T.C
FIRAT ÜNİVERSİTESİ
YAZILIM MÜHENDİSLİĞİ

SOSYAL AĞLARDA SİBER ZORBALIK TESPİTİNİN MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE BELİRLENMESİ

BİTİRME TEZİ

15290012- Edanur ÖZDEMİR
15290056-Şule ATMACA

Danışman: Prof. Dr. Bilal ALATAŞ

ELAZIĞ
MAYIS-2019

ÖNSÖZ

Bu çalışmada makine öğrenmesi yöntemlerinin siber zorbalık tespiti üzerinde etkilerinin belirtilmesi amaçlanmıştır. Tez konusunu seçerken isteklerimizi göz önünde bulundurup, araştırma ve deneysel çalışmalarımızda bilgi, birikim ve tecrübeleri ile bize yol gösteren tez danışmanımız Prof. Dr. Bilal ALATAŞ ‘a teşekkür ederiz.

Şule ATMACA
Edanur ÖZDEMİR
ELAZIĞ-2019

İÇİNDEKİLER

ÖZET

Gelişen teknoloji yenilik ve kolaylıklarla beraber bir takım sorunları da beraberinde getirmiştir. Bu sorunlardan en önemlisi ise siber zorbalıktır. Siber zorbalık çoğunlukla sosyal ağlar üzerinden yapılmaktadır. Bu sosyal ağlarda insanlar sahte hesaplar kullanarak suç teşkil eden birçok faaliyette bulunmakta, nefret söylemleri, tehdit ve rencide edici birçok mesaj ve yorum yazmaktadır. Özellikle çocuklar ve gençler yetişkinlere göre sosyal ağlarda daha çok vakit geçirdiğinden bu gelişmeleri yakından takip eden ve en çok etkilenen gruptur. Siber zorbalığa maruz kalan kişilerde bir takım psikolojik sorunlar ve intihara varan etkiler oluşabilmektedir. Ayrıca sosyal ağları daha sık kullanan insanların, az kullanan insanlardan daha fazla siber zorbalığa eğilimlerinin olduğu veya siber zorbalığa maruz kaldığı tespit edilmiştir. Bununla birlikte, geleneksel zorbalıkta kullanılan yöntemler çoğunlukla bilinirken, siber zorbalıkta kullanılan yöntemler sürekli olarak değişmekte ve tespiti zorlaşmaktadır. Siber zorbalığın tespitinin zor olması ve tespiti halinde ne yapılacağının tam olarak bilinememesi sebebiyle insanlar daha rahat bir şekilde bu zorbalığı gerçekleştirmektedir. Bu çalışmada, savunmasız kişilere karşı sosyal ağlarda gerçekleştirilen siber zorbalığın tespiti için nitelik seçme algoritması olarak Chi2 algoritması ve farklı sınıflandırma algoritmaları kullanılarak sonuçlar karşılaştırılmıştır. Çalışmanın deneysel sonuçları, siber zorbalık tespiti için SGD sınıflandırıcısının %92,67 doğruluk oranı ile en iyi yöntem olduğunu kanıtlamıştır.

Anahtar Kelimeler: Siber Zorbalık, Sosyal Ağlar, Zorbalık tespiti, Siber mağdur, Saldırgan

SUMMARY

Developing technology has brought some problems with innovations and facilities. The most important of these problems is cyberbullying. Cyber bullying is mostly done through social networks. In these social networks, people are engaged in a number of criminal activities using false accounts, writing hate speech, threatening and offensive messages and comments. As children and young people spend more time on social networks than adults, it is the most affected group that closely follows these developments. Persons exposed to cyber bullying may have some psychological problems and suicidal effects. It has also been found that people who use social networks more often tend to have more cyber bullying than people who use less, or they are exposed to cyber bullying. However, while the methods used in conventional bullying are generally known, the methods used in cyber bullying are constantly changing and difficult to detect. Cyber bullying is difficult to detect and can not be known exactly what to do in case of determination of this bullying people are more comfortable. In this study, Chi2 algorithm as a feature selection algorithm for the detection of cyber bullying in social networks against vulnerable persons and different classification algorithms were compared. The experimental results of the study proved to be the best method with the accuracy of 92.67% of the SGD classifier for the detection of cyberbullying.

Key Words: Cyber Bullying, Social Networks, Bullying detection, Cyber victim,

Attacker

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR

Chi2	: Chi-Square
RBF	: Radial Basis Function
SGD	: Stochastic Gradient Descent
SMO	: Sequential Minimal Optimization
KNN	: K Nearest Neighborhood
LWL	: Locally Weighted Learning
RBFN	: Radial Basis Function Network

1. GİRİŞ

Saldırganlık, tarih boyunca en ilkel topluluklardan, en uygar toplumlara varıncaya kadar dünyanın çeşitli yerlerinde karşılaşılan bir sorun olmakla birlikte, çağımızda daha da belirginleştiği, yaygınlaştığı ve şiddetli bir hal aldığı görülmektedir [1]. Zorbalık, saldırganlığı da içeren bir kavram olmasına rağmen bir davranışın zorbalık olarak tanımlamak için sadece saldırganlık özelliği taşımasına gerek yoktur. Aynı zamanda sürekli olması, taraflar arasındaki güç dengesinin eşit olmaması ve bilerek yapılması gibi özelliklere de sahip olması gerekir. Siber zorbalık (cyberbullying) kavramını ilk kullanan kişinin Kanadalı araştırmacı Bill Belsey olduğu bilinmektedir. Siber zorbalık olarak literatüre giren bu kavram bazı araştırmacılar (Belsey, 2004) tarafından geleneksel zorbalığın farklı bir şekli olduğu ifade edilmiştir. Teknolojinin getirdiği olanaklar, geleneksel zorbalık kavramından farklı olarak teknoloji üzerinden zorbalık yapmaya imkân tanıyan yeni bir kavram ortaya çıkarmıştır [2].

Sosyal ağ siteleri, bireylerin kendilerine profil oluşturmalarına, diğer profillerle iletişim kurmalarına, kendilerinin ya da sistemi kullanan diğer profillerin oluşturdukları bağlantılara bakmalarına ve takip etmelerine imkan sağlayan sitelerdir ve gün geçtikçe daha çok kullanıcıya ulaşmaktadırlar. Bazı insanlar profillerinde hayatlarına dair çok fazla detay bulundurmakta ve özel hayatın gizliliğini ortadan kaldırmaktadır. Kötü amaçlı kişilerin günlük hayatta öğrenemeyeceği birçok bilgi sosyal ağlar sayesinde çok rahat bir şekilde öğrenilebilmektedir. Bu sebeple, sosyal ağ profilleri artık farklı amaçlarla da açılmaya başlanmaktadır. Dış dünyada herhangi bir suç işleme potansiyeline sahip olmayan insanlar, sosyal ağlarda sahte hesaplar açmakta ve bu sahte hesapların ardında zorbalık yapmaktadırlar.

Bu sosyal ağ siteleri ise bazı araçlar üzerinden kullanılmaktadır. Bu ağlar ise telefon, tablet ve bilgisayar gibi iletişim araçlarıdır. Araştırmalar sonucunda bu iletişim araçlarının kullanım oranları belirlenmiştir. Bu oranlar ise ilginç bir tablo ortaya çıkartmaktadır. İngiltere'de 2016 yılında yapılan bir araştırmada, 3-4 yaş arasındaki çocukların %55'inin tablet ve %24'ünün masaüstü veya dizüstü bilgisayar kullandığı, %1'inin sosyal medya hesabı olduğu sonucuna ulaşılmıştır. 5-7 yaşındaki çocuklar arasında tablet kullanımı %67,

masaüstü veya dizüstü bilgisayar kullanımı %49 ve akıllı telefon kullanımı %2 ve %4'ünün sosyal medya hesabı olduğu bulunmuştur. 8-11 yaşındaki çocuklar arasında ise tablet kullanımı %80, masaüstü veya dizüstü bilgisayar kullanımı %66, akıllı telefon kullanımı %32 ve %18'inin sosyal medya hesabı olduğu gösterilmiştir. 12 ila 15 yaş arası gençlerin ise %83'ünün kendi cep telefonu , %62'sinin tabletinin ve %69'unun sosyal medya hesabının olduğu belirlenmiştir [3]. 2015 yılında ABD'de yapılan araştırmada, ilkokul çağındaki gençlerin %66'sı dizüstü bilgisayar, %53'ü akıllı telefon ve %78'i tablet kullanmaktadır. Ayrıca, bu gençlerin %35'inin bir dizüstü bilgisayarı, %36'sının bir akıllı telefonu ve %69'unun ise bir tabletinin olduğu belirlenmiştir [4]. Bu araştırmalardan yola çıkarak, küçük yaştaki çocukların dahi iletişim araçlarını kullanarak sosyal ağları ne kadar aktif olarak kullandığını görmekteyiz. Bu aktif kullanım sebebiyle zorbalığa uğrama ihtimalleri veya siber zorba olma ihtimalleri gün geçtikçe yükselmektedir.

Siber zorbalığın bu kadar yaygın olma sebeplerinden biri, zorbaların mağdurlarla yüz yüze olmaması, bu yüzden bir suçluluk duygusu hissetmemeleri ve sahte hesapların verdiği "kimlik gizliliği" düşüncesidir. Ayrıca bu şekilde, normal hayatta tek bir kişiye yapabilecekleri zorbalığı, kimliğini gizleyerek çok geniş bir kitleye karşı yapabilmektedirler. Üstelik zorbalık içeriği olarak sınırları da kalkmış olacaktır. Genel olarak en sık rastlanılan siber zorbalık çeşitleri cinsellik, engellilik, ırkçılık, terörizm, kişisel karakter, inanç, davranış, cinsiyet farklılığı, dış görünüş ve kilo gibi konuları barındırmaktadır [5].

Siber zorbalık eylemleri farklı şekillerde gerçekleştirilebilmektedir. Bazen mağdurların kişisel verilerini toplayıp web sitelerinde veya sosyal ağlarda paylaşarak mağduru rencide etmek veya itibarsızlaştırmak, bazense tehdit, taciz veya dedikodu gibi içeriklere sahip mesaj ve e-posta gönderimi olabilir. Tüm bu zorbalık çeşitleri çocuk, genç ya da yetişkin tüm insanları etkilemektedir. Çocuklardaki mağduriyet ileriki yaşamlarında toplumsal ilişkilerini etkilerken genç ve yetişkin insanlarda ise intihar isteği, pasifleşme ve asosyallik gibi duygulara sebep olmaktadır. Bu sebeple, Sosyal ağlardaki siber zorbalık tespiti çok hassas ve önemli bir konudur.

1.1. Siber Mağdurlar

Siber zorbalık; başka bir kişiyi tehdit ya da taciz etmek, utandırmak veya hedef almak için teknolojik platformların kullanımıdır. Siber zorbalık adını alabilmesi için gençler arasında gerçekleşmesi gerekmektedir. Ancak bir yetişkin söz konusu olduğunda buna siber taciz ya da siber saldırı denir. Siber taciz veya siber saldırı hukuki sonuçlara yol açar hatta hapis cezası gerektirecek kadar büyük bir suçtur [6].

Siber zorbalığın mağdurlarından biri de çocuklardır. Ancak çocukların çoğu siber zorbalığa maruz kaldığını ailesine söylemekten çekinmektedir. Çocukların maruz kaldıkları siber zorbalığı saklamaları sahip oldukları internet, tablet, akıllı telefon veya bilgisayar erişimlerinden mahrum kalma korkusundan kaynaklanmaktadır. Bu yüzden çocuklardaki bu mağduriyeti ortaya çıkartmak, yetişkinlere göre biraz daha güçtür.

Yetişkinler ve gençlerde de bu durum çok farklı değildir. Özellikle genç kesimde siber mağduriyet, çocuklar ve yetişkinlere göre daha ağır etki etmektedir. Ergen yaştaki gençlerin sağlıklı düşünememeleri ve kendilerine olan özgüvenlerinin henüz oluşmamasından dolayı bu yaş grubunda intihar eğilimleri daha fazladır. Araştırmalara göre 4 ergenden 1'inin siber zorbalığa maruz kaldığı ve 6 ergenden 1'inin de başkasına siber zorbalık yaptığı belirlenmiştir [6]. Ayrıca erkeklerin kızlardan daha çok siber zorbalık yaptığı ve boyun eğici davrandıkları belirlenmiştir [7]. Bu durumda kızların siber mağdur olma olasılığının daha yüksek olduğu görülmektedir.

