ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi
International Journal of Sustainable Engineering and Technology
ISSN: 2618-6055 / Cilt: 8, Sayı: 1, (2024), 8 – 25
Araştırma Makalesi – Research Article

SOSYAL MEDYA PAYLAŞIMLARINDA KARAR MEKANİZMALARININ ÖĞRENME ALGORİTMALARIYLA KARŞILAŞTIRMALI ANALİZİ

*Dudu DEMİRBİLEK[1], Mevlüt ERSOY[1]

[1]Süleyman Demirel Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Isparta

(Geliş/Received: 01.04.2024, Kabul/Accepted: 09.06.2024, Yayınlanma/Published: 26.06.2024)

ÖZ

Dünya'da ve Türkiye'de artan internet kullanımına bağlı olarak bireyler sosyal medya platformlarını da aktif olarak kullanmaktadır. Kullanıcılar sosyal medya platformlarını kişisel gelişim, alışveriş, ticaret, eğitim, sosyalleşmek, arkadaşlıklar edinmek, çevrimiçi içerik üretmek ve bu içerikleri diğer kullanıcılarla paylaşabilmek amacıyla kullanmaktadırlar. Ama bu iyi niyetli kullanımların yanı sıra karşıdaki kişiye zarar vermek, onu küçük düşürmek, itibarını zedelemek ya da bilerek ve isteyerek zorbalık yapmak amacıyla da kullanımlar söz konusudur. Araştırmadaki amaç sosyal medya platformlarından biri olan Twitter'dan alınan yorumları doğal dil işleme süreçlerine tabi tutarak yorumlar içerisinde siber zorbalık olup olmadığını tespit etmek ve bu verilerin girdi olarak kullanıldığı sınıflandırma algoritmalarından elde edilen sonuçları karşılaştırarak en iyi sonucu elde etmektir. Araştırmada 11114 yorumdan oluşan veri seti doğal dil işleme süreçlerinden geçirilerek sınıflandırma algoritmalarına giriş verisi olarak verilmiştir. Bu verilerin bir bölümü eğitim seti olarak bir bölümü de test seti olarak kullanılmıştır. Sonuçta sınıflandırma algoritmalarından Ekstra Trees algoritmasından %86,95 doğruluk oranı elde edilerek diğer sınıflandırma algoritmasına göre daha başarılı olduğu gözlemlenmiştir.

Anahtar kelimeler: Sosyal Medya, Öğrenme Algoritmaları, Siber Zorbalık, Doğal Dil İşleme (NLP).

COMPARATIVE ANALYSIS OF DECISION MECHANISMS IN SOCIAL MEDIA SHARING WITH LEARNING ALGORITHMS

ABSTRACT

Due to the increasing internet usage in the world and in Turkey, individuals also actively use social media platforms. Users use social media platforms for personal development, shopping, commerce, education, socializing, making friends, producing online content and sharing these contents with other users. But in addition to these well-intentioned uses, there are also uses to harm the other person, humiliate her/him, damage her/his reputation, or knowingly and intentionally bully her/him. The aim of the research is to subject the comments received from Twitter, one of the social media platforms, to natural language processing processes to determine whether there is cyberbullying in the comments and to obtain the best result by comparing the results obtained from the classification algorithms where these data are used as input. In the research, the dataset consisting of 11114 comments was passed through natural language processing processes and given as input data to classification algorithms. Some of these data were used as the training set and some as the test set. As a result, it was observed that the Extra Trees algorithm, one of the classification algorithms, was more successful than the other classification algorithm, with an accuracy rate of 86.95%.

Keywords: Social Media, Learning Algorithms, Cyberbullying, Natural Language Processing (NLP).

***Sorumlu Yazar/Corresponding Author:** yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

1. Giriş (Introduction)

Dünya'da ve ülkemizde internet kullanımında belirgin bir artış söz konusudur. İnternet kullanımındaki bu artış sosyal medya platformlarının kullanımını da aynı oranda artırmıştır. Kullanıcılar bu platformları kendi gelişimlerini sağlamak ve sürdürmek amacıyla kullandıkları gibi eğitim, alışveriş, sosyalleşme, çevrimiçi içerik üretme ve paylaşma için de kullanmaktadırlar. Dünya' da dijital platformların gelişmesi ve kullanıcı sayılarının artması bilginin hızlı yayılmasını sağlamaktadır. Bu durum normal insanların hayatlarını kolaylaştırmasının yanı sıra yasalara ve ahlaki değerlere karşı saygı duymayan insanların da faaliyetlerde bulunmasını da kolaylaştırmıştır. Örneğin; siber zorbalık, çevrimiçi dolandırıcılık, veri hırsızlığı, izinsiz erişim gibi suçlar daha erişilebilir hale gelmiştir. Bu durum, özellikle bireylerin duygusal ve psikolojik olarak etkilenmelerine neden olan önemli bir sorun haline gelmiştir [1].

Dünyadaki dijital verileri her yıl raporlayan We Are Social raporunun 2023 yılı için hazırladığı rapordaki veriler incelendiğinde Dünya'da her geçen yıl sosyal medya kullanıcı sayılarının hızlı bir şekilde artış gösterdiği görülmektedir. Dünya'daki verilere benzer bir durum ülkemizde de görülmektedir. Bu verilere göre ülkemizdeki 62.55 milyon kişi sosyal medya kullanmaktadır. Sosyal medya kullanıcılarının toplam nüfusa oranı %73.1' e karşılık gelmektedir. Bu veriler ışığında ülkemizde sosyal medya kullanım oranının oldukça fazla olduğu görülmektedir [2]. Sosyal medyada görülen en temel siber suçlardan birisi siber zorbalıktır. Siber zorbalık, yasa dışı ve ahlaki değerlere karşı saygı duymayan kullanıcıların gerçekleştirdiği tehdit ve taciz etme, aşağılama, uygunsuz içerik paylaşma, hakaret etme gibi davranışların ortaya çıktığı bir siber saldırı türü olarak görülmektedir. Sosyal medya ortamlarının sayıca büyük bir kitle tarafından kullanılması mağdur sayısının da fazla olmasına neden olabilmektedir. Bu durum siber zorbalık farkındalığı olmayan bireylerde önemli sorunlara neden olabilmektedir [3].

Sosyal medya platformlarında karşılaşılan, bireyleri olumsuz etkileyen, siber zorbalık içeren yorumlar, tweetler, paylaşımlar anlık olarak tespit edilmesi farkındalığı olmayan bireyleri korumak için önemli bir durumdur. Dünya' da sosyal medya platformlarında her ülkenin kendi dili ile yapılan siber zorbalık ifadeleri ve yöntemleri farklılık gösterebilmektedir. Bu çalışmada, Türkçe dilinde gerçekleştirilen siber zorbalık içeren mesaj, yorum, tweet gibi paylaşımlar için bir uyarı sistemi geliştirilmesi hedeflenmiştir. Bu çalışmada, sosyal medya platformlarından biri olan X' de yapılan Türkçe dilinde yazılmış 11114 yorumdan oluşan bir veri seti kullanılmıştır. Bu kapsamda her dilin farklı dil özellikleri olması sebebiyle Türkçe diline uygun doğal dil işleme teknikleri kullanılmıştır. Doğal Dil işleme teknikleri ile elde edilen ifadelerin siber zorbalık cümleleri içerip içermediğinin tespiti için makine öğrenme algoritmaları ile sınıflandırma yapılmıştır. Algoritmaların karşılaştırmalı analizleri yapılmıştır. Bu algoritmalardan Extra Trees algoritmasından %86,95 başarı oranı ile diğer algoritmalara göre daha başarılı sonuçlar verdiği gözlenmiştir.

2. Literatür Taraması (Literature Review)

Doğal Dil İşleme ile ilgili "metinlerin anlaşılır hale gelebilmesi için hangi işlem basamakları uygulanır, hangi sınıflar hangi kütüphaneler kullanılır, elde edilen sonuçlar makine diline nasıl dönüştürülür" gibi konular araştırılmıştır. Bu çalışmalarda doğal dil işleme teknikleri uygulandıktan sonra öğrenme algoritmalarının kullanıldığı görülmüştür. Bu algoritmaların kullanımıyla ilgili çalışmalar araştırılmıştır. Bu araştırmalarla ilgili detaylar sunulmuştur.

Sevli ve Sezgin [4] çalışmalarında sosyal medya platformlarında işlenen suçlardan biri olan siber zorbalık ve bunun yanında altı farklı kategoride sınıflandırma çalışmaları yapmışlardır. 48 bine yakın tweetten oluşan veri seti kullanmışlardır. Bu veri seti içerisindeki tweetler doğal dil işleme süreçleri ile yorumlanabilir hale getirilmiştir. Bu çalışmada sınıflandırma algoritmalarından Rastgele Orman, Destek Vektör Makinesi ve K-En Yakın Komşu makine öğrenmesi sınıflandırma algoritmalarını kullanmışlardır. Sonuç olarak da en iyi değerlendirme yapan algoritma olarak Destek Vektör Makine algoritması olduğunu belirtmişlerdir.

