağları, biyolojik sinir sistemlerinden ilham alarak tasarlanan ve karmaşık veri modellerini öğrenme yeteneğiyle öne çıkan güçlü bir makine öğrenimi teknolojisidir. Bu algoritmalar, birbirine bağlı nöronlardan oluşan katmanlar aracılığıyla bilgiyi işler ve öğrenir. Eğitim aşamasında, gerçek ve tahmin edilen sonuçlar arasındaki hatayı minimize etmek için ağırlıkları günceller, bu da ağın doğru tahminlerde bulunma yeteneğini artırır. Aktivasyon fonksiyonları sayesinde non-lineer ilişkileri modelleyebilirler ve derin yapılı modellerle karmaşık özellikleri öğrenerek görüntü tanıma, doğal dil işleme, oyun stratejileri ve birçok uygulama alanında etkili çözümler sunabilirler. Yapay sinir ağları, geniş veri setleri

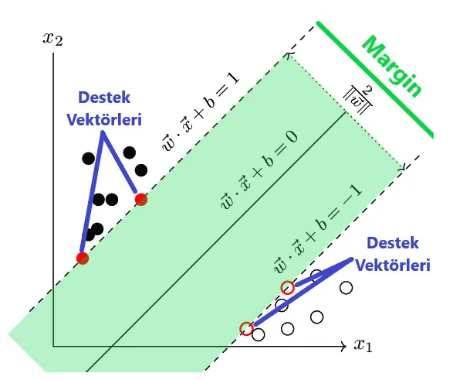
üzerindeki desenleri keşfetme ve genelleyebilme yetenekleriyle, bilgi işleme ve öğrenme konularında büyük bir devrim başlatmıştır.



Şekil 3 Yapay sinir ağaçları

## 2.5 Destek Vektör Makineleri

Destek Vektör Makineleri (SVM), veri noktalarını sınıflandırmak veya regresyon analizi yapmak için kullanılan güçlü bir makine öğrenimi algoritmasıdır. SVM, veri noktalarını çok boyutlu uzayda temsil eden ve bu uzayda en iyi ayrımı sağlayan hiper düzlemi bulma temeline dayanır. Bu hiper düzlem, farklı sınıflara ait veri noktalarını birbirinden mümkün olduğunca uzakta tutarak en iyi sınıflandırmayı elde etmeyi amaçlar. SVM, bu ayrımı en iyi sağlayan destek vektörleri kullanarak çalışır. Eğitim aşamasında, veri noktalarını sınıflandırmak için optimum hiper düzlemi bulmak için destek vektörleri belirlenir ve bu süreçte margin (marj) kavramı kullanılır. SVM, doğrusal ve doğrusal olmayan (Kernel trick kullanılarak) ayrımlar yapabilme esnekliğiyle, özellikle yüksek boyutlu ve karmaşık veri setlerinde etkili sonuçlar elde edebilen bir algoritmadır. Bu nedenle, SVM, özellikle sınıflandırma ve regresyon problemlerinde başarıyla uygulanan ve geniş bir uygulama yelpazesine sahip bir makine öğrenimi tekniğidir.

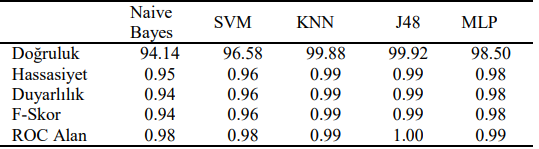


Şekil 4 Destek vektör makinesi

## 3.1 Algoritmaların Kullanımı

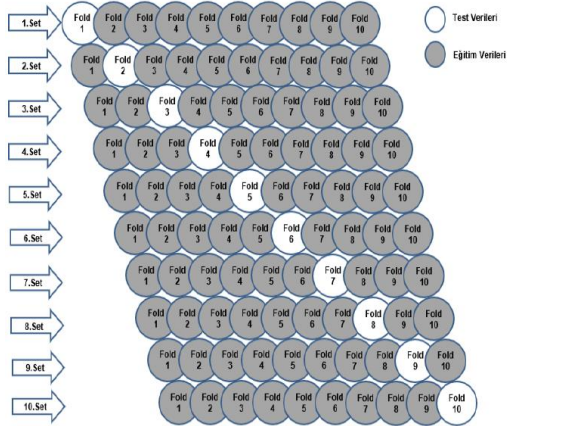
Ağ anomalisi tespiti için kullanılacak algoritma seçildikten sonra. Algoritmaların eğitimi için bir data sete ihtiyacımız ortaya çıkar, Kanada Siber Güvenlik Enstitüsü tarafından

oluşturulmuş CICIDS2017 veri seti kullanılarak algoritmaları eğitir isek her bir algoritmanın doğruluk oranını şekilde görebiliriz.