Sosyal ağlardaki siber zorbalığa maruz kalan mağdurların ortak özellikleri şunlardır:

- Kullandıkları sosyal medya veya e-posta hesaplarının güvenlik ayarlarını yapamamak
- Kişisel bilgilerini ve fotoğraflarını herkese açık şekilde kullanmak
- İnternet şifrelerini başkalarıyla paylaşmak ya da çok basit şifreler kullanmak
- İnternet üzerinden tanıştıkları yabancılara kişisel hayatları hakkında bilgi vermek

1.2. Siber Zorbalığın Sosyal Ağlarla İlişkisi

Siber zorbalık cep telefonu, bilgisayar ve tablet gibi dijital cihazlarda gerçekleşen bir zorbalık çeşididir [8]. Her gün, dünyanın dört bir yanındaki insanlar siber zorbalıkla karşı karşıya kalmaktadır. Sosyal ağlar ise siber zorbalığın uygulandığı alanlardan biridir. Araştırmalara göre, sosyal ağlardan biri olan Facebook'un kullanıcılarının yaklaşık %76'sı bu ağı günlük olarak kullanmaktadır. Ayrıca bu ağın 2.07 milyar aktif kullanıcısı bulunmaktadır [9]. Bu istatistik ise sosyal ağların etkisi hakkında bazı çıkarımlarda bulunmamızı sağlamaktadır. Sosyal ağları daha sık kullanan insanların, az kullanan insanlardan daha fazla siber zorbalığa eğilimlerinin olduğu veya siber zorbalığa maruz kaldığı tespit edilmiştir [10]. Ancak aynı zamanda sosyal ağları kullanan insanlarda daha önce sahip olmadığı bir özgüven ortaya çıkmaktadır. Bunun bir sebebi ise sosyal ağlardaki anonimlik özelliğidir. Bu sebeple, insanların büyük bir çoğunluğu gerçek kimliklerini gizleyerek duygularını rahatça ifade edebilmektedir. Ancak duygularını rahatça ifade ettiğini düşünen büyük bir çoğunluk siber zorbalık yaptığının farkına varamamaktadır.

Sosyal ağ sitelerinin, çevrimiçi etkinliklerin ve mesajlaşma uygulamalarının artmasıyla birlikte, siber zorbalık da artmaktadır [11]. Bu ağlar ise genellikle gençler tarafından kullanılmaktadır. Ditch the Label tarafından yapılan bir ankette, ankete katılan gençlerin %47'si sosyal ağ profillerinde kötü yorumlar almaktadır ve %62'si insanlara kötü amaçlı mesajlar göndermektedir [12]. Bu gibi durumlar çocuklar, gençler ve yetişkinler de dâhil olmak üzere her yaşta insanın hayatını ciddi şekilde etkilemektedir.

Birçok sosyal ağ kullanıcısı, bu ağları beğenilme arzusuyla kullanmaktadır. Ayrıca sosyal ağların kendilerini daha az yalnız hissettirmesinden dolayı kullanan kullanıcıların sayısı da oldukça fazladır. Ancak belli bir kesimin sosyal ağları kullanma sebebi bu kadar masum değildir. Çoğunlukla insanların sosyal ağları beğenilme arzusu ve yalnızlık sebebiyle kullandığını bilen bir kesim bu durumdan faydalanmaktadır. Sahte hesaplar açarak bu insanları rencide edici, cinsellik, tehdit ya da hakaret içeren mesaj veya yorumlar yazmakta ve kişilerin kendilerine olan özgüvenlerini düşürmelerine sebep olmaktadır. Bu yüzden sosyal ağların kullanımı sıklaştıkça bu gibi durumlara maruz kalma olasılığı da o kadar yükselmektedir.

1.3. Siber Zorbalığı Önleme ve Müdahale

Siber zorbalık ile ilgili araştırmalar diğer zorbalık türlerine göre karşılaştırıldığında daha yenidir. Teknolojinin yaygın kullanılması ile çoğunlukla geleneksel akran zorbalığının bir çeşidi olarak değerlendirilen siber zorbalık hem ulusal hem de uluslararası alanyazında sıkça görülmektedir. Hem teorik tartışmalar hem de veriye dayalı araştırma sonuçları incelendiğinde, iki tip zorbalığın ortak yönlerinin olduğu ve aynı kişilerin hem siber ortamda hem de fiziksel ortamda mağdur olduğu görülmektedir [13].

Siber zorbalığın geleneksel akran zorbalığıyla olan benzerliğinden yola çıktığımızda, siber zorbalığı önlemek için geleneksel akran zorbalığı önleme ve müdahale programları kullanılabilir [14]. Yapılan araştırmaların çoğu, ne tür bir müdahalenin ergenlere yardımcı olabileceğin odaklanmıştır ve siber zorbalığı önleme ve müdahale etkinliklerine dair çok az çalışma gerçekleştirilmiştir.

Siber zorbalığı geleneksel akran zorbalığından ayıran en önemli özellikler, siber zorbalığın bilgi ve iletişim teknolojileri aracılığıyla gerçekleşmesi, mağdura sadece evinin dışında değil cep telefonu, tablet ya da bilgisayarını kullandığı her yerde ve her anda ulaşılabilmesi ve siber ortamın anonim olması nedeniyle zorbanın kimliğini gizlemesine olanak tanımasıdır [15]. Bu nedenle, siber zorbalık önleme ve müdahale programları mağdurların bazı teknik donanımları da edinmesini gerektirmektedir.

Müdahaleden önce, mağdurlar olayları rapor etmelidir. Siber zorbalık mağdurların olayları rapor edip etmediklerini ve neden rapor etmediklerini araştırmak için iki çalışma yapılmıştır [16, 17]. İlk çalışmada, 177 yedinci sınıf öğrencisi arasında gerçekleştirilen ankette; %52 si herhangi birine karşı siber zorbalık gerçekleştirdiğini, %25'i ise siber zorbalığa maruz kaldığını bildirmiştir. Genel olarak, ankete katılanların %67'si okullardaki yetişkinlerin bilinçli olarak siber zorbalığı durdurmaya çalıştığına düşünmektedir, ancak buna rağmen mağdurların %66'sı yaşadıkları durumu bir yetişkine rapor etmemiştir [16]. Yapılan diğer çalışmada ise, banliyö ve kırsal okullardan 7. Sınıftan 12. Sınıfa kadar olan 247 öğrenci siber mağduriyet sonrası davranışları analiz edilmiştir. Bu çalışmada

öğrencilerin %42,5'i siber zorbalık deneyiminden sonra hiçbir şey yapmadığını bildirirken, %11,7'si durumu bir yetişkine, %23,5'i ise bir arkadaşına bildirmiştir [17].

Teknolojik temelli programların bazılarında ise siber zorbalık vakalarının bilgisayar programları tarafından otomatik olarak tespit edilebilmesi için bir sistem hazırlanmıştır [18]. Bir diğer çalışmada ise (Szuster, Barlinska ve Kozubal, 2016) video kullanımı gibi teknolojik temelli olan ve fotoğraf kullanımı gibi teknolojik olmayan uygulamalar bir arada kullanılmıştır [19].

Bu çalışmaların sonucunda öğrencilerin birçoğu yaşadıkları mağduriyetlerini bir yetişkine anlatmaktan çekinmektedir. Bu durum siber zorbalığın tespitini ve önlenmesini de zorlaştırmakta ve mağdurların yaşadıkları duygusal, sosyal ve akademik problemlerle mücadele etmelerinde yalnız kaldıkları sonucunu göstermektedir [20]. Bu yüzden siber zorbalık ile mücadelede ilk olarak kısım eylemlerin bildirilmesi ve raporlanmasıdır daha sonra bilgilendirme işlemi gerçekleştirilmelidir.

1.4. Makine Öğrenmesi

Makine öğrenmesi, açıkça programlanmadan, otomatik olarak öğrenme ve deneyimle daha iyi olma becerisine sahip sistemi güçlendirir. Makine öğrenimi algoritmaları, açıkça yazılmış algoritmaları yüksek hızlı performansla dağıtmanın mümkün olmadığı alanlarda faydalıdır. Sayıların sıralanması gibi basit bir işlem kolaydır ve girdi olarak bazı sayılar vererek ve çıktı olarak sıralı bir liste alarak gerçekleştirilebilir. Makine öğrenmesi algoritmaları genellikle denetimli ve denetimsiz olarak iki kategoriye ayrılmaktadır.

Denetimli Makine Öğrenmesi'nde, algoritmalar etiketli verilerden öğrenirler. Verileri anladıktan sonra, algoritma, desene dayanarak yeni verilere hangi etiketi vermesi gerektiğini belirler ve desenleri etiketlenmemiş yeni verilere ilişkilendirir. Denetimli Öğrenme, Sınıflandırma ve Regresyon olmak üzere 2 kategoriye ayrılabilir. Sınıflandırma, verinin ait olduğu kategoriyi tahmin eder. Regresyon, önceki gözlenen verilere dayanarak sayısal bir değer öngörür. Denetimli öğrenme için temel fikir, verileriniz durumların örneklerini sunar ve her örnek için bir sonucu belirtir. Daha sonra, makine, eski örneklere

dayanarak yeni verilerin sonucunu tahmin edebilecek bir model oluşturmak için eğitim verilerini kullanacaktır [21].

Denetimsiz Makine Öğrenmesi'nde, bilinen veya etiketlenmiş sonuçlara atıfta bulunmadan bir veri setinden kalıpları çıkarır. Denetimli makine öğrenmesinden farklı olarak, denetlenmeyen makine öğrenme yöntemleri doğrudan bir regresyona veya bir sınıflandırma problemine uygulanamaz çünkü çıktı verisi için değerlerin ne olabileceği hakkında hiçbir fikir yoktur ve bu da algoritmayı normalde yapılan gibi eğitmeyi imkansız hale getirir. Denetimsiz öğrenme bunun yerine verinin temel yapısını keşfetmek için kullanılabilir [22].

Makine öğrenmesi karmaşık problemlere karşı tahmin yürütebilme yeteneğine sahip olduğundan birçok alanda kullanılabilmektedir. Makine Öğreniminin Birkaç Uygulaması şunlardır [23]:

- Metinlerin veya belgelerin sınıflandırılması. (Örneğin: Spam mesajlarını filtreleme) [24].
- Konuşma tanıma [25].
- Görüntü tanıma ve yüz tanıma gibi bilgisayarlı görme görevleri [26].
- Kendi kendine sürüş araçlar [27].
- Arama amacıyla olduğu gibi web sayfası sıralaması [28].
- Ortak filtreleme [29].
- Tıbbi tanı [30].
- Hesaplama biyolojisi uygulaması [31].
- Tavsiye sistemleri, arama motorları, bilgi çıkarma sistemleri [32].

1.5. Metin Madenciliği

Metin madenciliği, verilerdeki kavramları, kalıpları, konuları, anahtar kelimeleri ve diğer nitelikleri tanımlayabilen yazılım destekli büyük miktarda yapılandırılmamış metin verilerini keşfetme ve analiz etme sürecidir. Bazılarının iki terim arasında bir ayrım

yapmasına rağmen, metin analizi olarak da bilinir; Bu görüşe göre, metin analitiği, veri kümelerini sıralamak için metin madenciliği tekniklerinin kullanılmasıyla sağlanan bir uygulamadır.

Metin madenciliği, büyük veri platformlarının geliştirilmesi ve büyük yapılandırılmamış veri kümelerini analiz edebilen derin öğrenme algoritmaları nedeniyle veri bilimcileri ve diğer kullanıcılar için daha pratik hale gelmiştir. Metin incelemesi ve analizi, kuruluşların kurumsal belgelerde, müşteri e-postalarında, çağrı merkezi günlüklerinde, yazılı anket incelemelerinde, sosyal ağ paylaşımlarında, tıbbi kayıtlarda ve diğer metin tabanlı verilerin kaynaklarında potansiyel olarak değerli iş öngörüleri bulmalarına yardımcı olur.

Metin madenciliği doğada veri madenciliğine benzer, ancak yapılandırılmış veri biçimleri yerine metne odaklanır. Bununla birlikte, metin madenciliği sürecindeki ilk adımlardan biri, verileri bir şekilde düzenlemek ve yapılandırmaktır, böylece hem nitel hem de nicel analize tabi tutulabilir. Bunu yapmak, tipik olarak, veri kümelerini ayrıştırmak ve yorumlamak için hesaplamalı dilbilim ilkelerini uygulayan doğal dil işleme (NLP) teknolojisinin kullanılmasını içerir [33]. Doğal Dil İşleme (NLP) ve Metin Madenciliği (ayrıca Metin Analitiği olarak da bilinir), kullanıcıları metin belgelerindeki anahtar içeriği hızlı bir şekilde nicel, eyleme geçirilebilir içgörülere dönüştürmeye zorlayan Yapay Zeka (AI) teknolojileridir [34]. Kısaca metin madenciliği, anahtar kavramları ve temaları yakalamak ve yazarların bu kavramları ifade etmek için kullandıkları kesin kelimeleri veya terimleri bilmenizi gerektirmeden gizli ilişkileri ve eğilimleri ortaya çıkarmak için metinsel materyal koleksiyonlarını analiz etme sürecidir [35].

1.6. Nitelik Seçimi

Nitelik seçimi (diğer adıyla özellik seçimi), makine öğreniminde modelin performansını büyük ölçüde etkileyen temel kavramlardan biridir. Makine öğrenim modellerini eğitmek için kullanan veri özellikleri, başarılabilecek performans üzerinde büyük bir etkiye sahiptir. Alakasız veya kısmen ilgili özellikler model performansını

olumsuz yönde etkileyebilir ve modellerin doğruluğunu azaltabilir. Nitelik seçimi ve veri temizleme, model tasarımının ilk ve en önemli adımı olmalıdır [36].