Yazğılı [5] çalışmasında sosyal medya platformlarında siber zorbalık kavramının üzerinde duran yazar, siber zorbalığa maruz kalan kişilerin bu olaylar sonucunda intihara kadar varabilen olumsuz sonuçlarla karşı karşıya kaldıkları üzerinde durmaktadır. Bu çalışmada "kaggle" sitesinden temin ettiği 3000 cümleden oluşan Türkçe bir veri seti ile çalışmıştır. Bu veri setindeki veriler Label Encoder kodlayıcısı aracılığıyla metinsel veriler sayısal verilere dönüştürülmüştür. Bu veriler on üç farklı algoritmayla

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

işlenerek sonuçlar elde edilmiştir. Bu algoritmalar içerisinden en yüksek başarı sonucunu Logistik Resresyon algoritmasının verdiğini tespit etmiştir.

Ballı [6] çalışmasında iki farklı veri seti ile çalışmıştır. Bu veri setleri üzerinde gerekli ön işlemleri gerçekleştirmiştir. İki farklı kütüphane kullanılarak ön işlemden geçirilen veri setleri duygu analizlerinin yapılması için birden fazla farklı sınıflandırma algoritmaları ile eğitilmiştir ve bu kütüphane kullanımlarının sonuçları karşılaştırılmıştır.

Delibaş [7] çalışmasında Türkçe olarak girilen bir metin içerisinde varsa yer alan yazım yanlışlarını tespit etmeyi ve tespit ettiği bu hataları düzeltmeyi hedeflemiştir. Bu tespit ve düzeltmelerin yapılabilmesi için girilen metinlerdeki sözcüklerin doğru yazılıp yazılmadığı, doğru yazılmamışsa doğru kelimelerin önerilmesi sağlanmıştır.

Yelmen [8] çalışmasında Türkiye'de kullanılan GSM operatörlerinin kullanıcılarına ait Türkçe tweetlerdeki metinleri detaylı bir şekilde ön işlemeden geçirmiştir. Ön işlemeden geçirilen bu veriler Yapay Sinir Ağları, Destek Vektör Makineleri ve Centroid Tabanlı sınıflandırma algoritmaları Bilgi Kazancı, Gini İndeks ve Genetik algoritmalarla beraber hibrit olarak kullanılmıştır. Sonuçta Destek Vektör Makineleri Genetik algoritma ile birlikte hibrit olacak şekilde kullanıldığında tüm GSM operatörlerinde çok başarılı sonuçlar vermiştir.

Dolar [9] çalışmasında Türkiye'de satış yapan internet sitelerinde yer alan 27 ürüne ait 11236 Türkçe yorumlar rastgele bir şekilde uzmanlara verilmiş, manuel olarak etiketlemeler yapılarak kategorize edilen eğitim verileri, sınıflandırma algoritmaları, oyunlaştırma ve Doğal Dil İşleme teknikleri kullanılarak değerlendirilerek sonuçlar 5 farklı kategoriye ayrılmıştır.

Kesgin [10] çalışmasında sosyal medya platformlarında otomatik olarak metinler üzerinde saldırıdan dil tespiti yapmayı amaçlamıştır. Sosyal medya platformlarında kullanıcıların oluşturdukları içeriklere LR, SVM, LSTM gibi çoklu sınıflandırma algoritmaları uygulanıp değerlendirilmiştir. Algoritmaların performansları F1 Skoru, AUC skoru ve doğruluk gibi ölçütlere göre değerlendirilmiş ve sonuçları karşılaştırılmıştır.

Kontuk [11] çalışmasında haber metinlerini Doğal Dil İşleme tekniklerini kullanarak Çocukluk, Ergenlik ve Yetişkinlik yaş gruplarına göre sınıflandırmayı amaçlamıştır. Bu çalışmayı yaparken Doğal Dil İşleme için Zemberek kütüphanesini kullanmıştır. 3925 haber öğesini içeren bir veri kümesi kullanmıştır. Bu veri kümesinin bir kısmı eğitim için bir kısmı da test için kullanılmış ve sonuçlar karşılaştırılmıştır.

Çelik [12] çalışmasında sosyal medya platformlarından biri olan Twitter üzerinden kullanıcıların yaptıkları paylaşım ve yorumları içerisinde hakaret içeren kelime ya da cümle olup olmadığı konusunda Doğal Dil İşleme yöntemleriyle incelemiş, sonuçları sınıflandırma algoritmaları kullanarak karşılaştırmıştır. Sonuç olarak yapılan yorumlara göre duygu ve düşünce analizi ya da saldırgan veya hakaret içeren, tepkisi olmayan veya olumlu tepki içeren yorum tespiti hedeflenmiştir.

Öz [13] çalışmasında Türkçe dili için siber zorbalık tespitinde kullanılan doğal dil işleme yöntemleriyle makine öğrenmesi algoritmalarından bahsetmiştir. Bu konuda Doğal Dil İşleme için Google geliştiricileri tarafından geliştirilmiş BERT algoritmasının ise veri setine herhangi bir ön işlemeye gerek kalmadan kullanıldığından bahsetmiştir. Bu çalışmasında makine öğrenmesi sınıflandırma algoritmaları ile BERT algoritmasının performansları karşılaştırılmıştır.

Yapılan çalışmalar incelendiğinde siber zorbalık, hakaret vs. tespitini doğal dil işleme teknikleri ile analizleri yapılması ile elde edilen sonuçlar öğrenme algoritmalarına girdi olarak verilmiş ve sınıflandırma başarıları karşılaştırılmıştır.

3. Materyal ve Metot (Material and Method)

3.1. Sosyal medya (Social media)

Sosyal medya, kişilerin gerçek hayattaki ve sanal ortamlardaki bireylerle ilişkiler ve arkadaşlıklar kurabilmek, çevrimiçi içerikler paylaşabilmek ve çeşitli bağlantılar kurabilmek için kullandıkları

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

çevrimiçi ortamlardır. Bireyler sosyal medya mecralarını kendi ilgi ve gereksinimleri doğrultusunda iş bulma, arkadaş bulma, hobi edinme, bilgi paylaşma, içerik üretme ve üretilen içeriği paylaşma vb. amaçlarla kullanabilmektedir [14].

Sosyal medya platformları her zaman doğru amaçlar ve hedefler doğrultusunda kullanılmamaktadır. Bu platformlarda bireyler karşılarında bulunan kişilere hakaret içeren, aşağılayan, küçük düşüren, tehdit ifadeleri içeren vb. içerikleri ve mesajları gönderebilmektedir. Siber zorbalık olarak tanımlanan bu tehdit ve güvenlik riskleri sosyal medya platformlarında çoğu kullanıcıyı endişelendirmektedir.

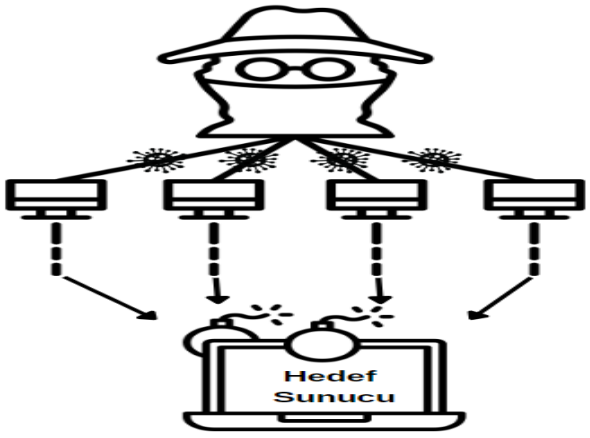
3.2. Siber zorbalık (Cyber bullying)

Dünya çapında sosyal medya ağlarının kullanımına artan güven, bilgi güvenliği için büyük endişe oluşturmaktadır [15]. Aynı zamanda sosyal medya platformları kullanıcılar ve kuruluşlar için çeşitli ciddi güvenlik riskleri ve tehditleri de oluşturabilmektedir [16]. Bu tehdit ve risklerden bazıları şunlardır:

- **Sosyal mühendislik saldırıları**: Bu saldırı türünde siber suçlu sahte sosyal medya hesapları kullanarak ve zaman içinde güven inşa ederek bireylerin kişisel bilgilerini ortaya çıkarmak için yoğun bir şekilde sosyal mühendisliği kullanmaktadır [17].