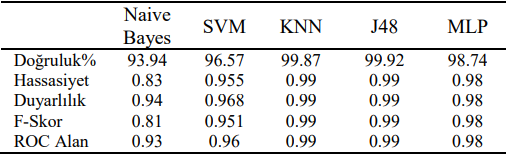
Şekil 5 Algoritma Doğruluk Oranları

Algoritmalar sınanır iken çapraz doğrulama kullanılmış olup kat sayısı 10 olarak belirlenmiştir. İlk katmanı test verisi kalan 9 katmanı eğitim verisi olarak kullanılmıştır, bütün adımlar tüm algoritmalarda aynı şekilde tekrar etmiştir.



Şekil 6 Çapraz Doğrulama Yapısı

Veri seti üzerinde boyutsal indirgeme algoritması (PCA) kullanılıp veri setinin boyutu küçülttüğünde. Her bir algoritma için doğruluk oranları değişmiştir



Şekil 7 PCA Kullanıldıktan sonra Doğruluk oranları

## 3.2 Sonuçlar

Yapay Zeka Algoritmalarının Ağ Anomalisi Tespitinde kullanımında doğru bir algoritma seçilmesi oldukça önemlidir. Aksi taktirde ağ içinde dolaşan paketlerin yanlış sınıflandırılmasından dolayı sorunlar ile karşılaşılma ihtimali oldukça yüksektir.

Doğru algoritma seçiminin ardından gelen en önemli kısım doğru data setinin seçilmesidir,

CICIDS2017 gibi bu çalışmada örnek olarak gösterilen veri seti open-source ve oldukça yaygın kullanılan bir veri setidir bundan mütevellit aynı özellikleri taşıyan başka veri setleri doğru veri setlerine örnek gösterilir.

Bu çalışma sonucunda Yapay Zeka Algoritmalarının Ağ Anomalisi Tespitinde kullanımında kullanılan algoritmalarının değerlendirilmesi ve doğruluk oranlarının karşılaştırılması yapılmıştır.

**Kaynakça**

Şekil 1

https://dergipark.org.tr/tr/download/article-file/2416699

Şekil 2 <https://www.google.com/imgres?imgurl=https%3A%2F%2Feditor.analyticsvidhya.com%2Fuploads%2F23385Capture6.PNG&tbnid=afFRnYbTIkmd9M&vet=12ahUKEwjf5YCTmKiDAxULif0HHb0LDFcQMygEegQIARBX..i&imgrefurl=https%3A%2F%2Fwww.analyticsvidhya.com%2Fblog%2F2022%2F03%2Fbuilding-naive-bayes-classifier-from-scratch-to-perform-sentiment-analysis%2F&docid=JFlOV1-weQNNvM&w=879&h=715&q=naive%20bayes&ved=2ahUKEwjf5YCTmKiDAxULif0HHb0LDFcQMygEegQIARBX>

Şekil 3

<https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRvsJ38daCyuw7jTkOVa665cLVWkRHY_PiH6DFe0BoMatOyJLoM>

Şekil 4

[https://miro.medium.com/v2/resize:fit:569/1\*OGs3M3e9zPDfRaVx2BRoPg.png](https://miro.medium.com/v2/resize:fit:569/1*OGs3M3e9zPDfRaVx2BRoPg.png)

Şekil 5

https://dergipark.org.tr/tr/download/article-file/2416699

Şekil 6

https://dergipark.org.tr/tr/download/article-file/2416699

Şekil 7

https://dergipark.org.tr/tr/download/article-file/2416699

<https://mkotan.sakarya.edu.tr/sites/mkotan.sakarya.edu.tr/file/EKO469_VM_H12_Siniflandirma3.pdf>

https://mail.baskent.edu.tr/~20410964/DM\_8.pdf