Verilerdeki yüksek özellik sayısı, modelde Aşırı Uyum riskini artırır. Nitelik Seçimi yöntemi, fazla bilgi kaybı olmadan özelliklerin boyutunun azaltılmasına yardımcı olur. Nitelik Seçimi yapmanın faydaları şunlardır [36]:

- **Gereksiz veriyi azaltır:** Daha az gereksiz veri, gürültüye dayalı kararlar almak için daha az fırsat demektir.
- **Doğruluğu Artırır:** Daha az yanıltıcı veri, modelleme doğruluğunun iyileştirildiği anlamına gelir.
- **Eğitim Süresini Azaltır:** Daha az veri noktası algoritma karmaşıklığını azaltır ve algoritmalar daha hızlı çalışır.

2. KAYNAK ARAŞTIRMALARI

2.1. Metin Sınıflandırma

Metin sınıflandırma (diğer adıyla metin etiketleme), serbest metne önceden tanımlanmış bir dizi kategori atamak görevidir. Metin sınıflandırıcıları hemen hemen her şeyi organize etmek, yapılandırmak ve kategorilere ayırmak için kullanılabilir. Örneğin, yeni makaleler konulara göre düzenlenebilir, destek biletleri ivedilikle düzenlenebilir, sohbet konuşmaları dile göre düzenlenebilir, marka sözleri duyarlılıkla düzenlenebilir.

Metin sınıflandırması iki farklı şekilde yapılabilir: manuel ve otomatik sınıflandırma. Birincisinde, bir insan noteri metnin içeriğini yorumlar ve buna göre sınıflandırır. Bu yöntem genellikle kaliteli sonuçlar sağlayabilir ancak zaman alıcı ve maliyetlidir. Sonuncusu, metni daha hızlı ve daha uygun maliyetli bir şekilde otomatik olarak sınıflandırmak için makine öğrenmesi, doğal dil işleme ve diğer teknikleri uygular [37].

2.1.1. Siber Zorbalık Tespiti

Siber zorbalık, birisini rahatsız etmek, küçük düşürmek, tehdit etmek, taciz etmek veya kötüye kullanmak amacıyla dijital teknolojilerin kullanılmasıdır [38]. Siber zorbalık, başkası hakkında olumsuz, zararlı, yanlış veya kötü niyetli içerik göndermeyi, yayınlamayı veya paylaşmayı içerir. Utanmaya veya küçük düşürmeye neden olan, başka biri hakkında kişisel veya özel bilgilerin paylaşılmasını içerebilir. Siber zorbalığın gerçekleştiği en yaygın yerler:

- Facebook, Instagram, Snapchat ve Twitter gibi Sosyal Medyalar
- SMS (Kısa Mesaj Servisi), cihazlar aracılığıyla gönderilen Kısa Mesaj olarak da bilinir.
- Anlık Mesajlaşma (cihazlar, e-posta sağlayıcı servisleri, uygulamalar ve sosyal medya mesajlaşma özellikleri ile)
- E-posta

Ayrıca siber zorbalık olabilecek davranışların bazıları şunlardır:

- E-posta, metin veya anlık mesaj gönderme.
- Sosyal medyada biri hakkında küçük düşürücü şeyler yayınlamak.
- Birisiyle ilgili çevrimiçi olarak söylentiler ya da dedikodular yaymak.
- Birden fazla kişiyi içeren çevrimiçi bir sohbette biriyle dalga geçme.
- Sürekli olarak ve bilerek çevrimiçi bir oyunda bir avatar veya karaktere saldırmak veya öldürmek.
- Sahte bir çevrimiçi profil oluşturarak başka biri gibi davranmak.
- Birini çevrimiçi veya kısa mesajla tehdit etmek veya korkutmak.
- Utanç verici bir fotoğraf veya video çekmek ve izinsiz paylaşmak.

Başka bir yönden bakılacak olursa siber zorbalık, gençlerin diğer gençlere zarar vermek için çevrimiçi teknolojileri kullanmasıdır [39]. Gençler arasındaki tüm çevrimiçi çatışmalar siber zorbalık değildir. Bazen sosyal medyada tartışmaya girebilirler. Birbirleriyle şakalaşabilirler ya da mesajlaşırken bu şakaları kullanabilirler. Ancak bir davranışın siber zorbalık olup olmadığını belirlemenin yolu, bunu kasıtlı ve düzenli olarak yapılıp yapılmadığını belirlemektir. Eğer kasıtlı ve tekrarlı olarak yapılıyorsa bu siber zorbalıktır.

Selçuk Üniversitesi'nde 2013 yılında 500 üniversite öğrencisiyle yapılan bir araştırmaya göre, öğrencilerin %97.6'sı sosyal ağları kullanmaktadır [40]. Çıkan sonuç ise oldukça yüksektir. Sosyal ağların bu kadar sık kullanımının bir sonucu olarak insanların siber zorbalığa uğrama ihtimalleri veya siber zorba olma ihtimalleri gün geçtikçe artmaktadır.

Yapılan bir araştırmada, dünya nüfusunun %42'sinin sosyal ağ kullanıcısı olduğu ve bunların %20'sinin de siber zorbalığa maruz kaldığı belirtilmiştir [41]. Bu durum sosyal ağların yaygınlaşmasıyla siber zorbalığın artması arasında doğru orantı olduğunu göstermektedir.

Zorbalık, geleneksel zorbalık ve siber zorbalık olmak üzere iki çeşittir. Geleneksel zorbalıkta kurbanlar zorbanın kim olduğunu bilmektedir. Bununla birlikte, geleneksel

zorbalıkta kullanılan yöntemler çoğunlukla bilinirken, siber zorbalıkta kullanılan yöntemler sürekli olarak değişmekte ve tespiti zorlaşmaktadır. Siber zorbalığının tespitinin zor olmasının yanı sıra geleneksel zorbalıkla arasındaki en önemli fark zorbanın kimliğinin bilinmemesidir. Sanal kurbanların en az %50 veya %60'ı kendilerine eziyet eden kişiyi tanımamaktadır [42].

Siber zorbalık tespiti için yapılan çalışmalar incelendiğinde metin madenciliği yöntemleri kullanılarak bir takım çalışmalar gerçekleştirildiği görülmektedir. Bu çalışmalardan biri de Naive Bayes, K-NN, J48 ve SVM yöntemleri kullanılarak, siber zorbalık tespiti için yapılan araştırmasın sonucunda SVM yönteminde %97.11 doğruluk oranı ölçülmüştür [43]. Massachusetts Institute of Technology'de yapılan bir araştırmada YouTube video yorumlarında metin bağlamında siber zorbalık tespit edilmiştir. İlk sınıflandırma seviyesi, yorumun cinsellik, ırk/küfür, zeka ve fiziksel özellikler gibi hassas konuda olup olmadığını belirlemek olmuştur. Bu denemede %66.7 doğruluk oranı bulunmuştur [44]. Başka bir araştırma ise Formspring.Me web sitesindeki siber zorbalık tespitini ilk araştıran Kelly Reynolds, April Kontostathi ve Lynne Edwards'ın çalışmasıdır. Bu çalışmada makine öğrenmesi sonucu %78,5 doğruluk oranı bulunmuştur [45]. Bir başka araştırma da Twitter üzerindeki siber zorbalık tespiti çalışmasıdır. 2011 yılında yapılan bu çalışmada Naive Bayes kullanılarak doğruluk oranı %67.3 çıkmıştır [46]. Yine Twitter veri kümesi kullanılarak yapılan başka bir çalışma ise Paul Roumeliotis, Hao Xu tarafından 2014 yılında yapılan siber zorbalık tespiti sonucu SVM sınıflandırıcı kullanılarak %85 doğruluk oranı bulunmuştur. M. Munezero, M. Mozgovoy, T. Kakkonen, V.Klyuev ve E. Sutinen tarafından yapılan bir araştırmada zararlı dil tespiti için kullanılabilir bir veri seti kullanmışlardır. Bu veri seti için SMO, 48 ve NBM algoritmalarını kullanarak %98 doğruluk oranı elde etmişlerdir. Zubiaga ve diğerlerinin yaptığı çalışmada ise Twitter veri kümesi incelenmiş ve bu veri kümesi üzerinden %81.2 doğruluk oranı bulunmuştur [47].

2.2. Nitelik Seçimi

Bir veri seti çok fazla özelliğe sahip olduğunda, hepsini makine öğrenme modeline dahil etmek ideal bir yöntem değildir. Bazı özellikler bağımsız değişken için önemsiz olabilir. Bu nedenle veri setindeki her türlü gereksiz veya alakasız özellikleri kaldırmak için nitelik seçimi(diğer adıyla özellik seçimi veya değişken seçimi) kullanılmalıdır. Yani kısaca, veri kümelerinin boyutunu azaltmak için kullanılmaktadır ve makine öğrenme sonuçlarını daha güçlü hale getirebilir [5]. Büyük veri kümelerinde sınıflandırma çalışması yaparken, en önemli aşamalardan biridir [48]. Nitelik seçimi kullanılan algoritmaya göre veri setindeki n adet nitelik arasından en iyi k adet niteliği seçme işlemidir [49]. Nitelik seçiminin avantajları şunlardır [50]:

- Depolama gereksinimlerini sınırlamak ve algoritma hızını artırmak için nitelik alanının boyutunu azaltır,
- Gereksiz, alakasız veya gürültülü verileri kaldırır,
- Veri analizi görevlerinin anlık etkileri, öğrenme algoritmalarının çalışma süresini hızlandırır,
- Veri kalitesini arttırır,
- Ortaya çıkan modelin doğruluğunu arttırır,
- Bir sonraki veri toplama işleminde veya kullanım sırasında kaynak tasarrufu için veri kümesindeki gereksiz özellikleri azaltma,
- Performansı iyileştirir, tahmindeki doğruluğu arttırır,
- Verinin anlaşılabilmesi için görselleştirir ve daha basit bir şekilde tanımlanmasına yardımcı olur.

2.2.1. Filtre Yöntemleri

Filtre özelliği seçme yöntemleri, her özelliğe bir puanlama atamak için istatistiksel bir ölçü uygulanır. Özellikler puanla sıralanır ve veri kümesinden tutulması veya çıkarılması için seçilir. Yöntemler genellikle tek değişkenlidir ve özelliği bağımsız olarak veya bağımlı değişkene göre değerlendirir. En çok kullanılan filtreleme yöntemleri ise Ki-Kare testi, t-Skor, Bilgi Kazancı ve Kazanç Oranı'dır.

Ki-Kare Testi, iki değişken arasında anlamlı bir ilişki olup olmadığını belirlemek için yapılan istatistiksel bir testtir. Basit bir deyişle Ki-Kare istatistiği, gözlemlenen her iki değişkenin beklenen frekansları arasında anlamlı bir fark olup olmadığını test eder. İki olay bağımlıysa, sınıfın oluşumunu tahmin etmek için özelliğin oluşumunu kullanabiliriz. Oluşumunun sınıfın oluşumuna bağlı olduğu özellikleri seçmeyi amaçlıyoruz. İki olay bağımsız olduğunda ise Ki-Kare puanının değeri ne kadar yüksekse, özellik sınıfla ilişkilendirilebilme olasılığı o kadar fazladır ve bağımsızlık hipotezinin yanlış olduğunu gösterir. Bu nedenle model eğitimi için seçilmelidir [51].

T-Skor, yaygın olarak kullanılan özellik seçim yöntemlerinden biridir. Bu yöntem, her sınıf için özelliklerin örneklem büyüklüğü, ortalama ve standart sapma değerlerini kullanarak bir ilişki puanı hesaplar. Daha az puan alan özellikler veri setinden çıkarılır. T-score yönteminin özellik seçim süreci, hesaplanan puanlara göre azalan sıraya göre sıralanan özellikler şeklinde yürütülür, ardından istenen özellik sayısı üstten başlayarak seçilir [52].

Bilgi Kazancı, bir özelliğin bize sınıf hakkında ne kadar bilgi verdiğini ölçer. Karar Ağacı Algoritmaları tarafından Karar Ağacı oluşturmak için kullanılan ana anahtardır. Karar Ağaçları algoritması her zaman Bilgi kazancını en üst düzeye çıkarmaya çalışır. En yüksek Bilgi kazancı olan bir özellik ilk önce test edilecek / bölünecektir. Bilgi kazancının hesaplanmasında Entropi modeli kullanılmaktadır [53].

Kazanç Oranı, karşılıklı bilginin bir çeşididir. Karşılıklı bilgi değerlerinin 0'dan 1'e normalize edilmesi olarak görülebilir. Bilginin, hedef niteliğin entropisine oranıdır. Bunu yaparak, birçok değere sahip niteliklere yönelik önyargıları da azaltır [54]. Başka bir deyişle, kazanç oranı yanlılığını azaltan Bilgi Kazancı'nın bir modifikasyonudur. Bir özellik seçerken kazanç oranı dalların sayısını ve boyutunu dikkate alır. Bir bölünmenin iç bilgisini hesaba katarak bilgi kazancını düzeltir. İçsel bilgi, örneklerin dallara dağılma entropisidir (yani bir örneğin hangi dalın ait olduğunu söylemek için ne kadar bilgiye ihtiyacımız var). Özgün bilgiler büyüdükçe özniteliğin değeri de azalır [55].