Şekil 3.1. Sosyal mühendislik saldırıları(Social engineering attacks)

- **Sosyal ağ altyapısı saldırıları:** Bu saldırı türünde saldırgan, kullanıcıların platform tarafından sağlanan hizmetlere erişimini kesmek amacıyla sosyal hizmeti sağlayan platforma saldırı başlatır. Bu saldırı türünü kullanan ve kullanıcıları doğrudan etkileyen en büyük saldırı DDoS'tur [15].



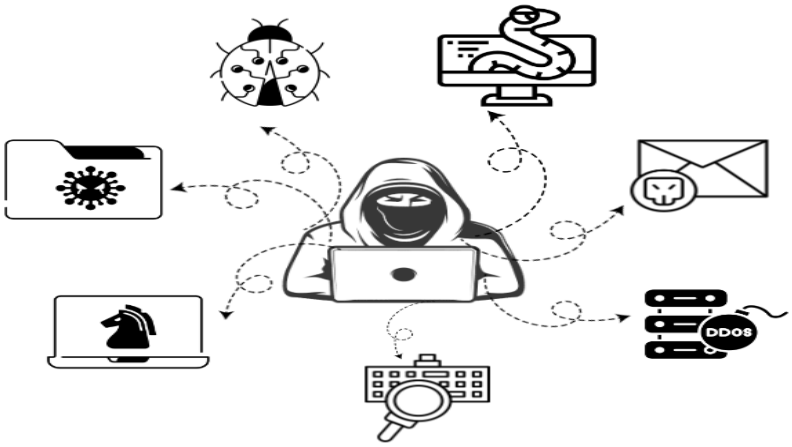
Şekil 3.2. Sosyal ağ altyapısı saldırıları (Social network infrastructure attacks)

- **Kötü amaçlı yazılım saldırıları:** Bu tür saldırılarda korsan, kontrolü ele geçirmek ve kullanıcının cihazını kullanarak DoS saldırısı başlatma, tuş vuruşlarını kaydetme, kimlik bilgilerinin, kredi kartı numarası veya banka bilgilerinin vb. çalınması gibi amaçları hedeflemektedir. Bu saldırıyı yaparken kullanıcılara sosyal ağlar üzerinden bağlantılar veya

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

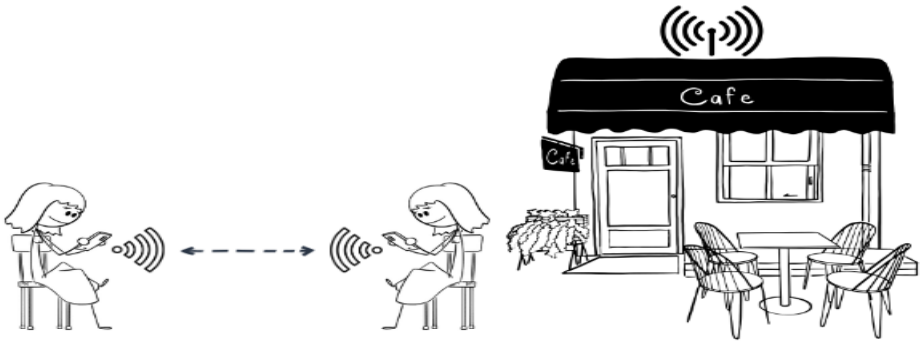
ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

resimler gönderirler ve sosyal ağlardan geldiği için kullanıcıların bu bağlantılara mutlaka tıklayacaklarını düşünürler. Bu bağlantılara tıklandıktan sonra saldırı gerçekleşmiş olur [15].



Şekil 3.3. Kötü amaçlı yazılım saldırıları (Malware attacks)

- **Kötü ikiz saldırıları:** Bu tür saldırılarda, bilgisayar korsanı ücretsiz, herkese açık, kafe, restoran veya umuma açık yerlerde bulunan wifi üzerinden gerçek kullanıcıyı taklit etmek için hesap oluşturmak üzere hedefin profilini kullanır. Bu profil ile gerçek kişinin arkadaşlarına ulaşır [15].



Şekil 3.4. Kötü ikiz saldırıları (Evil twin attacks)

- **Kimlik hırsızlığı:** Bu tür saldırılarda kullanıcıların kimlik bilgileri çalınır ve kullanıcının sosyal medya platformuna güvenli bir şekilde erişmek için kullanılır. Erişim sağlandıktan sonra önceden tasarlanmış saldırılar başlatılır [15].

Şekil 3.5. Kimlik hırsızlığı (Identity theft)

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

- **Siber zorbalık:** Siber zorbalık bu risk ve tehditlerin başında gelmektedir. Bir sosyal medya kullanıcısını mesajlarla ya da sosyal medya ağında sakıncalı içerik yayınlayarak hedef kullanıcıyı taciz etmek ya da korkutmak için tehdit etme ya da yıldırmanın bir yoludur [15]. Siber zorbalık, dijital teknolojiler kullanılarak yapılan zorbalıktır. Bilgi ve iletişim teknolojisi sayesinde kasıtlı siber zorbalık olayları ara sıra veya sürekli olarak meydana gelebilir. Siber zorbalık, içerik paylaşmak, iletişim kurmak veya hakaret içeren elektronik mesajlar göndermek gibi farklı şekillerde gerçekleştirilebilmektedir. Teknolojinin gelişmesi, insanların sosyal platformları çok aktif bir şekilde kullanmaları siber zorbalıkla ilgili sorunların da artmasına sebep olmuştur. Siber zorbalık, sosyal medya platformlarında, insanların birbiriyle iletişim kurmalarını sağlayan mesajlaşma ortamlarında, online oyun alanlarında yer alabilir [13].

Şekil 3.6. Siber zorbalık (Cyber bullying)

Siber zorbalık çeşitleri listelenmiş ve açıklanmıştır.

- **Karalama(Aşağılama):** Siber zorbalık türleri içerisinde en fazla görülen çeşittir. Bireyler veya topluluklar hakkında gerçek olmayan bilgileri gerçekmiş gibi söylemek veya bu doğru olmayan bilgiyi sosyal medya platformlarında paylaşmak şeklinde gerçekleştirilir. Daha çok ergenlik dönemindeki gençler arasında rastlanılır. Bu zorbalık türünü gençler arkadaşlarına karşı yapabildikleri gibi çevrelerinde bulunan öğretmenlerine ve diğer yetişkinlere karşı da gerçekleştirebilmektedirler [18].

Şekil 3.7. Karalama (Aşağılama) (Humiliation)

- **Kimliğe bürünme:** Bu siber zorbalık türünde zorba, zarar vermek istediği, zarar görmesini beklediği kişinin bilgilerine sahip olarak gerçek dışı bir profil oluşturur. Oluşturmuş olduğu bu sahte hesaptan zarar görmesini istediği kişinin ağzından onu çok zor durumda bırakacak paylaşımlarda bulunur. Zorbanın nihai amacı hedefindeki kişinin saygınlığının zarar görmesi, arkadaşları ve çevresindeki güvenilirliğinin ortadan kalkmasını sağlamaktır [13].

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Şekil 3.8. Kimliğe bürünme (Impersonation)

- **İfşalama:** Bireylerin izinleri olmadan, onlarla ilgili özel ve gizli bilgi veya belgelerini sosyal medya platformlarında herkese açık olacak şekilde paylaşma eylemine verilen addır. Bu siber zorbalık türünde zorbanın amacı mağdura şantaj yapmak, onu başkalarının gözünde zor durumda bırakmak, küçük düşürmektir [19].

Şekil 3.9. İfşalama (Disclosure)

- **Hile:** Bu siber zorbalık türü ifşalamaya benzer özellikler taşısa da ifşalamadan farklı özelliklere sahiptir. Bu türde zorba önce zarar vermek istediği kişinin kendisine güvenmesi için gerekli bütün çabaları sergiler. Karşısındaki kişinin güvenini temin ettikten sonra ondan çok özel görüntüler, belgeler ve bilgiler talep eder. Kişi kendisine zarar gelmeyeceğini düşündüğü, güvendiği kişi olan zorbaya en özel görüntülerini, belge ve bilgileri tereddüt etmeden gönderir. Ancak bir süre sonra zorba asıl işini gerçekleştirir ve mağdurun özel görüntü, belge ve görüntülerini herkesin kolayca ulaşabileceği sosyal medya platformlarında paylaşarak o kişinin zarar görmesini, utanmasını sağlar [18].