3. MATERYAL VE YÖNTEM

Bu bölümde, bu çalışmada önerilen yöntemler ve kullanılan materyallerle ilgili ayrıntılar yer almaktadır.

3.1. Materyaller

Formspring.Me veri kümesiyle ilgili ayrıntılar, Knime ve Weka Veri Madenciliği Araçları kullanılarak gerçekleştirilen işlemler ve algoritmalar bu bölümde sunulmuştur.

3.1.1. Formspring.Me Veri Kümesi

Formspring.Me veri kümesi 1994 iletiden oluşan bir xlsx dosyasıdır. Her bir veri için siber zorbalık durumu barındırıp barındırmamasına göre etiketlenmiştir. Veri seti içerisinde yer alan bilgiler aşağıdaki etiketleri içermektedir:

- <Text>, kullanıcılara ait ileti sorularını içerir.
- <Cyberbullying>, siber zorbalık olup olmadığını belirtir. 0 (zorbalık yok), 1 (zorbalık var).

	A	B	C
1	Text	Ciberbullying	
2	would you/have you been in an interracial relationship?	0	
3	i wunt y0 di!ckk .	1	
4	I ment boyfriend u know like the kissing the hugging estera.....unless u do that with your bes	0	
5	what the fuck is everyones problem with u ??? u seem nice as far as i know :)	0	
6	hey this is actually Danny Grammes and i didnt write thatvvvv someone is writing shit and pu	1	
7	you think someone should have to compete for the girl they love	1	
8	if ur friends set u up on a blind-date.. and it turned out u were on the blind date show AND u	0	
9	whyy dose rubinathy15 ask stoopid questions? erase the dum betch	1	
10	your a dirty bitch int ya?	1	
11	2 weeks? WOW i totally change my mind!! thats like sooooo long! im sorry i ever said anythin	1	
12	http://www.meatspin.com/	1	
13	I'm so bored why am i sat in alone on a saturday night?!	0	
14	do you think girls look better with makeup on or none?	0	
15	beach with the Blonde how about thursday? :)	0	
16	i jsut washed mine couple days ago...	0	
17	Do you own any sex toys? If so..why?	0	
18	Would u end up in heaven or hell. Or in purgatory?	0	
19	im not Jewish im catholic so suck a dick	1	
20	did you go to an awesome party or sumthin?	0	
21	Name 3 of the best places you have ever been to?	0	
22	Suck it	1	
23	My home page it's all of your shit.	1	

Şekil 3.1 Formspring.me veri kümesinin bir örneği

Veri Kümesi "Siber Zorbalık İçeren" ve "Siber Zorbalık İçermeyen" olmak üzere iki sınıfa ayrılır. Siber Zorbalık İçeren iletiler 976 mesaj ve Siber Zorbalık İçermeyen iletiler 1018 mesaj içermektedir. Veri kümesini test ve eğitim olarak ayırmak için "Cross-validation" yöntemi uygulanmıştır. 10 katlama değeri kullanılarak veri setinin %90'lık kısmı eğitim için, %10'luk kısmı test için kullanılmıştır.

3.1.2. Weka Veri Madenciliği Aracı

Weka(Waikato Environment for Knowledge Analysis), veri madenciliği görevleri için makine öğrenmesi algoritmaları topluluğudur. Weka birleştirme kuralları, veri ön işleme, sınıflandırma, regresyon, kümeleme ve görselleştirme için araçlar içeren ve GNU Genel Kamu Lisansı altında yayınlanan açık kaynak kodlu bir yazılımdır. Weka, herhangi bir programlama yapmak zorunda kalmadan, grafik ara yüzü kullanarak uygulamalı makine öğrenmesi sürecinden geçmektedir. Weka'nın grafiksel ara yüzü Şekil 3.2'de gösterilmiştir. Weka'da algoritmalar doğrudan bir veri kümesine uygulanabilir veya Java koduyla çağırılabilmektedir. Ayrıca Weka'da 4 adet kullanıcı ara yüzü bulunmaktadır.

Şekil 3.2 Weka kullanıcı ara yüzü

Explorer: Weka'nın en sık kullanılan ortamıdır. Explorer modunda sınıflandırma, ilkelleme, veri önişleme, gruplandırma, özellik seçimi ve görselleştirme seçenekleri mevcuttur. Sınıflandırma sekmesinde 71 adet algoritma bulunmaktadır ve bu algoritmalar 6 kategoriye ayrılmıştır.

Experimenter: Experimenter sınıflandırma ve regresyon tekniklerini uygularken verilen sorun için hangi yöntem ve parametre değerleri en iyi sonucu verdiğini göstermek için tasarlanmıştır. Kısaca çeşitli öğrenme tekniklerinin karşılaştırılmasını sağlayan bir ortamdır.

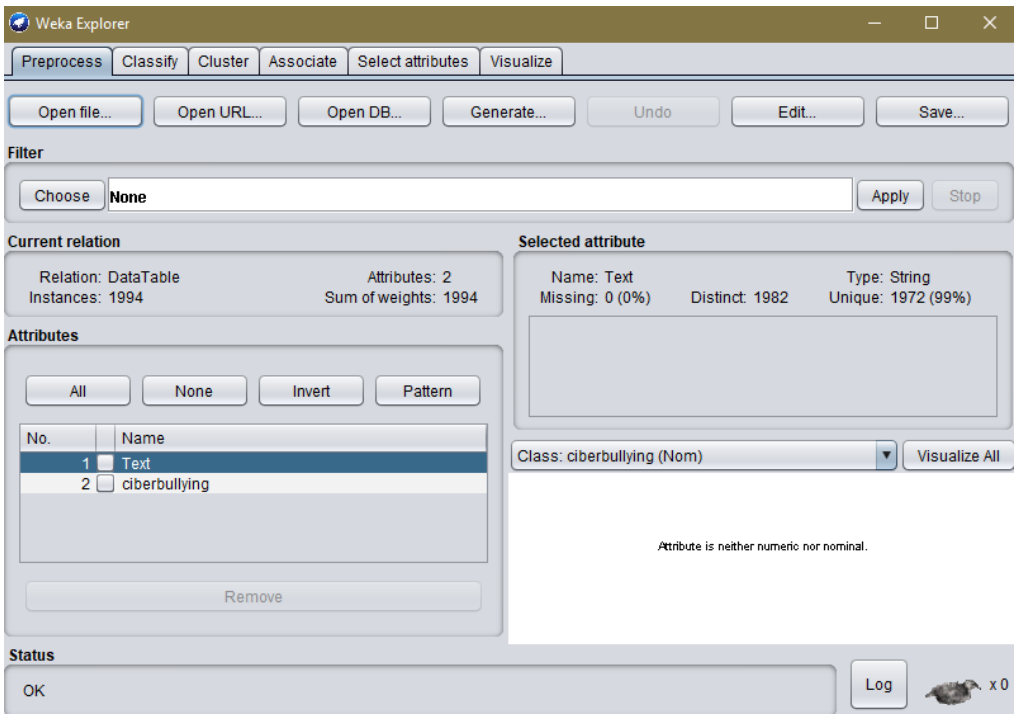
KnowledgeFlow: Akışlı veri işleme için yapılandırma tasarlanmasını sağlamaktadır. Ekrandaki öğrenme algoritmalarını ve veri kaynaklarını temsil eden kutuların sürüklenmesini ve bunları istenen konfigürasyona birleştirilmesini sağlar. Veri kaynaklarını temsil eden bileşenleri, ön işleme araçlarını, öğrenme algoritmalarını, değerlendirme

yöntemlerini ve görselleştirme modüllerini birleştirerek bir veri akışı belirlemenizi sağlar [56].

Workbench: Ortak bir kullanıcı ara yüzü ile birbirine bağlanmış bir takım araçlardır [57].

Simple CLI: Weka komut satırı ara yüzü, komutlarını hızlı ve kolay bir şekilde deneyebileceğiniz bir ortam sağlar.

Verilerin veri tabanından çekilebilmesi için bir dosya verisi şeklinde olması gerekmektedir. Ayrıca Weka'da pek çok kütüphane hazırdır [58]. Bunlar regression(ilkelleme), data preprocessing(veri önişleme), classification(sınıflandırma), clustering(gruplandırma), feature extraction (özellik seçimi veya özellik çıkarımı) bunlardan bazılarıdır. Görsel olarak görüntüleme aracı ise Visualization(Görselleştirme)'dır. Ayrıca Weka arff, json, csv, data gibi veri tiplerini destekler.



Şekil 3.3 Weka Explorer sayfası

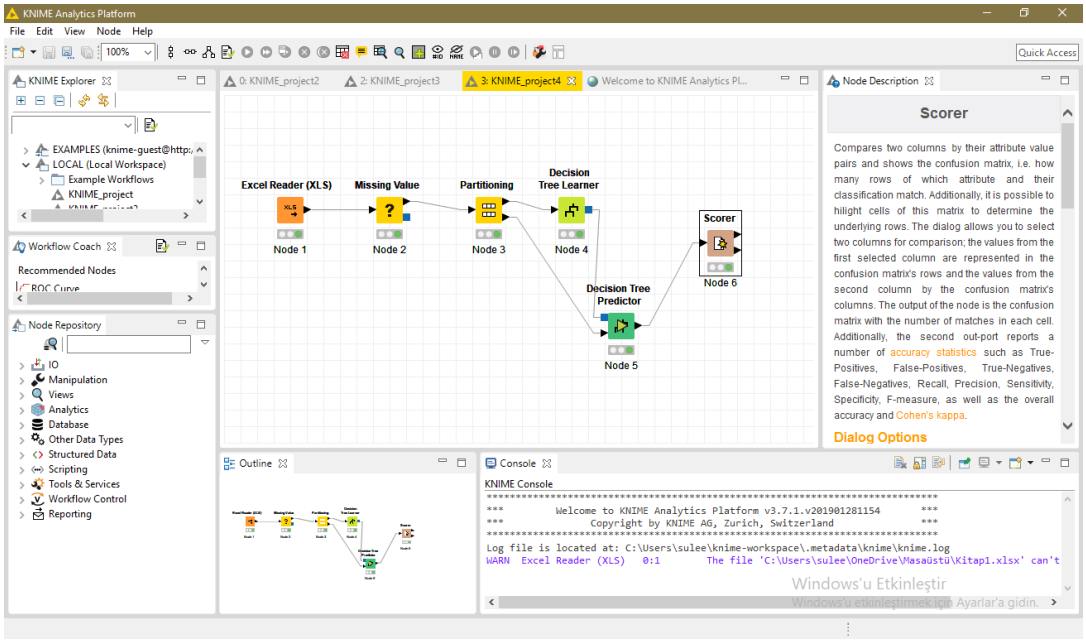
```
@RELATION iris
@ATTRIBUTE sepallength NUMERIC
@ATTRIBUTE sepalwidth  NUMERIC
@ATTRIBUTE petallength NUMERIC
@ATTRIBUTE petalwidth  NUMERIC
@ATTRIBUTE class {Iris-setosa,Iris-versicolor,Iris-virginica}
@DATA
5.1,3.5,1.4,0.2,Iris-setosa 4.9,3.0,1.4,0.2,Iris-setosa 4.7,3.2,1.3,0.2,Iris-
setosa 4.6,3.1,1.5,0.2,Iris-setosa 5.0,3.6,1.4,0.2,Iris-setosa 5.4,3.9,1.7,0.4,Iris-
setosa 4.6,3.4,1.4,0.3,Iris-setosa 5.0,3.4,1.5,0.2,Iris-setosa 4.4,2.9,1.4,0.2,Iris-
setosa 4.9,3.1,1.5,0.1,Iris-setosa
```

Şekil 3.4 Örnek bir .arff dosyası

3.1.3. Knime Veri Madenciliği Aracı

Knime 2008 yılında geliştirilmiş, açık kaynak kodlu ve kullanımı kolay, Java tabanlı bir veri madenciliği programıdır. Knime, Konstanz Information Miner (Konstanz Bilgi Madencisi)'nin kısaltmasıdır. Big Data süreçlerinde sınırlı sabit disk alanıyla kullanıma uygundur.

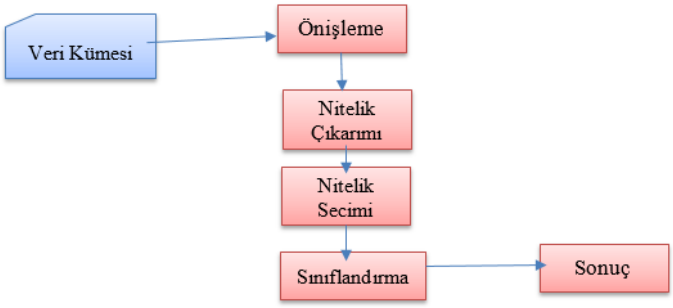
Knime workflow mantığıyla çalışmaktadır. Sürükle bırak yapılarak node'lar birbirine bağlanmakta ve akış diyagramı oluşturulmaktadır. Şekil 3.5'te bir veri setine öğrenme ve eğitim algoritmaları uygulanmıştır sonucunun görüntülenmesi için Scorer düğümü eklenmiştir.



Şekil 3.5 Örnek bir Knime ekranı

3.2. Yöntemler

Bu bölümde önerilen önişleme, nitelik çıkarımı, nitelik seçimi ve sınıflandırma algoritmaları için kullanılan yöntemler açıklanmıştır. Siber zorbalık tespiti için kullanılan yöntemlerin akış şeması Şekil 3.6'da gösterilmiştir.



Şekil 3.6 Veri seti sınıflandırılmasında kullanılan ana yöntemlerin akış şeması

Bu çalışmada önerilen yöntem, Önişleme, Nitelik Çıkarımı, Nitelik Seçimi ve Sınıflandırma olmak üzere 4 ana adımdan oluşmaktadır. Bu çalışmada kullanılan veri seti

Bölüm 3.1.1'de anlatıldığı gibi hazırlanmıştır. Öncelikle veri seti Önişleme adımından geçirilmiştir. Daha sonra veri setinin nitelikleri çıkartılmış ve Nitelik Seçimi yapılmıştır. Nitelik seçimi olarak Chi2 algoritması kullanılmıştır. Son aşamada ise seçilen nitelikler kullanılarak veri seti sınıflandırma işlemleri gerçekleştirilmiş ve bulunan sonuçlar karşılaştırılmıştır. Sınıflandırmada Naive Bayes, J48, LibSVM, RBFClassifier, SGD, SMO, K-NN, HoeffdingTree, RandomTree, LWL, MultiClassClassifier, RandomForest, RBFNetwork, REPTree, Dld4jMlpClassifier, VotedPerceptron, DecisionTable sınıflandırıcıları kullanılmıştır. Bu ana adımlar sonraki bölümlerde daha detaylı anlatılmıştır.

3.2.1. Önişleme

Bu çalışmanın önişleme adımında küçük harfe dönüştürme, kelimelerin kökenine bakma, etkisiz kelimeleri çıkartma işlemleri bir kriter olarak değerlendirilmiş ve bu işlemlerin sınıflandırma performansı üzerinde nasıl etkiler oluşturacağı gözlenmek istenmiştir. Gerçekleştirilen bu işlemler metin madenciliği işlemlerinde sık kullanılan önişleme adımları arasında yer almaktadır.

İlk önişleme kriteri olarak veri setinin <text> sütununda bulunan kelimeleri küçük harfe dönüştürme adımı uygulanmıştır. Bu işlemin yapılmasının amacı yorum olarak yazılan kelimelerin düzensiz bir şekilde büyük/küçük harf kurallarına uyulmadan yazılmasıdır. Daha doğru bir sonuç elde edilmesi için bütün kelimeler küçük harfe dönüştürülmüştür.

İkinci önişleme kriteri olarak bir kelimenin köküne bakılıp bakılmaması adımı gerçekleştirilmiştir. Bu adımda bir kelimenin köküne bakılması için Snowball Stemmer yöntemi kullanılmıştır. Böylece veri setinde bulunan kelimelerin orijinal halleri ve kelimenin kökünün kullanılması şeklinde iki durum oluşturulmuştur.

Üçüncü önişleme kriteri olarak tek başına kullanıldığında bir anlam ifade etmeyen etkisiz kelimelere bakılmıştır. Genelde konu sınıflandırma çalışmalarında performansa bir etkisi olmadığı için kullanılmayan bu işlem, siber zorbalık tespit yaparken etkisiz kelimelerin kullanılmasının sınıflandırma performansındaki etkisinin araştırılması amacı ile gerçekleştirilmiştir.

Bu çalışmada, yukarıda belirtilen önişlem yöntemlerinin kombinasyonları değerlendirilmiştir. Tüm kelimelerin küçük harfe dönüştürülmesi işleminden sonra kelimelerin kökenine bakılıp bakılmaması; tüm kelimlerin orijinal halinin kullanılması [0], tüm kelimelerin sadece köklerinin alınması [1] ve etkisiz kelimelerin kullanılıp kullanılmaması; etkisiz kelimelerin kullanılması [0], etkisiz kelimelerin kullanılmaması [1] şeklinde 3 önişleme kriteri belirlenerek 4 farklı önişleme durumu Tablo 3.1' de gösterildiği şekilde oluşturulmuştur.

Önişleme Yöntemi	**Kökünü Almama (0)/ Kökünü Alma (1)**	**Etkisiz Kelimelerin Kullanılması (0)/ Etkisiz Kelimelerin Kullanılmaması(1)**
00	0	0
01	0	1
10	1	0
11	1	1

Tablo 3.1 Önişleme Adımlarının Kodlanması

3.2.2. Nitelik Çıkarımı

Bu çalışmada veri setindeki olumlu ve olumsuz mesajlar kullanılarak nitelikler çıkarılmıştır. Nitelikleri ayıklamak için veri setinde yer alan <Text> ve <Cyberbullying> etiketlerinde bulunan mesajlar kullanılmıştır. Bu adımda, nitelikleri ayıklamak metnin her satırı boşluk karakteri ile ayrılır. Bundan sonra nitelikleri elde etmek için önişlem adımları gerçekleştirilmiştir.

Nitelik çıkarma adımından sonra nadir kullanılan kelimelerin ve yanlış yazılan kelimelerin elenmesi için belge frekansı 0.001'in altında olan nitelikler kaldırılmıştır.

3.2.3. Nitelik Seçimi

Nitelik çıkarımı işleminden sonra en iyi nitelik alt kümelerinin seçilmesi gerçekleştirilmiştir. Nitelik seçimi adımında Chi2 nitelik seçimi algoritması kullanılmıştır.

3.2.3.1 Chi2 Nitelik Seçim Yöntemi

Özniteliklerin belirlenmesinde kullanılan Chi2 yöntemi, iki bağımsız kategorik değişken arasında anlamlı bir ilişki olup olmadığını belirleyen istatiksel bir yöntemdir. Chi2 nitelik seçim yöntemi, gözlemlenen her iki değişkenin beklenen frekansları arasında anlamlı bir fark olup olmadığını test ederek bir terimin bir sınıf ile ilişkili olup olmadığını belirlemek amacıyla nitelik seçimlerinde kullanılmaktadır. Bu yöntem, metin madenciliğinde elde edilmiş niteliklere kolaylıkla uygulanabilmektedir.

Ayrıştırma yoluyla özellik seçimi yapan Chi2 testi, çok sınıflı verilerle çalışabilir ve alakasız, gereksiz özellikleri kaldırabilir. Nitelik seçiminde, belirli bir niteliğin ve belirli bir sınıfın ortaya çıkışının bağımsız olup olmadığı test edilmektedir. İki olay bağımlıysa, sınıfın oluşumunu tahmin etmek için bu niteliğin oluşumunu kullanabiliriz. Nitelik oluşumun, sınıfın oluşumuna yüksek ölçüde bağlı olduğu niteliklerin seçilmesi amaçlanmaktadır. Çünkü nitelik ve sınıf oluşumu bağımsız olduğunda, gözlemlenen frekans, beklenen frekansa yakın çıkar ve küçük bir chi2 değeri elde edilir. Dolayısıyla model eğitiminde en iyi chi2 değeri için sınıfla ilişkilendirileceğinden, daha yüksek nitelikler seçilmelidir.

Chi2 testi denklem 3.1'deki formül ile hesaplanır:

$$\sum_{k=1}^{n} \frac{O_k - E_k}{E_k} \tag{3.1}$$

3.2.4. Sınıflandırma

Bu çalışmada, siber zorbalık tespiti için veri setinin sınıflandırılmasında; Naive Bayes, J48, LibSVM, RBFClassifier, SGD, SMO, K-NN, HoeffdingTree, RandomTree, LWL, MultiClassClassifier, RandomForest, RBFNetwork, REPTree, Logistic Regression, VotedPerceptron, DecisionTable algoritmaları ayrı ayrı kullanılmış ve en uygun sınıflandırma algoritmasını tespit etmek için çıkan sonuçlar birbirleriyle karşılaştırılmıştır. Bu bölümde yer alan alt başlıklarda kullanılan sınıflandırma algoritmaları hakkında detaylı bilgi verilmiştir.

Birkaç farklı hipotez için posterior olasılığı hesapladıktan sonra, en yüksek olasılığı olan hipotez seçilmelidir.

3.2.4.1 Naïve Bayes Sınıflandırıcısı

Naïve Bayes algoritması, verilen bir veri setindeki değerlerin sıklığını ve kombinasyonlarını sayarak bir olasılık kümesini hesaplayan basit bir olasılık sınıflandırıcısıdır. Algoritma Bayes teoremini kullanır ve tüm değişkenlerin sınıf değişkeninin değeri göz önüne alındığında bağımsız olduğunu varsayar. Bu şartlı bağımsızlık varsayımı, gerçek dünya uygulamalarında nadiren geçerlidir, dolayısıyla algoritma, çeşitli denetimli sınıflandırma problemlerinde iyi performans sergileme ve hızlıca öğrenme eğilimindedir [59].

Naïve Bayes sınıflandırıcı, Bayes teoremine ve toplam olasılık teoremine dayanmaktadır. f = < $f_1 \ldots f_n$> vektörlü bir f verisi SE hipotezine ait olma olasılığı [60]:

$$\boldsymbol{P(SE \mid f)} = \frac{\boldsymbol{P(f \mid SE) * P(SE)}}{\boldsymbol{P(f)}} \qquad (3.2)$$

***P (SE | d)* :** d Verisi verilen hipotezin olasılığıdır. Buna posterior olasılık denir.
***P (f | SE)* :** h hipotezinin doğru olduğu göz önüne alındığında d verisinin olasılığıdır.
***P (SE)* :** Hipotez h'nin gerçek olma olasılığıdır (veriler ne olursa olsun). Buna h'nin önceki olasılığı denir.

$\boldsymbol{P(f)}$ **:** Verinin olasılığıdır (hipotezden bağımsız olarak) [61].

Birkaç farklı hipotez için posterior olasılığı hesapladıktan sonra, en yüksek olasılığı olan hipotez seçilmelidir.

3.2.4.2. J48 Decision Tree Sınıflandırıcısı

J48, ID3'ün bir uzantısıdır. J48'in ek özellikleri eksik değerleri, karar ağaçları budamasını, sürekli özellik değer aralıklarını, kuralların türetilmesini vb. İçerir. WEKA veri madenciliği aracında J48, C4.5 algoritmasının açık kaynaklı bir Java uygulamasıdır. WEKA aracı, ağaç budama ile ilgili bir dizi seçenek sunar. Potansiyel aşınması durumunda budama, hassaslaştırma için bir araç olarak kullanılabilir. Diğer algoritmalarda sınıflandırma, her bir yaprak saf olana kadar tekrarlı bir şekilde gerçekleştirilir, yani verilerin sınıflandırılması mümkün olduğu kadar mükemmel olmalıdır. Bu algoritma, söz konusu verinin belirli bir kimliğinin üretildiği kuralları oluşturur. Amaç, karar ağacının esneklik ve doğruluk dengesi kazanana kadar aşamalı olarak genelleştirilmesidir [62].

Kazanç sayma süreci, veri bozukluklarının bir ölçüsü olan "Entropi" yi kullanır. Entropisi Denklem 3.3 ve Denklem 3.4 ile hesaplanır:

$$\boldsymbol{Entropi(y)} = -\sum_{\boldsymbol{j=1}}^{\boldsymbol{n}} \frac{|\boldsymbol{y_i}|}{|\boldsymbol{y}|} \boldsymbol{log}\left(\frac{\boldsymbol{y_i}}{\boldsymbol{y}}\right) \tag{3.3}$$

$$\boldsymbol{Entropi(j \mid y)} = \frac{|\boldsymbol{y_j}|}{|\boldsymbol{y}|} \boldsymbol{log}\left(\frac{|\boldsymbol{y_j}|}{|\boldsymbol{y}|}\right) \tag{3.4}$$

Ve kazancı ise Denklem 3.5'deki formül kullanılarak hesaplanır:

$$\boldsymbol{Kazan}\text{ç}(\boldsymbol{y \mid j}) = \boldsymbol{Entropi}\big(\boldsymbol{y} - \boldsymbol{Entropi(j \mid y)}\big) \tag{3.5}$$

3.2.4.3. LibSVM Sınıflandırıcısı

LIBSVM, destek vektör sınıflandırma, (C-SVC, nu-SVC), regresyon (epsilon-SVR, nu-SVR) ve dağılım tahmini (tek-sınıf SVM) için entegre bir yazılımdır. Çok sınıflı sınıflandırmayı destekler [63].