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Şekil 3.10. Hile (Cheat)

- **Taciz:** Siber taciz, internet üzerinden gerçekleştirilen, kişinin dijital platformlarda maruz kaldığı rahatsız edici, tehdit edici veya zarar verici davranışları içerir. Bu tür taciz biçimleri genellikle e-posta, sosyal medya, anlık mesajlaşma veya diğer çevrimiçi iletişim araçları aracılığıyla gerçekleştirilir. En belirgin özelliği bu eylemin tekrarlaması ve tehdit edici unsurları içermesidir. Yani bir kez yapılıp bırakılmaz karşıdaki kişi sürekli olarak rahatsız edilir. Bu duruma maruz kalan kişi açısından desteğe ihtiyaç duyulan bir zorbalık türüdür. Kişinin psikolojik destek alması gerekebilir [20].

Şekil 3.11. Taciz (Abuse)

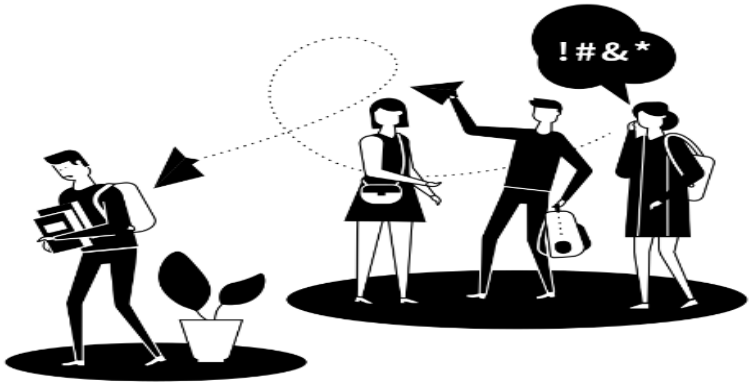
- **Siber takip:** Tacizle çok benzer özelliklere sahip olsa da siber takip zorbalık türü taciz zorbalık türüne göre daha ağır, sert ve zorlayıcıdır. Tacizde kişi tekrar tekrar rahatsız edilir ve tehdit edilir ancak siber takip de bu tehdit sadece söz de kalmaz. Zorbalığa uğrayan kişide her an başına bir şey gelecekmiş hissi çok bariz bir şekilde hissettirilir. Kişi gerçek anlamda korkar. Bu zorbalık türü daha çok kendini koruyamayan, rahat ifade edemeyen, yaş olarak küçük bireylere uygulanır. Tabi bu durumda siber takibe uğrayan kişi kendini koruyamadığı ve ifade edemediği için yaşadığı zorbalıktan olumsuz olarak etkilenmekte ve çevrelerinde olan her durumdan şüphelenmektedir [5].

Şekil 3.12. Siber takip (Cyber stalking)

- **Dışlama:** Siber zorbalık türlerinden dışlama türü, bireyleri sosyal medya platformlarında gruplardan çıkarma, whatsapp, telegram gibi anlık iletişim kurma, haberleşme ortamlarından çıkarma şeklinde gerçekleştirilir. Bu zorbalık türünde amaç karşıdaki kişinin özgüvenini kaybetmesini sağlamak, grup veya ortamlarda bulunan diğer kişilerin gözünde o kişi ile ilgili olumsuz izlenim yaratmaktır [19].

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808



Şekil 3.13. Dışlama (Exclusion)

- **Parlama:** Çevrimiçi platformlarda bireyler arasında gergin, tehditkar, küfür içerikli olan, kısa süreli devam eden tartışmalardır. Bu ortamın içerisine dahil olan bireyler sinirli ve gergindirler, bu durumdan kaynaklı karşılarındaki kişilere akıllarına gelen her türlü kötü içerikli mesajları gönderip tartışmayı alevlendirmektedirler. Ancak bu tartışmalar uzun sürmez [20].

Şekil 3.14. Parlama (Flare)

Ülkemizde de bu tehdit ve riskler söz konusudur. Bu nedenle bu konu ülkemiz için çok önemlidir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı konu ile ilgili koordinasyonu sağlamakta ve gerekli tedbirleri almaktadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinesinde rehber hazırlanmıştır. Hazırlanan rehber ihtiyaçların değişmesi ve gelişmesi, teknolojinin sürekli gelişmesi, şartların değişmesi nedeni ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler de göz önünde bulundurularak sürekli güncellenmektedir [21].

3.3. Öğrenme algoritmaları (Learning algorithms)

3.3.1. Extra trees algoritması (Extra trees algorithm)

Extra Trees (Ekstra Ağaçlar) algoritması 2006 senesinde Geurts ve arkadaşlarının geliştirdiği, budanmamış karar ağaçlarından oluşan bir topluluk öğrenme algoritmasıdır. Bu algoritma Random Forest (Rastgele Orman) algoritmasına benzer özelliklere sahiptir. Rastgele Orman Algoritmasında ağaçların bölünmesi esnasında en iyi bölünme için en iyi değişken seçimi yapılırken, Ekstra Ağaçlar Algoritmasında bölünme için rastgele değişken ve rastgele bir kesim noktası tercih edilmektedir. Bu yöntem sayesinde çok çeşitli ağaçlar ortaya çıkmakta ve bölünme adedi de düşmektedir. Bu durum modelin eğitim süresinin düşmesini de sağlamaktadır [22].

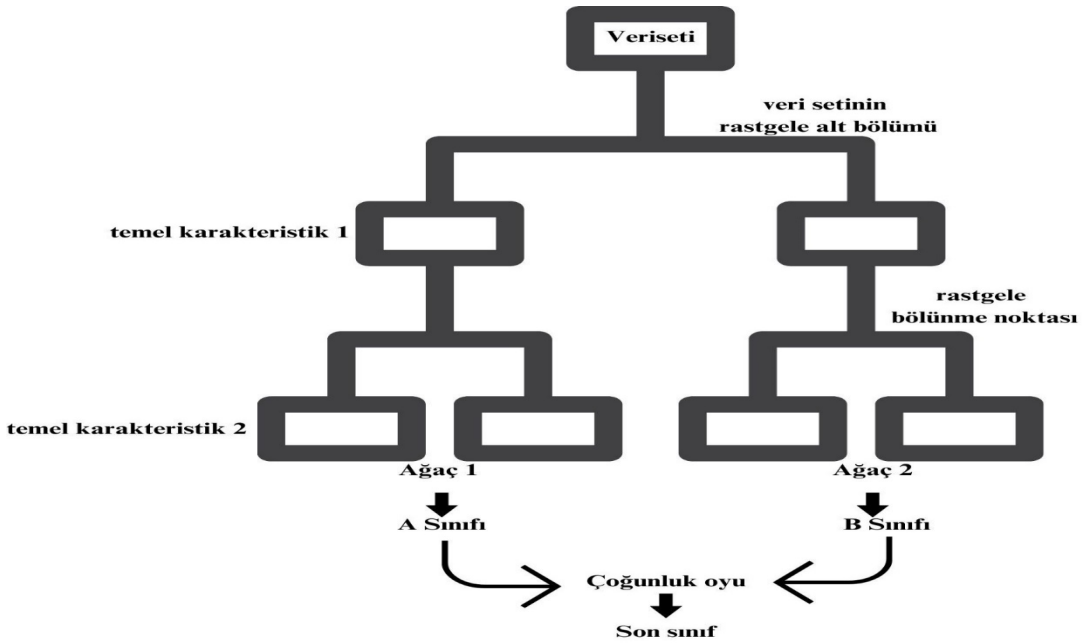
*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Extra Trees Algoritması Random Forest algoritmasına benzer bir çalışma sergilemesine rağmen karar ağaçlarını oluşturma biçiminde değişiklik vardır. Çalışma disiplini sınıflandırma sonucunda elde edilen veriyi alarak çoklu korelasyonu sonuçlarını kaldırılmış karar ağacı toplayan bir topluluk öğrenme tekniğidir [23].

Ekstra Ağaçlar Algoritması sayesinde bazı problemlerin çözümünde yaşanan karmaşıklık ve bu problemlerin çözümünde yer alan iş yükü hafifler. Bu algoritma problem çözümlerinde hızlı bir yöntemdir, ancak yüksek gürültülü büyük verilerin analizinde ve çözümünde performansı oldukça düşüktür. İstatistiksel olarak değerlendirildiğinde Ekstra Ağaçlar Algoritması çoğunlukla bias artışına ve varyansın düşmesine neden olur [24].

Şekil 3.15'te Ekstra Ağaçlar Algoritması Çalışma Yapısı gösterilmektedir.