LibSVM, SVM sınıflandırıcısını oluşturmak için LibSVM kullandığından SMO'dan daha hızlı çalışır. LibSVM, kullanıcıların LibSVM aracı tarafından desteklenen One-class SVM, Regressing SVM ve nu-SVM ile deneme yapmalarını sağlar. SVM, hem sınıflandırma hem de regresyon için güçlü bir yöntemdir. Bu operatör, sınıflandırma görevleri için *C-SVC* ve *nu-SVC* SVM tiplerinin yanı sıra regresyon görevleri için *epsilon-SVR* ve *nu-SVR* SVM tiplerini de destekler [63].

Amacımız, diğer alanlardaki kullanıcıların SVM'i bir araç olarak kolayca kullanmalarına yardımcı olmaktır. LIBSVM, kullanıcıların kendi programları ile kolayca bağlayabilecekleri basit bir ara yüz sağlar. LIBSVM'in başlıca özellikleri şunlardır:

- Farklı SVM formülasyonları
- Verimli çoklu sınıflandırma
- Model seçimi için çapraz doğrulama
- Olasılık tahminleri
- Çeşitli çekirdekler (önceden hesaplanmış çekirdek matrisi dahil)
- Dengesiz veriler için ağırlıklı SVM
- Hem C ++ hem de Java kaynakları
- SVM sınıflandırma ve regresyon gösteren GUI

3.2.4.4. Radyal Temel Fonksiyon Sınıflandırıcı (Radial Basis Function Classifier) - RBFClassifier

RBF: Öklid mesafelerini (girişler ve ağırlıklar arasında, merkez olarak görülebilir) ve (genellikle) Gauss aktivasyon fonksiyonlarını (çok değişkenli olabilir) kullanır, bu da nöronları daha yerel olarak hassas yapar. Dolayısıyla, RBF nöronları, merkez / ağırlıklar girdilere eşit olduğunda maksimum aktivasyona sahiptir. Bu özellik nedeniyle, RBF sinir ağları yenilik algılaması için iyidir (eğer her bir nöron bir eğitim örneğine odaklanmışsa, tüm nöronlardan gelen girdiler yeni kalıplar oluşturur), ancak ekstrapolasyonda çok iyi değildir. Ayrıca, RBF'ler öğrenme için geri yayılma veya gizli katmandaki denetimsiz öğrenme ile karma yaklaşımlar kullanabilir (genellikle sadece 1 gizli katmana sahiptirler). Son olarak, RBF'ler eğitim sırasında yeni nöronların büyümesini kolaylaştırır [64].

3.2.4.5. Stokastik Degrade İniş (Stochastic Gradient Descent) – SGD

' *Stokastik* ' kelimesi, rastgele bir olasılık ile bağlantılı olan bir sistem anlamına gelir. Çeşitli doğrusal modelleri (ikili sınıf SVM, ikili sınıf lojistik regresyon, kare kaybı, Huber kaybı ve epsilon duyarsız kaybı doğrusal regresyonu) öğrenmek için stokastik degrade inişini uygular. Global olarak tüm eksik değerleri değiştirir ve nominal özellikleri ikili değerlere dönüştürür. Aynı zamanda tüm özellikleri normalleştirir.

Stokastik Gradyan İnişinde, her bir yineleme için ayarlanan verilerin tamamı yerine rastgele birkaç örnek seçilir. Her bir yinelemeyi gerçekleştirmek için SGD'de sadece tek bir numune kullanır. Numune rastgele karıştırılır ve yinelemeyi gerçekleştirmek için seçilir.

SGD algoritması Denklem 3.6'da gösterilmiştir.

$$\textit{for i in range (m):} \qquad (3.6)$$
$$\boldsymbol{\theta_j = \theta_j - \alpha(\hat{y}^i - y^i)x_j^i}$$

Buna göre, SGD'de, tüm örneklerde maliyet fonksiyonunun gradyanının toplamı yerine her bir yinelemede tek bir örneğin maliyet fonksiyonunun gradyanını buluyoruz.

SGD'de, veri kümesinden yalnızca bir örnek her yineleme için rastgele seçildiğinden, algoritmanın minimaya ulaşmak için kullandığı yol genellikle tipik Gradient İniş algoritmasından daha gürültülüdür. Fakat bu kadar önemli değil çünkü algoritmanın aldığı yol, minimaya ulaştığımız sürece ve önemli ölçüde daha kısa bir eğitim süresinde önemli değil.

3.2.4.6. Sıralı Minimal Optimizasyon (Sequential Minimal Optimization) – SMO

Sıralı Minimal Optimizasyon (SMO), destek vektörünün eğitimi sırasında ortaya çıkan QP problemini çözmek için bir algoritmadır. SMO, büyük QP problemini alt problemlere ayrıştırır. SMO, her adımda çözmek için mümkün olan en küçük optimizasyon problemini seçer. Standart SVM QP problemi için, mümkün olan en küçük optimizasyon problemi iki Lagrange çarpanı içerir, çünkü Lagrange çarpanları doğrusal bir eşitlik sınırına uymak zorundadır. Önce iki çarpan bulur ve sonra onu optimize etmeye çalışır. Bu, yakınsama kriterlerini karşılayana kadar tekrarlanacaktır [65].

SMO algoritması, Osuna vd. tarafından kanıtlanan teoremden faydalanır [66]. Bu algoritma, SVM durumunda iki Lagrang çarpanı içeren en küçük QP problemini çözecektir. SMO eğitim yönteminin en büyük avantajı, adım başına sadece iki Lagrangian çarpanı içermesidir, böylece QP problemini sayısal optimizasyon yapmadan analitik olarak çözebilir. SMO eğitim algoritmasının iki ana bölümü vardır, bu iki Lagrangian çarpanı QP problemini çözerek hangi çarpanların kullanılacağını belirler. İlk önce, çözülecek olan iki Lagrang çarpanı tanımlanmalıdır. Algoritma önce bu çarpanlar üzerindeki kısıtlamaları hesaplar ve sonra kısıtlanan maksimum değeri elde etmektedir [67].

3.2.4.7. K En Yakın Komşu (K Nearest Neighborhood)-KNN Sınıflandırıcısı

Gözetimli Öğrenme metotları sınıflandırıcısıdır. Çapraz onaylamaya göre uygun K değerini seçebilir. Ayrıca mesafe ağırlıklandırma yapabilir. Veri madenciliği ve makine öğreniminde kullanılan birçok (denetimli öğrenme) algoritmalarından biridir, öğrenmenin

diğerlerinden bir veri (vektör) ile ne kadar benzer olduğunu temel alan bir sınıflandırma algoritmasıdır.

KNN, sınıflandırılmamış verileri diğerleriyle karşılaştırmaz, sınıflandırmayı yapan veriler arasındaki mesafeyi ölçmek için matematiksel bir hesaplama yapar. Bu matematiksel hesaplar ise Öklit Mesafesi ve Manhattan Uzaklığı'dır. Öklit Mesafesi'nde ve Manhattan Uzaklığı'nda örnek olarak bir K=3 değeri seçilir ve ona en yakın sınıflandırılmış komşulardan en yakın 3 tanesi alınır. Önceden sınıflandırılmış bu elemanlar hangi sınıfa dahilse yeni eleman da o sınıfa dahil edilir. Mesafe hesabında genelde bu kullanılmaktadır. Mesafe fonksiyonlarının formülü Denklem 3.7, Denklem 3.8, Denklem 3.9 şeklindedir:

$$\boldsymbol{Euclidean} = \sqrt{\sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} (\boldsymbol{x_i} - \boldsymbol{y_i})^2} \tag{3.7}$$

$$\boldsymbol{Manhattan} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{l}} | \boldsymbol{x_i} - \boldsymbol{y_{i|}} \tag{3.8}$$

$$\boldsymbol{Minhowski} = \left(\sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} (|\boldsymbol{x_i} - \boldsymbol{y_i}|)^{\boldsymbol{q}}\right)^{\boldsymbol{1/q}} \tag{3.9}$$

Denklemlerde x_i değeri ve $\boldsymbol{y_i}$ değeri mesafe ölçümü yapılacak özelliklerdir. Bu hesaplar yapıldıktan sonra sonuçlar ne kadar küçük olursa, çıkan sonuç istenen sonucun sınıfa dâhil olur.

3.2.4.8. Hoeffding Ağacı (Hoeffding Tree) Sınıflandırıcısı

Bir Hoeffding Ağacı (VFDT), dağıtım üreten örneklerin zaman içinde değişmediğini farz ederek, büyük veri akışlarından öğrenme yeteneğine sahip, artımlı, her zaman karar ağacı indüksiyon algoritmasıdır. Hoeffding ağaçları, küçük bir örneğin genellikle en iyi bölme özelliğini seçmek için yeterli olabileceği gerçeğinden yararlanır. Bu sınıflandırma yönteminin ilgi çekici özelliği ise verdiği performans garantisidir. Hoeffding

ağacı tarafından öğrenilen model, eğer eğitim durumlarının sayısı yeterince büyükse, artımlı olmayan bir öğrenen tarafından yapılan modelle neredeyse aynıdır.

3.2.4.9. Random Tree Sınıflandırıcısı

Random Tree(Rastgele Ağaçlar), Leo Breiman ve Adele Cutler tarafından tanıtılan denetimli bir sınıflandırıcıdır ve genellikle makine öğrenmesiyle ilgisi olmayan rastgele oluşturulmuş ağaçları ifade etmektedir. Bir karar ağacı oluştururken rastgele bir veri seti oluşturmak için torbalama fikrini kullanmaktadır. Bu algoritma hem sınıflandırma hem de regresyon problemleriyle ilgilenebilir. Rastgele ağaçlar, orman denilen ağaç kestiriciler topluluğudur. Rastgele Ağaçlar, esasen Makine Öğreniminde var olan iki algoritmanın birleşimidir: Tekli Model ağaçlar Rastgele Orman fikirleriyle birleştirilir. Model ağaçlar, her bir yaprağın bu yaprak tarafından açıklanan yerel alt alan için optimize edilmiş doğrusal bir modele sahip olduğu karar ağaçlarıdır [68].

Sınıflandırma şu şekilde çalışır: rastgele ağaçlar sınıflandırıcısı giriş özelliği vektörünü alır, ormandaki her ağaçla sınıflandırır ve "oyların" çoğunluğunu alan sınıf etiketini çıkarır. Bir gerileme durumunda, sınıflandırıcı tepkisi ormandaki tüm ağaçlar üzerindeki tepkilerin ortalamasıdır. Bütün ağaçlar aynı parametrelerle fakat farklı eğitim takımlarında eğitiliyor. Bu setler önyükleme prosedürü kullanılarak orijinal eğitim setinden üretilir: her eğitim seti için rastgele orijinal setindeki (= N) aynı sayıda vektörü seçersiniz. Vektörler değiştirme ile seçilir. Yani, bazı vektörler bir kereden fazla gerçekleşecek ve bazıları bulunmayacak. Her eğitimli ağacın her düğümünde, tüm değişkenler en iyi bölünmeyi bulmak için kullanılmaz, ancak bunların rasgele bir alt kümesini kullanır. Her düğümde yeni bir alt küme oluşturulur. Ancak, büyüklüğü tüm düğümler ve tüm ağaçlar için sabittir. Varsayılan olarak XXX olarak ayarlanmış bir eğitim parametresidir. Yapılan ağaçların hiçbiri budanmaz.

3.2.4.10. Yerel Ağırlıklı Öğrenme (Locally Weighted Learning) - LWL Sınıflandırıcısı

Yerel Ağırlıklı Öğrenme, geçerli ilgi noktası çevresinde yaklaşık bir yerel model kullanarak bir tahmin yapılan bir fonksiyon yaklaşımı teknikleri sınıfıdır. Fonksiyon yaklaşımı ve regresyonun amacı, girdi ile çıktı arasındaki ilişkiyi bulmaktır. Denetimli bir öğrenme probleminde, her bir girişin bir çıktıyla ilişkilendirildiği eğitim verileri, gerçek işleve yaklaşan değerleri öngören bir model oluşturmak için kullanılır. Bu modellerin tümü, küresel işlevi türetmek için eksiksiz eğitim verileri kullanır. Bununla birlikte, küresel yöntemlerin bir dezavantajı, bazen hiçbir parametre değerinin yeterli bir yaklaşıklık sağlayamayacağıdır. Ayrıca bu gibi durumlarda hesaplama maliyetleri de çok yüksektir.

Global fonksiyon yaklaşımına bir alternatif Lokal Ağırlıklı Öğrenme'dir (LWL). LWL yöntemleri parametrik değildir ve mevcut tahmin yalnızca bir veri alt kümesi kullanan yerel işlevlerle yapılır. LWL'nin arkasındaki temel fikir, tüm fonksiyon alanı için küresel bir model oluşturmak yerine, her bir ilgi çekici nokta için, sorgu noktasının komşu verilerine dayanarak yerel bir model oluşturulmasıdır [69].

LWL'nin temel maliyet fonksiyonu Denklem 3.10'da gösterildiği gibidir:

$$\boldsymbol{J = \frac{1}{2}\sum_{i=1}^{n} w_i(x_q)\left(y_i - x_i\beta_q\right)^2} \qquad (3.10)$$

3.2.4.11. Çok Sınıflı (MultiClass) Sınıflandırıcısı

Çok sınıflı sınıflandırma, ikiden fazla sınıf içeren bir sınıflandırma görevi anlamına gelmektedir. Örneğin, portakal, elma veya armut olabilen bir dizi meyvenin sınıflandırılması. Çok sınıflı sınıflandırma, her numunenin bir ve sadece bir etikete atandığı varsayımını yapar: bir meyve hem elma hem de armut olabilir, ancak her ikisi de aynı anda olamaz

Her eğitim noktası N farklı sınıflardan birine aittir. Amaç, yeni bir veri noktası verildiğinde, yeni noktanın ait olduğu sınıfı doğru şekilde tahmin edecek bir fonksiyon oluşturmaktır. Noktaların ait olduğu birden fazla kategorinin olduğu birçok senaryo vardır,

ancak verilen bir nokta birden fazla kategoriye ait olabilir. En temel haliyle, bu problem önemsiz bir şekilde ikili sınıflandırma tekniklerini kullanarak doğal olarak çözülebilen bir dizi bağlantısız ikili problemde ayrışır. Her N sınıfı için pi (x) yoğunluğunu bildiğimizi varsayalım. Ardından 3.11'deki fonksiyonu kullanarak tahmin ediyoruz [70]:

$$\boldsymbol{f(x) = \arg\max p_i(x)} \qquad (3.11)$$
$$\boldsymbol{i \in 1, .., N}$$

Yoğunluklar bilinmez ancak klasik teknikler kullanılarak tahmin edilebilir. Yoğunluğu tahmin etmek, özellikle sınırlı veri içeren yüksek boyutlarda zordur.

3.2.4.12. Rastgele Orman (Random Forest) Sınıflandırıcısı

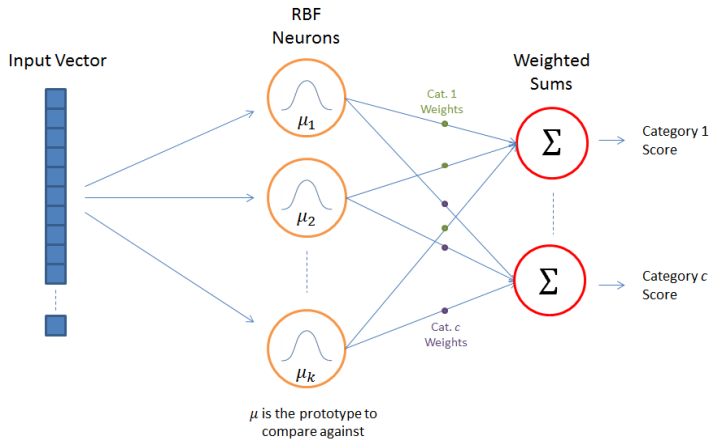
Rastgele Orman (Random Forest), hiper parametre ayarı olmasa da, çoğu zaman mükemmel sonuç veren esnek, kullanımı kolay bir makine öğrenme algoritmasıdır. Aynı zamanda en çok kullanılan algoritmalardan biridir, çünkü basitliği ve hem sınıflandırma hem de regresyon görevleri için kullanılabilmektedir.

Random Forest algoritması Karar ağacı gibi hem Sınıflandırma hem de Regresyon için kullanılabilir. Aynı zamanda en esnek ve kullanımı kolay bir algoritmadır. Bir orman ağaçlardan oluşur. Sahip olduğu ağaç sayısı ne kadar fazlaysa orman o kadar sağlamdır. Rastgele ormanlar, rastgele seçilen veri örnekleri üzerinde karar ağaçları oluşturur, her ağaçtan tahmin alır ve oylama yoluyla en iyi çözümü seçer. Ayrıca, özellik öneminin oldukça iyi bir göstergesidir. Bir sonuç üreteceği zaman bu karar ağaçlarındaki ortalama değer alınır ve sonuç üretilir.

3.2.4.13. Radyal Temel Fonksiyon Ağı (Radial Basis Function Network) - (RBFN) Sınıflandırıcısı

Bir Radyal Temel Fonksiyon Ağı (RBFN), belirli bir sinir ağı türüdür. RBFN yaklaşımı MLP'den daha sezgiseldir. Bir RBFN, girişin eğitim setindeki örneklerle olan benzerliğini ölçerek sınıflandırma yapar. Her RBFN nöronu, eğitim setindeki örneklerden sadece biri olan bir "prototip" depolar. Yeni bir girişi sınıflandırmak istediğimizde, her bir

nöron, giriş ile prototipi arasındaki Öklid mesafesini hesaplar. Kısaca giriş, A sınıfı prototiplere B sınıfı prototiplerden daha çok benziyorsa, A sınıfı olarak sınıflandırılır.



Şekil 3.7 RBF Ağ Mimarisi

Yukarıdaki çizim bir RBF Ağı'nın tipik mimarisini göstermektedir. Bir giriş vektöründen, bir RBF nöron katmanından ve kategori veya veri sınıfı başına bir düğüme sahip bir çıkış katmanından oluşur.

3.2.4.14. REPTree Sınıflandırıcısı

RepTree, regresyon ağacı mantığını kullanır ve farklı yinelemelerde birden fazla ağaç oluşturur. Bundan sonra üretilen tüm ağaçlardan en iyisini seçer. Bu temsilci olarak kabul edilecektir. Ağacın budamasında kullanılan ölçü, ağacın öngördüğü ortalama karedeki hatadır. Temelde Azaltılmış Hata Budama Ağacı ("REPT") hızlı karar ağacı öğrenmesidir ve bilgi kazanımına veya varyansı azaltan bilgilere dayanarak bir karar ağacı oluşturur. REP Ağacı, ayrıştırma ölçütü olarak bilgi kazancını kullanarak bir karar / regresyon ağacı oluşturan ve azaltılmış hata budaması kullanarak budama yapan hızlı bir karar ağacı öğrenicisidir. Sayısal niteliklerin değerlerini yalnızca bir kez sıralar. Eksik değerler C4.5'in kesirli örnekleri kullanma yöntemi kullanılarak ele alınmaktadır. REP Ağacı algoritması örneği UCI deposuna uygulanır ve karışıklık matrisi altı olası değere sahip sınıf cinsiyet için üretilir [71].

3.2.4.15. Logistic Regression Sınıflandırıcısı

Lojistik Regresyon, “Sınıflandırma” görevlerine adanmış “Denetimli” Makine Öğrenimi (ML) yöntemlerinde kategorize edilmiş bir “İstatistik Öğrenme” tekniğidir. Sınıflandırma için adı “Regresyon” kelimesini içeren bir sınıflandırıcı tanımladığımızda bir çelişki ortaya çıkmaktadır. Bunun iyi tarafı ise ayrık ikili çıktılar üretmek için doğrusal bir regresyon denklemi kullanmaktır.

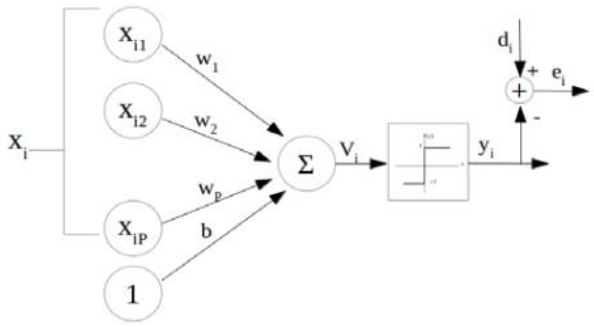
X_{ij} girişleri, K uzunluğunun sürekli özellik vektörleridir (x_is), burada j = 1… k ve i = 1…n. Bu nedenle, giriş matrisi, N sayısı olan girişleri (veri noktaları) içeren X'tir ve her biri K sayısı özelliğini içerir. Girişler aşağıdaki gibi bir matris X olarak gösterilebilir:

$$\boldsymbol{X} = \begin{bmatrix} \boldsymbol{x_{11}} & \cdots & \boldsymbol{x_{1k}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{x_{n1}} & \cdots & \boldsymbol{x_{nk}} \end{bmatrix}_{\boldsymbol{nxk}}, \boldsymbol{Y} = \begin{bmatrix} \boldsymbol{y_1} \\ \vdots \\ \boldsymbol{y_n} \end{bmatrix}_{\boldsymbol{nx1}}$$

Çıktı y_i , y ∈ {0,1} olacak şekilde ayrık ve ikili değişkendir. Böylece, y_i 'nin Bernoulli olduğunu ve olasılık parametresi p_i ile dağıldığını varsayabiliriz.

3.2.4.16. Voted Perceptron Sınıflandırıcısı

Oylanmış bir Perceptron, Rosenblatt'ın algı algoritmasını Helmbold ve Warmuth'un bir kez dışarıda bırakma yöntemiyle birleştiren doğrusal sınıflandırma için bir algoritmadır [72]. Öğrenme sürecinde karşılaşılan tüm ağırlık vektörleri bir oylamaya oy verir. Ağırlık vektörünün doğru şekilde sınıflandırıldığı ardışık deneme sayısına göre ağırlık vektörünün doğruluğunun bir ölçüsü, ağırlık vektörüne verilen oy sayısı olarak kullanılabilir. Oylanan Perceptron'un mimarisi Şekil 3.8'de verilmiştir.



Şekil 3.8 Voted Perceptron Mimarisi

Voted Perceptron'un çıktısı Denklem 3.12'deki gibi hesaplanır:

$$y_i = sgn\{\sum_{p=0}^{p} c_p sgn(w_p x_{i,p})\} \quad (3.12)$$

Burada $x_{i,p}$ girişler, w_p ağırlıklar, v_i tahmin vektörü, y_i öngörülen sınıf etiketi, d_i istenen etiket ve e_i hatadır.

Eğitimin sonucu, w_p'nin hayatta kalma süresi c_p ile birlikte w_p'nin lineer ayırıcıları $w_1, w_2, \ldots w_p$'nın bir toplamıdır. Bu w_p'nin güvenilirliğinin bir ölçüsüdür.

Voted Perceptron'un kısaltması, eğitim süresinin genellikle sınırsız olduğu ve eğitim verilerinin boyutuna ve karmaşıklığına bağlı olmasıdır. "algoritma mükemmel bir çözüm bulunana kadar yinelenir, ancak yalnızca veriler doğrusal olarak ayrılırsa düzgün çalışır" [73]. Eğitim sırasında yanlış sınıflandırılmış bir örnek bulunduğunda, hiper düzlem değiştirilir ve yanlış kategorize edilmiş örnekler yeniden sınıflandırılır. Veriler doğrusal olarak ayrılabilirse, yineleme sayısı sonludur. Aksi takdirde, algoritma sonsuz döngüde olacaktır; bu nedenle, maksimum sayıda yineleme belirtilmelidir [74].

3.2.3.17. Karar Tabloları (Decision Table) Sınıflandırıcısı

Karar tabloları karmaşık mantığı modellemek için kullanılır. Tüm olası koşul kombinasyonlarının göz önüne alındığını ve şartların gözden kaçırılması durumunda bunu görmenin kolay olduğunu görmeyi kolaylaştırabilirler.

Bir karar tablosunda, koşullar genellikle doğru (T) veya yanlış (F) olarak ifade edilir. Tablodaki her sütun, iş mantığında, işlemlerle sonuçlanacak benzersiz koşulların kombinasyonunu açıklayan bir kurala karşılık gelir.

Karar tablolarını kullanmanın bir avantajı, aksi halde bulunmayan ve bu nedenle test edilmemiş veya geliştirilmemiş koşulların kombinasyonlarını tespit etmeyi mümkün kılmalarıdır. Gereksinimler çok daha netleşir ve genellikle gereksinimlerin yalnızca metin olarak ifade edildiğinde görülmesi zor olan bazı gereksinimlerin mantıksız olduğunu fark edersiniz.

Tekniğin bir dezavantajı, bir karar tablosunun, hangi sırada ne yapılması gerektiğine dair adım adım talimatları içeren test durumlarının tamamlanmasına eşdeğer olmamasıdır. Bu ayrıntı seviyesine ihtiyaç duyulduğunda karar tablosunun test durumlarına daha ayrıntılı bir şekilde dahil edilmesi gerekmektedir.

Karar tabloları, sonucun farklı seçeneklerin kombinasyonlarına bağlı olduğu ve genellikle çok sık olduğu durumlarda tüm durumlarda kullanılabilir. Pek çok sistemde karar tablolarının çok fazla değer kattığı tonlarca iş kuralı vardır.