Şekil 3.15. Ekstra ağaçlar algoritması çalışma yapısı (Extra trees algorithm working structure) [25]

3.3.2. XGBoost algoritması (XGBoost algorithm)

XGBoost olarak da adlandırılan Extreme Gradient Boosting, hem regresyon hem de sınıflandırma problemlerinde kullanılabilecek makine öğrenme tekniklerinden biridir. XGBoost (eXtreme Gradient Boosting), Gradient Boosting algoritmasının çeşitli ayarlarla optimize edilmiş yüksek performanslı bir versiyonudur. XGBoost, bir dizi karar ağacını kullanarak tahminlerde bulunur ve gradyan artırma çerçevesi üzerine inşa edilmiştir. Algoritmanın en önemli özellikleri yüksek tahmin gücüne ulaşabilmesi, aşırı uyumun önüne geçebilmesi, boş verileri yönetebilmesi ve bunları hızlı bir şekilde yapabilmesidir [26]. XGBoost algoritması, temelde Karar Ağaçları ve Gradyan Arttırma yöntemine dayanmaktadır [27].

Extreme Gradient Boosting, genellikle bir dizi karar ağacından yararlanarak zayıf tahmin modellerinin tahminlerini güçlendiren bir makine öğrenme yöntemidir. Modelin kademeli olarak oluşturulması yoluyla bu yöntem, herhangi bir türevlenebilir kayıp fonksiyonunun optimizasyonunu sağlayarak modeli genelleştirir. Daha az kaynakla daha iyi sonuçlar elde etmek için XGBoost'ta yazılım ve donanım optimizasyon yaklaşımları kullanılmıştır. Bazılarına göre en iyi karar ağacı tabanlı algoritma budur [28].

Belirli değişkenler göz önüne alındığında hedef değişkeni tahmin etmek için alternatif bir teknik olarak Chen ve Guestrin (2016) XGBoost'u sundu. Bu algoritmanın temel prensibi, D sınıflandırma ve regresyon ağaçlarını tek tek oluşturarak her yeni modelin bir önceki modelin artıkları kullanılarak eğitilmesine olanak sağlamasıdır. Başka bir deyişle yeni model, önceden eğitilmiş ağacın neden olduğu hataları düzelttikten sonra sonucu tahmin ediyor.

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

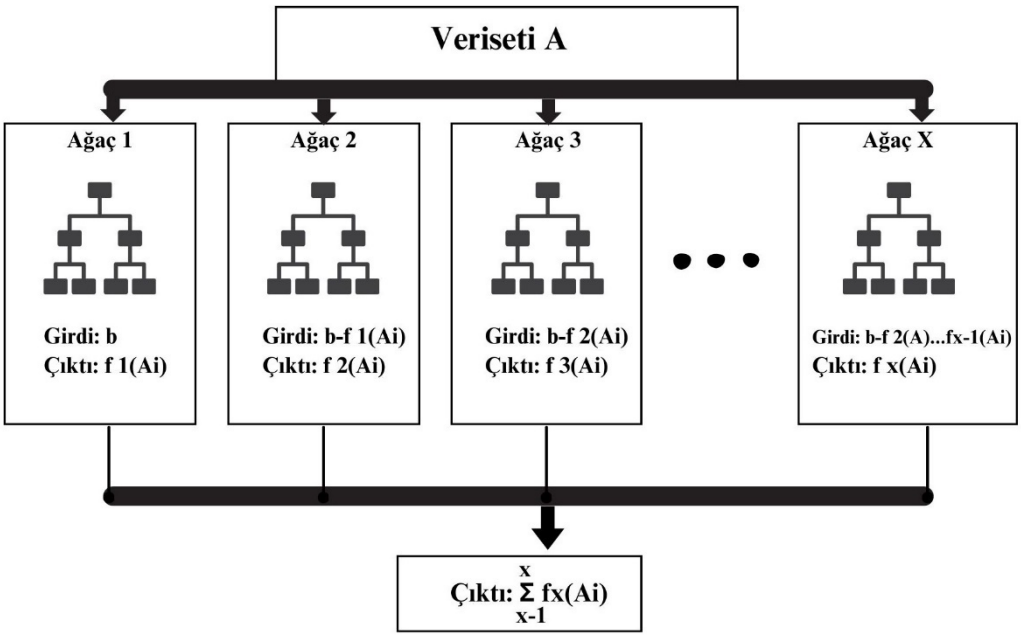
ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Aynı temelde, XGBoost ve degrade artırmanın her ikisi de çalışır. Ayrıştıkları nokta ayrıntılardır. Çeşitli metodolojiler kullanan XGBoost, daha yüksek tahmin başarısı sergiliyor ve büyük verileri işleyecek şekilde tasarlandı.

XGBoost'u Gradient Boosting'den ayıran ana konular aşağıdadır.

- Düzenleme
- Budama
- Boş değerlerle çalışma
- Sistem optimizasyonu

Şekil 3.16'da XGBoost (Extreme Gradient Boosting) temel yapısı gösterilmektedir.



Şekil 3.16. XGBoost algoritması çalışma yapısı (XGBoost algorithm working structure) [28]

3.4. Model performans metrikleri (Model performance metrics)

3.4.1. Doğruluk (Accuracy)

Doğruluk (Accuracy) değeri, modelde doğru olarak sınıflandırılan pozitif ve negatif sonuçların(TP+TN) toplam veri sayısına (TP+TN+FP+FN) oranı ile bulunmaktadır [29].

$$\text{Doğruluk (Accuracy)} = \frac{TP(True\ Positive)+TN(True\ Negative)}{TP(True\ Positive)+TN(True\ Negative)+FP(False\ Positive)+FN(False\ Negative)}$$

3.4.2. Duyarlılık (Recall)

Duyarlılık, gerçek değeri pozitif olarak sınıflandırılan tahminlerin (TP) sayısının toplam gerçek pozitif sınıf sayısına yani gerçek değeri pozitif ve yanlış negatif tahmin sayısına (TP+FN) bölünmesiyle hesaplanır. Bu değere recall, sensitivity veya gerçek pozitif oran (TPR) denir. Duyarlılık, gerçek değeri pozitif olan değerlerin ne kadarının pozitif olarak etiketlendiğini gösterir. Gerçek pozitif sayısı ne kadar fazla olursa duyarlılık değeri artarken yanlış negatif sayısı ne kadar fazla olursa bu sefer de duyarlılık değeri azalır. En kötü duyarlılık değeri 0 iken, en iyi duyarlılık değeri ise 1'dir [30].

$$\text{Duyarlılık (Recall)} = \frac{TP(True\ Positive)}{TP(True\ Positive)+FN(False\ Negative)}$$

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

3.4.3. Kesinlik (Precission)

Kesinlik (Precision), gerçek değeri pozitif olup pozitif olarak sınıflandırılan tahmin sayısının (TP) tahmin değeri pozitif olan tüm gözlemlere (TP+FP) oranıdır. En kötü kesinlik değeri 0 iken, en iyi kesinlik değeri 1 değerine sahiptir [31].

$$\text{Kesinlik (Precision)} = \frac{\boldsymbol{TP(True\ Positive)}}{\boldsymbol{TP(True\ Positive)+FP(False\ Positive)}}$$

3.4.4. F1 skoru (F1 score)

F1 skoru, modelin kesinlik(precision) ve duyarlılık(recall) değerlerinin harmonik ortalaması alınarak hesaplanır. F1 skoru 0 ile 1 arasında değer almaktadır. F1 skoru değeri 1'e yaklaştıkça kategorizasyon sonuçları da o kadar doğru olur [32].

$$\text{F1 Skoru} = 2*\frac{\boldsymbol{Kesinlik(Precision)*Duyarlılık(Recall)}}{\boldsymbol{Kesinlik(Precision)+Duyarlılık(Recall)}}$$

3.4.5. Ortalama mutlak hata (MAE) değeri (Mean absolute error (MAE) value)

Ortalama Mutlak Hata (MAE) veri setinde bulunan gerçek değer ile bir makine öğrenmesi algoritması kullanılarak tahmin edilen değer arasındaki farkların mutlak değerlerinin toplamı sonucunun örnek sayısına bölünmesiyle elde edilen değerdir. Başka bir ifadeyle veri setindeki gerçek değerler ile tahmin edilen değerler arasındaki hataların mutlak değerlerinin ortalamasıdır. Ortalama Mutlak Hata (MAE) 0 ile ∞ arasında değerler alır. MAE değerinin düşük olması istenen ve beklenen durumdur. MAE değerinin 0'a yaklaşması modelin performansının oldukça iyi olduğu anlamı taşımaktadır [33].

3.4.6. Ortalama kare hatası (MSE) değeri (Mean square error (MSE) value)

Ortalama Kare Hatası (MSE), tahmin edilen sonuçların gerçek değerlerden ne kadar farklı olduğuna dair vermiş olduğu mutlak sayıdır. Başka bir deyişle gerçek değerler ile tahmin edilen değerler arasındaki farkların karesinin ortalamasıdır. Ortalama Kare Hatası (MSE), bir makine öğrenmesi algoritmasının, tahmin etme performansını ölçer ve aldığı değer daima pozitiftir. Algoritmanın MSE değeri ne kadar sıfıra yakın ise tahmin edilen sonuçların o kadar iyi bir performans göstermiş olduğu anlamına gelir [34].

3.4.7. R kare değeri (R squared value)

R-kare değeri, bir regresyon modelinin uyum iyiliğinin bir ölçüsüdür. R-kare değeri olarak elde edilen sonuç ne kadar yüksek olursa modelin verilere daha iyi uyduğu sonucuna ulaşılır. R-karenin alabileceği değerler 0 ile 1 arasında değişir. 0 değeri, modelin verilere uymadığını gösterirken, 1 değeri modelin verilere tamamen uyduğunu gösterir, ancak R-kare değerinin tam 1 olmasının uygulamada mümkünlüğü yoktur [33].

3.4.8. Karışıklık matrisi (Confusion matrix)

Karışıklık matrisine (Confusion Matrix) hata matrisi de denilmektedir. Orijinal veri seti eğitim veri seti ve test veri seti olarak ikiye ayrılır. Eğer sınıflandırma yapılacaksa eğitim seti ile makine öğrenimi gerçekleştirilir. Makine öğrenimi gerçekleştirildikten sonra elde edilen model ile tahmini sınıf değerleri oluşturulur. Makine öğrenimi ile tahmin edilen değerler, makinenin daha önce öğrenmediği test veri seti olarak ayrılan set ile karşılaştırılmaktadır. Tahmini sınıf değerleri ile orijinal test değerlerinin karşılaştırılması için bir karışıklık matrisi oluşturulur ve sonuçlar değerlendirilir [29].

3.4.9. ROC eğrisi (ROC curve)

ROC eğrisi, bir modelin farklı eşik değerlerinde sağladığı duyarlılık ve özgüllük oranlarını görselleştirir [10]. ROC eğrisi, bir olasılık eğrisidir ve altında kalan alan olan AUC ayrılabilirliğin ölçüsünü göstermektedir. Eğrinin altında kalan alan ne kadar fazla olursa sınıflar arasındaki ayırt etme performansı da aynı oranda artmaktadır.

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

3.5. Veri Setinin Oluşturulması ve Ön İşleme (Creating the dataset and Preprocessing)

Araştırmada kullanılacak veri seti, erişime açık paylaşım sitesi Kaggle'dan [35] temin edilmiştir. Bu veri seti içeriği sosyal medya platformlarından biri olan Twitter platformunda yer alan 11114 adet Türkçe yorumdan oluşmaktadır. Verisetinde yer alan yorumlarda siber zorbalık içerip içermediği aranmaktadır.

Bu çalışmada Doğal Dil İşleme süreçleri uygulanmıştır. Bunun için Python programlama dili için geliştirilmiş, Doğal Dil İşleme kütüphanelerinden "nltk(natural language toolkit)" kütüphanesi kullanılmıştır. Bu kütüphane, dil işleme süreçleri için farklı özellik, fonksiyon ve araçlar içerir [12]. Bu kütüphane içerisinde yer alan corpus paketinden stopwords özelliği ile yorum içerisinde yer alan etkisiz, önemsiz kelimeler anlaşılmıştır. Bu işlemden sonra kelimeleri köklerine ayırabilmek için "nltk" kütüphanesi içerisindeki stem paketinden WordNetLemmatizer özelliği programda kullanılmıştır.

Araştırmada "Count Vectorizer" sınıfı kullanılarak yorumlardaki sözcük veya simge sayımlarından oluşan bir matris oluşturulmuştur. Bu sınıf sayesinde metinler varsayılan olarak küçük harfe dönüştürülür ve utf 8 kodlaması kullanılır. Dönüştürülen matris normalleştirilmiştir.

Doğal Dil İşleme süreçleri tamamlanan veri seti sınıflandırma algoritmalarına giriş verisi olarak verilmiş ve elde edilen değerler karşılaştırılmıştır.

4. Araştırma Bulguları (Research Findings)

Bu araştırmada elde edilen sonuçlar şekiller ve tablolarla verilmiştir.

- **XGBoost sınıflandırma algoritması sonuçları(XGBoost classification algorithm results)**

  Kullanılan veriseti XGBoost sınıflandırma algoritmasına giriş verisi olarak verildikten sonra elde edilen sonuçlar incelenmiştir. Tabloda TP (True Pozitive-Doğru Pozitif) 1149, TN (True Negative-Doğru Negatif) 700, FP (False Positive-Yanlış Pozitif) 65, FN (False Nagative- Yanlış Negatif) 309 olarak elde edilmiştir. Bu sonuçlarda araştırmanın doğruluk (accuracy)değeri %83,18 oranında doğru tahminde bulunduğunu göstermektedir. Duyarlılık (Recall)değeri araştırmada %94,65 olarak ölçülmüştür. Kesinlik (Precision) değeri bu araştırmada %78,81 olarak elde edilmiştir. F1 Skoru değeri olarak %86 sonucuna ulaşılmıştır. Ortalama Mutlak Hata (MAE) Değeri ile Ortalama Kare Hatası (MSE) Değeri araştırmada %16,82 olarak elde edilmiştir. Son olarak R Kare Değeri %32,13 olarak elde edilmiştir.

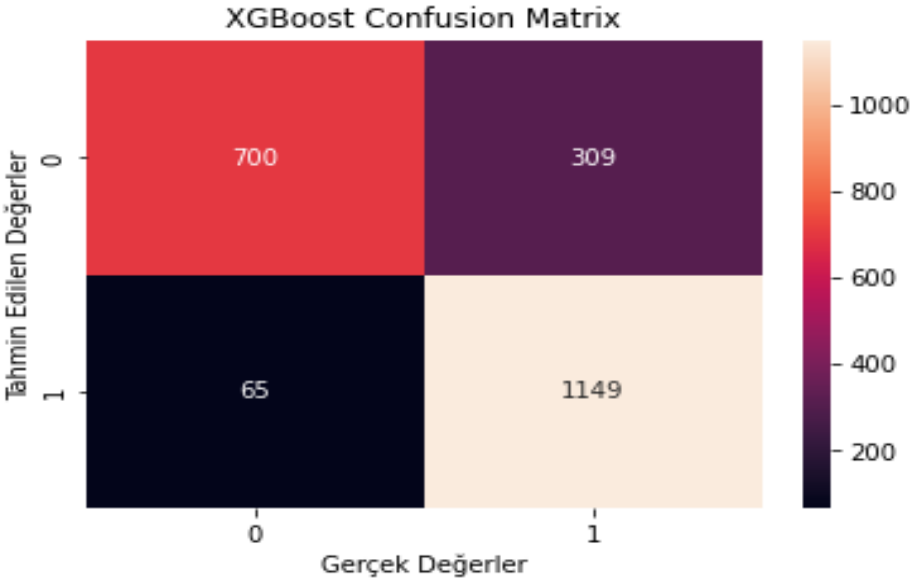
Tablo 4.1. XGBoost sınıflandırma algoritması sonuçları (XGBoost classification algorithm results)

Ölçütler (Metrics)	Hesaplanan Değerler (XGBoost)
Doğruluk (Accuracy)	%83.18
Duyarlılık (Recall)	%94.65
Kesinlik (Precision)	%78.81
F1 Skoru	%86.0
Ortalama Mutlak Hata (MAE) Değeri	%16.82
Ortalama Kare Hatası (MSE) Değeri	%16.82
R Kare Değeri	%32.13

Şekil 4.1'de XGBoost sınıflandırma algoritması sonucunda elde edilen karışıklık matrisi verilmiştir.

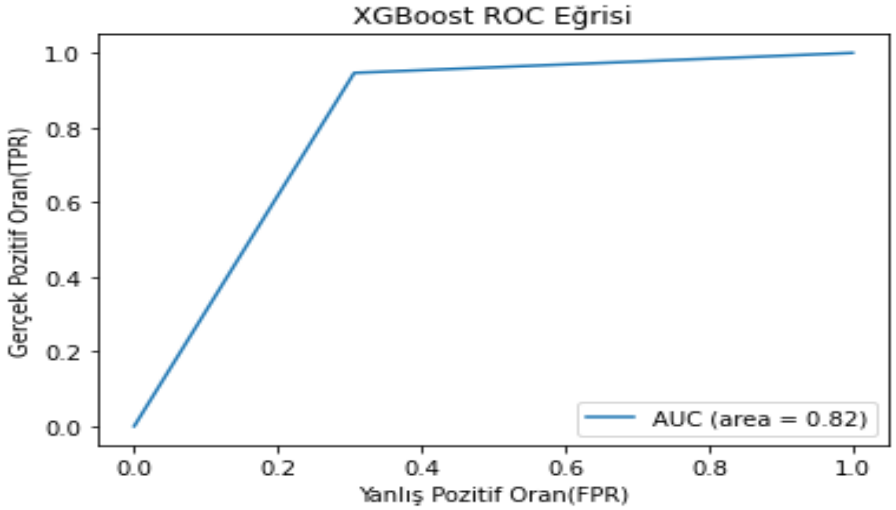
*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808



Şekil 4.1. XGBoost algoritması karışıklık matrisi (XGBoost algorithm confusion matrix)

XGBoost algoritmasına ait ROC eğrisi ise Şekil 4.2'de gösterilmiştir. XGBoost algoritmasının Roc eğrisinde AUC değeri 0,82 olarak belirlenmiştir.



Şekil 4.2. XGBoost algoritması ROC eğrisi (XGBoost algorithm roc curve)

- **Ekstra trees sınıflandırma algoritması sonuçları(Extra trees classification algorithm results)**

Kullanılan veriseti Ekstra sınıflandırma algoritmasına giriş verisi olarak verildikten sonra elde edilen sonuçlar incelenmiştir. Tabloda TP (True Pozitive-Doğru Pozitif) 1107, TN (True Negative-Doğru Negatif) 826, FP (False Positive-Yanlış Pozitif) 107, FN (False Nagative- Yanlış Negatif) 183 olarak elde edilmiştir. Bu sonuçlarda araştırmanın doğruluk (accuracy) değeri %86,95 oranında doğru tahminde bulunduğunu göstermektedir. Duyarlılık (Recall) değeri %91,19 olarak ölçülmüştür. Kesinlik (Precision) değeri araştırmada %85,81 olarak elde edilmiştir. F1 Skoru değeri olarak %88,42 sonucuna ulaşılmıştır. Ortalama Mutlak Hata (MAE) Değeri %13,05, Ortalama Kare Hatası (MSE) Değeri ise %13,05 olarak elde edilmiştir. Son olarak R Kare Değeri % 47,37 olarak hesaplanmıştır. Ekstra Trees algoritmasının Roc eğrisinde AUC değeri 0,87 olarak belirlenmiştir.

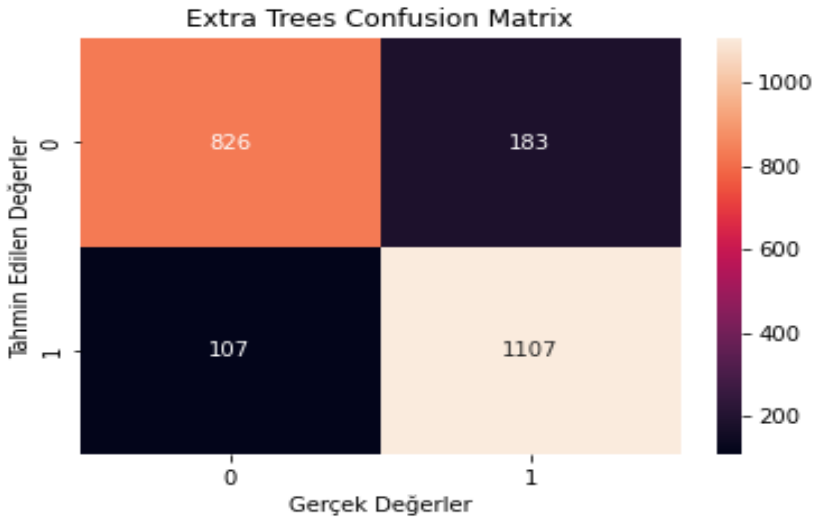
*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Tablo 4.2. Ekstra trees sınıflandırma algoritması sonuçları (Extra trees classification algorithm results)

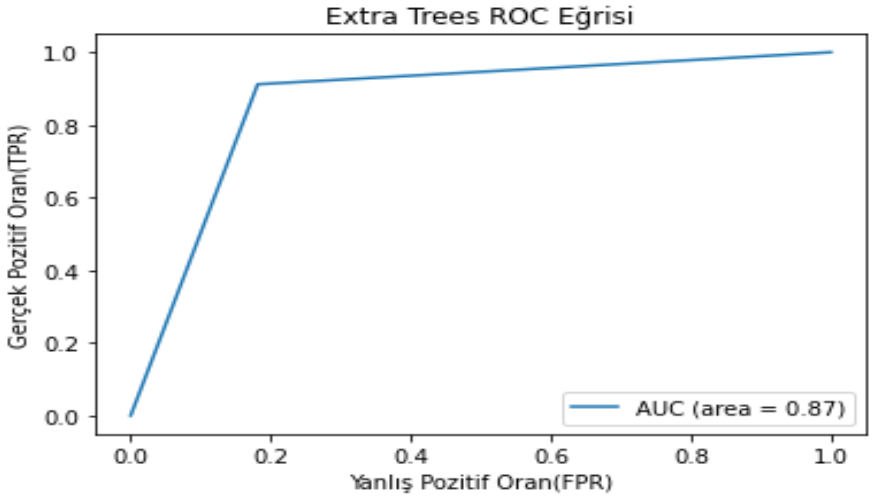
Ölçütler (Metrics)	Hesaplanan Değerler (Extra Tree)
Doğruluk (Accuracy)	%86.95
Duyarlılık (Recall)	%91.19
Kesinlik (Precision)	%85.81
F1 Skoru	%88.42
Ortalama Mutlak Hata(MAE) Değeri	%13.05
Ortalama Kare Hatası(MSE) Değeri	%13.05
R Kare Değeri	%47.37

Şekil 4.3'te Ekstra trees algoritması sonucunda elde edilen karışıklık matrisi verilmiştir.



Şekil 4.3. Ekstra trees algoritması karışıklık matrisi (Extra trees algorithm confusion matrix)

Ekstra trees algoritmasına ait ROC eğrisi ise Şekil 4.4'te verilmiştir.



Şekil 4.4. Ekstra trees algoritması ROC eğrisi (Extra trees algorithm ROC curve)

5. Tartışma (Discussion)

Yapılan bu çalışmada veri setine uygulanan doğal dil işleme yöntemlerinden sonra elde edilen veri öğrenme algoritmalarına girdi olarak verilmiş ve araştırma bulgularında verilen sonuçlar elde edilmiştir.

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Sonuçlar incelendiğinde Doğruluk değeri XGBoost algoritmasında %83,18 olarak elde edilirken Extra trees algoritmasında %86,95 olarak bulunmuştur. Duyarlılık değeri XGBoost algoritmasında %94,65 iken Ekstra trees algoritmasında %91,19'dur. XGBoost algoritmasının kesinlik değeri %78,81 olarak elde edilmişken Ekstra trees algoritmasının kesinlik değeri %85,81 olarak bulunmuştur. F1 skoru değeri olarak XGBoost algoritmasında değer %86, Ekstra trees algoritmasında ise %88,42'dir. Ortalama mutlak hata (MAE) değeri ve ortalama kare hatası (MSE) değeri XGBoost algoritmasında %16,82 iken Ekstra trees algoritmasında %13,05 elde edilmiştir. R kare değeri ise XGBoost algoritmasında %32,13, Ekstra trees algoritmasında %47,37 olarak ölçülmüştür. Ayrıca XGBoost algoritmasının AUC değeri 0,82 iken Ekstra trees algoritmasının AUC değeri 0,87 olarak elde edilmiştir.

Algoritmalardan elde edilen sonuçlara bakıldığında doğruluk, kesinlik, F1 skoru değeri, ortalama mutlak hata değeri, ortalama kare hatası değeri, r kare değeri ve AUC değerleri Ekstra trees algoritmasında XGBoost algoritmasına göre daha başarılı sonuçlar vermiştir.

6. Sonuç (Results)

Çalışmada erişime açık paylaşım sitesi Kaggle'dan elde edilen veriseti üzerinde, doğal dil işleme tekniklerinden stopwords, wordnet lemmatizer, count vectorizer ve tfidf transformers işlemleri uygulanmıştır. Bu uygulamalar neticesinde veriler sayısallaştırılmıştır yani bilgisayarın anlayabileceği şekle dönüştürülmüştür. Elde edilen model öğrenme algoritmalarına girdi olarak verilip modelin bir bölümü test verisi, bir bölümü ise eğitim verisi olarak kullanılmıştır. Sınıflandırma algoritmaları çalıştırıldığında modelin başarı oranlarına bakılmıştır.

Yapılan araştırma sonucunda XGBoost algoritması ile Ekstra Trees algoritmasından elde edilen veriler karşılaştırılmıştır. Yapılan karşılaştırma sonucunda Ekstra Trees algoritmasından elde edilen veriler doğruluk, kesinlik, F1 skoru, ortalama mutlak hata değeri, ortalama kare hatası değeri R kare değeri ve AUC değeri bakımından XGBoost algoritmasına göre daha başarılı sonuçlar vermiş ve dolayısıyla daha başarılı olmuştur.

Gelecekteki çalışmalarda yapılan çalışmada kullanılan verisetindeki yorum sayısı arttırılarak ve farklı öğrenme algoritmaları kullanılarak, daha fazla veriyle daha fazla algoritmadan elde edilecek sonuçlar karşılaştırılarak daha geniş kapsamlı bir çalışma yapılabilir.

Kaynaklar (References)

[1] A.İ. Kesici, S. Mert, D.M. Gezgin, Siber Dünyanın Karanlık Yüzü: Güvenlikten Zorbalığa Modern Problemler, Balkan 10th International Conference On Applied Sciences (2024) 6-7.

[2] We Are Social Meltwater, Digital 2023 Global Overview Report (2023) 213.

[3] E.S. Dinç, Sosyal Medya Ortamlarında Siber Zorbalik: Lise Öğrencilerinin Siber Zorbalık Deneyimlerinin İncelenmesi, Electronic Journal of New Media 4(1) (2020) 24–39.

[4] O. Sevli, S. Sezgin, Sosyal Medya Paylaşımlarında Siber Zorbalığın Tespiti ve Kategorizasyonuna Yönelik Makine Öğrenmesine Dayalı Bir Sınıflandırma, Burs 3rd International Scientific Research Congress, 2022.

[5] E. Yazğılı, Makine Öğrenmesi Yöntemleri Kullanarak Siber Zorbalık Tespiti, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Yazılım Mühendisliği Anabilim Dalı, Fırat Üniversitesi (2021).

[6] Ç. Ballı, Doğal Dil İşleme İle Türkçe İçerikli Paylaşımlardan Sosyal Medya Kullanıcılarının Duygu Analizi, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Ankara Üniversitesi (2021).

[7] A. Delibaş, Doğal Dil İşleme İle Türkçe Yazim Hatalarinin Denetlenmesi, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul Teknik Üniversitesi (2008).

[8] İ. Yelmen, Doğal Dil İşleme Yöntemleriyle Türkçe Sosyal Medya Verileri Üzerinde Duygu Analizi, Yüksek

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doğuş Üniversitesi (2016).

[9] R.M. Dolar, E-Ticaret Ürünlerindeki Türkçe Kullanıcı Yorumlarının Oyunlaştırma, NLP ve Makine Öğrenmesi Teknikleri İle Sınıflandırılması, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul Teknik Üniversitesi (2021).

[10] B.F. Kesgin, Offensive Language Detection In Turkish Language By Using NLP, Yüksek Lisans Tezi, Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Bahçeşehir Üniversitesi (2023).

[11] R. Kontuk, NLP Kullanılarak Haberlerin Yaş Gruplarına Göre Sınıflandırılması, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul Ticaret Üniversitesi (2020).

[12] C.B. Çelik, Sosyal Medya Platformlarında Yapay Zeka Ve Makine Öğrenim Tekniklerini Kullanarak, Doğal Dil İşleme İle Hakaret İçeren Cümle Tespiti ve Duygu Analizinin Ölçülmesi, Yüksek Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul Nişantaşı Üniversitesi (2023).

[13] F. Öz, Çift Yönlü Enkoder Transformatör Tabanlı Siber Zorbalık Tespiti Derin Öğrenme Modeli Geliştirilmesi, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Yazılım Mühendisliği Anabilim Dalı, Manisa Celal Bayar Üniversitesi (2022).

[14] D. Kantar, Sosyal Medya Uygulamalarında Dijital Mahremiyet Farkındalığının Ölçülmesi, Yüksek Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler Anabilim Dalı, Hitit Üniversitesi (2023).

[15] E. Etuh, F.S. Bakpo, E.A.H, Social Media Network Attacks and their Preventive Mechanisms: A Review, Computer Science & Information Technology (CS & IT) (2021) 59–74.

[16] R.S. Kunwar, P. Sharma, Social media: A new vector for cyber attack, Proceedings - 2016 International Conference on Advances in Computing (2016).

[17] K. Thakur, T. Hayajneh, J. Tseng, Cyber Security in Social Media: Challenges and the Way Forward, IEEE World Congress On Services 2019 (2019) vol. 21, no. 2, pp. 41–49.

[18] E. Öztürk, Cyberbullying Detection Using Text Classification For Turkish Language, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Çukurova Üniversitesi (2019).

[19] C. Kacar, Sosyal Medya Kullanan Bireylerin Siber Zorbalık Deneyimlerinin İncelenmesi, Yüksek Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Hemşirelik Anabilim Dalı, Haliç Üniversitesi (2023).

[20] B. Öztürk, Türkiye'deki Y Kuşağı Mensubu Bireylerin Siber Zorbalık ve Siber Mağduriyet Algıları: Bir Alan Çalışması, Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Sosyoloji Anabilim Dalı, Marmara Üniversitesi (2023).

[21] Cumhurbaşkanlığı Genelge, 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi (2019).

[22] E. Gümüştaş, Kayıp Gözlem İçeren Dengesiz Veri Setlerinin Topluluk Öğrenme Algoritmaları İle Sınıflandırılması, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstatistik Anabilim Dalı, Mimar Sinan Güzel Sanatlar Üniversitesi (2019).

[23] V. Bayırbağ, H. Bakır, Çalışan Yıpranması Tahmin Etmek için Hiper Parametresi Ayarlanmış Makine Öğrenme Algoritmaların Kullanılması, 2nd International Conference on Scientific and Academic Research (2023) vol. 1, pp. 466–471.

[24] M. Öztürk, Birinci Servikal Vertebranın Antropometrik Ölçümleri İle Makine Öğrenme Algoritmaları Kullanılarak Cinsiyet Tayini Üzerine Bir Çalışma, Yüksek Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Anatomi Anabilim Dalı, Karabük Üniversitesi (2021).

[25] Y. Lou, Y. Ye, W. Zuo, M. Strong, Individualized Empirical Baselines For Evaluating The Energy Performance of Existing Buildings, Science and Technology for the Built Environment (2023) vol. 29, no. 1, pp. 19–33.

[26] Y. Şener, Predicting Participant Risk Profiles In Private Pension Funds Using Machine Learning Techniques, Yüksek Lisans Tezi, Lisansüstü Eğitim Enstitüsü, Büyük Veri Analitiği ve Yönetimi Anabilim Dalı,

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr

ISSN: 2618-6055 / 8, (1), 8 – 25, 2024
DOI: 10.62301/usmtd.1462808

Bahçeşehir Üniversitesi (2023).

[27] S. Diler, Veri Kalitesinin Bozulduğu Durumlarda Veri Madenciliği Sınıflandırma Algoritmalarının Performanslarının Karşılaştırılması, Doktora Tezi, Fen Bilimleri Enstitüsü, İstatistik Anabilim Dalı, Van Yüzüncü Yıl Üniversitesi (2023).

[28] E. Çekiç, Increasing Firm's Efficiency With Machine Learning Algorithms: An Application In The Logistics Industry, Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, İşletme(İngilizce) Anabilim Dalı, Marmara Üniversitesi (2023).

[29] G. Kaba, Hastalık Tahmininde Makine Öğrenmesi Sınıflandırma Algoritmalarının Karşılaştırılması ve Bootstrap Metodu Kullanımı, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstatistik Anabilim Dalı, İstanbul Ticaret Üniversitesi (2022).

[30] A. Acet, SVM, NB, KNN, ADABoost ve Random Forest Sınıflandırma Algoritmaları Kullanılarak Meme Kanserinin Tahmini, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İnönü Üniversitesi (2022).

[31] A.G. Güneş, Tele-Bankacılık İçin Potansiyel Müşteri Tahmininde Sınıflandırma Algoritmalarının Performans analizi, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Kocaeli Üniversitesi (2023).

[32] M.T. Sattı, Urdu News Categorization Using Machine Urdu News Categorization Using Machine Learning Approaches, Yüksek Lisans Tezi, Lisansüstü Programları Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Beykoz Üniversitesi (2023).

[33] E.N.H. Kırğıl, Makine Öğrenmesi Teknikleriyle Yazılım Uyum Metriklerinin Tahmini, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Başkent Üniversitesi (2022).

[34] S. Beyaztoprak, Kuruluşların Enerji Talebi Analizi ve Tahmini, Yüksek Lisans Tezi, Cerrahpaşa Lisansüstü Eğitim Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, İstanbul Üniversitesi (2019).

[35] Kaggle, <https://www.kaggle.com/code/moneyshot495/fork-of-do-al-dil-leme-metotlar-ile-siber-zorba/input?select=tweetset.csv.>, 2024 (accessed 24.06.2024)

*Sorumlu Yazar/Corresponding Author: yl2230138902@ogr.sdu.edu.tr