4. BULGULAR

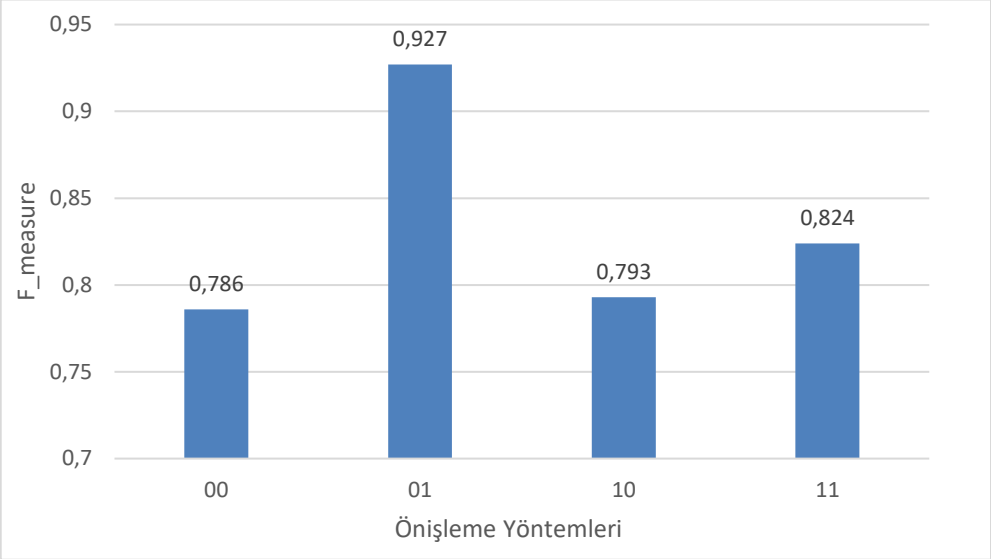
Bu bölümde önerilen yöntemlerin deneysel sonuçları sunulmuştur. Bu tez çalışmasında gerçekleştirilen siber zorbalık tespiti için veri setinin ön işleme, nitelik çıkarımı ve nitelik seçimi adımlarında Knime programı kullanılmıştır. Sınıflandırma adımı için kullanılan Naive Bayes, J48, LibSVM, RBFClassifier, SGD, SMO, K-NN, HoeffdingTree, RandomTree, LWL, MultiClassClassifier, RandomForest, RBFNetwork, REPTree, Dld4jMlpClassifier, VotedPerceptron, DecisionTable yöntemleri WEKA aracında gerçekleştirilmiştir.

Yapılan deneysel çalışmada birçok önişleme ve sınıflandırma yöntemi denenmiştir. Deneylerde Formspring.me platformundan elde edilen yorum iletileri kullanılmıştır. Bu bölümün alt başlıklarında, gerçekleştirilen deneysel sonuçlar sırasıyla aktarılmaktadır.

4.1 Önişleme Adımlarının Karşılaştırılması ve Sınıflandırma Yönteminin Belirlenmesi

Bu analiz çalışmasında yapılan, Bölüm 3.2.1'de anlatılan önişleme yöntemlerinin veri seti için sınıflandırma performansı üzerindeki etkisi araştırılmıştır. Önişleme yöntemleri sınıflandırma performansını etkileyebileceği için en iyi önişleme yöntemi belirlenmiştir. Her bir önişlemin F-ölçüt değeri SGD sınıflandırma yöntemi kullanılarak karşılaştırılmıştır ve Şekil 4.1'de sunulmuştur.

Şekil 4.1'de belirtilen önişleme kodlarının ilk basamağı kelimenin kökünün alınıp alınmadığı, ikinci basamağı etkisiz kelimelerin çıkarılıp çıkarılmadığını temsil etmektedir. Bu önişleme kodlarına göre nitelikler çıkarılarak nitelik vektörü oluşturulur. Daha sonra sınıflandırma performansına etkisi olmayacak nadir bulunan veya yanlış yazılmış nitelikleri kaldırmak için %0.1 belge frekans filtrelemesi uygulanmıştır. Formspring.me veri setinin önişleme yöntemlerine göre uygulanan sınıflandırma performansı sonuçları Şekil 4.1'de sunulmuştur.



Şekil 4.1 Önişleme yöntemlerinin sınıflandırma performansı karşılaştırılması(F-ölçütü)

Şekil 4.1'de grafiğe göre önişleme yöntemlerinin F-ölçüt değeri incelendiğinde 01 ve 11 yöntemi benzer sonuçlar göstermektedir. Fakat 01 yönteminin çok az bir farkla daha iyi performans verdiği görülmektedir.

Tabo 4.1'de gösterildiği gibi en iyi önişleme yöntemi 01 yani kelimelerin kökünü almayıp, etkisiz kelimeleri çıkararak uygulanan yöntemdir. En kötü önişleme yöntemi ise 00 yani kelimelerin kökünü almama ve etkisiz kelimeleri çıkarmadan uygulanan yöntemdir.

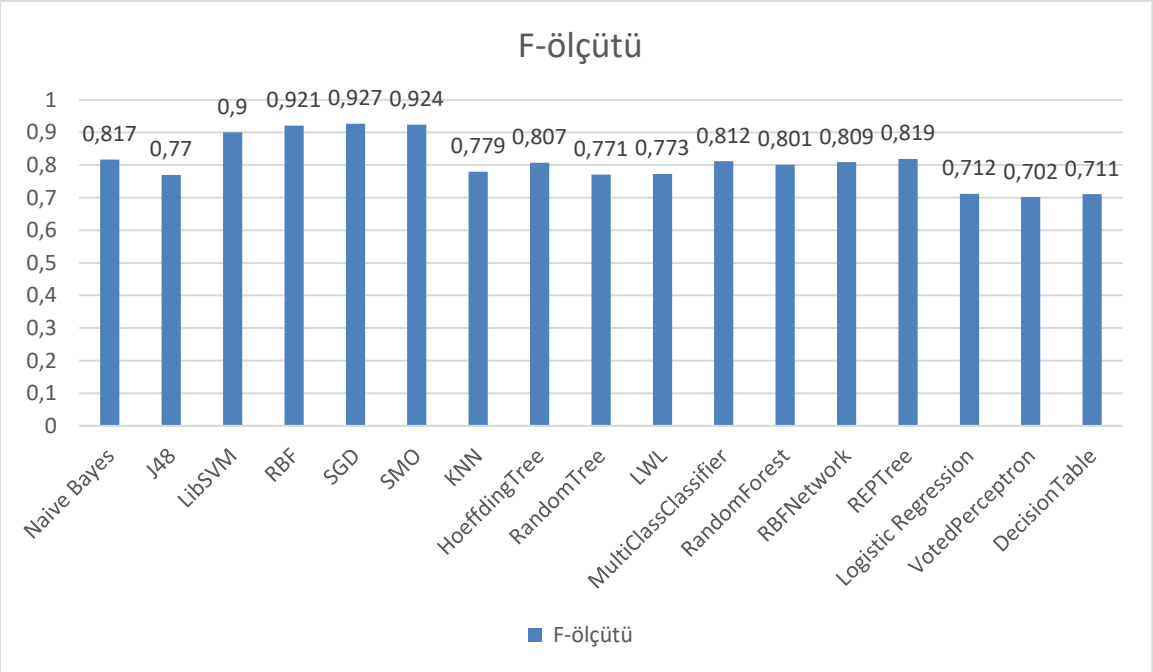
Veri Kümesi	**En İyi Yöntem**	**En İyi F_ölçütü**	**En Kötü Yöntem**	**En Kötü F_ölçütü**
Formspring.me	01	0,927	00	0,786

Tablo 4.1 SGD sınıflandırıcısı uygulanarak en yüksek ve en düşük performans önişleme yöntemlerinin F-ölçüt değeri

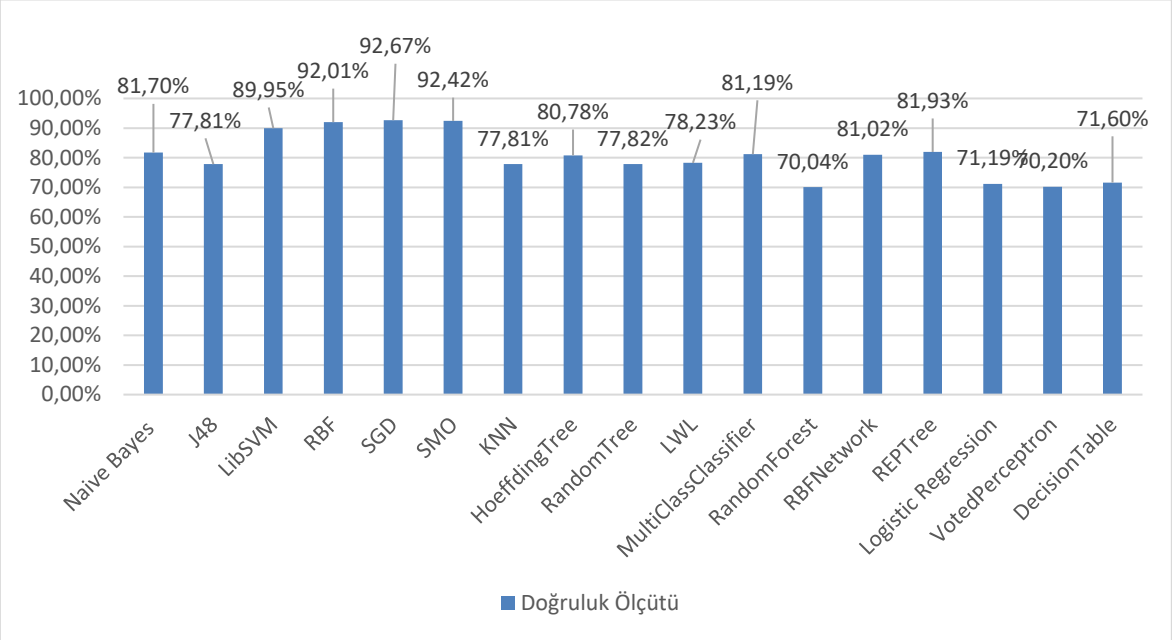
4.2 Sınıflandırıcı Çeşitlerinin Performans Analizi

Bu bölümünde siber zorbalık tespiti için kullanılan sınıflandırıcıların performans karşılaştırmaları gerçekleştirilmiştir. Veri kümesi için Naive Bayes, J48, LibSVM, RBFClassifier, SGD, SMO, K-NN, HoeffdingTree, RandomTree, LWL, MultiClassClassifier, RandomForest, RBFNetwork, REPTree, Logistic Regression, VotedPerceptron, DecisionTable sınıflandırma yöntemleri kullanılmıştır. Bölüm 4.1'de anlatılan 01 önişlemi uygulandıktan sonra sınıflandırıcılar için WEKA metin madenciliği aracı kullanılmıştır.

Gerçekleştirilen sınıflandırma sonuçları Şekil 4.2 ve Şekil 4.3 'te gösterilmiştir.



Şekil 4.2 Formspring.me veri setine uygulanan sınıflandırıcı yöntemlerinin F-ölçütü karşılaştırılması



Şekil 4.3 Formspring.me veri setine uygulanan sınıflandırıcı yöntemlerinin doğru sınıflandırılmış örnekler yüzde karşılaştırılması

Şekil 4.2 ve Şekil 4.3 incelendiğinde sınıflandırma performanslarından en iyi F-ölçütü ve doğruluk oranı sonucunun SGD sınıflandırıcısının verdiği görülmektedir. En kötü sonucu ise Voted Perceptron sınıflandırıcısı vermektedir.

Sınıflandırıcıların sadece doğruluk ölçütüne göre değerlendirmek hatalı sonuç verebilir. Bir sınıflandırmanın doğruluğu kadar sınıflandırma hızı da önemli olduğu için sınıflandırıcıların sınıflandırma süreleri Tablo 4.2'de gösterilmiştir.

Sınıflandırıcı	Süre Performansı(sn)	Sınıflandırıcı	Süre Performansı (sn)
Naive Bayes	20.48	**HoeffdingTree**	437
J48	38.74	**RandomTree**	189.21
LibSVM	69.82	**LWL**	98.09
RBFClassifier	107.84	**MultiClassClassifier**	127.13
SGD	24.67	**RandomForest**	184.91
SMO	45.28	**RBFNetwork**	25
K-NN	22.54	**REPTree**	76.93
Logistic Regression	67.55	**DecisionTable**	121
VotedPerceptron	161.11		

Tablo 4.2 Sınıflandırıcıların Süre Performansları (sn)

Tablo 4.2'deki süreler incelendiğinde HoeffdingTree algoritmasının çok yavaş kaldığı NaiveBayes algoritmasının en hızlı algoritma olduğu görülmektedir. SGD sınıflandırıcısının ise hem yüksek doğrulukta hem de süre performansının kabul edilebilir seviyede olduğu görülmektedir.

5. SONUÇLAR VE TARTIŞMA

Bu tez çalışmasında, sosyal ağların kullanımının son yıllarda büyük bir artış göstermesi sebebiyle yaşanan siber zorbalığın makine öğrenmesi algoritmaları ile tespit edilmesi ve sınıflandırılması üzerine çalışılmıştır. Formspring.me platformundan elde edilen veri seti kullanılmıştır. Veri setine önişleme, nitelik çıkarımı, nitelik seçimi uygulanarak siber zorbalığı tespit etmek için farklı sınıflandırma algoritmalarının performansları karşılaştırılmıştır.

İlk olarak veri setine farklı önişleme adımları uygulanarak siber zorbalık tespiti için gerçekleştirilen yöntemlerin etkileri gösterilmiştir. Bu adımdan sonra nitelik çıkarımı adımı için veri setine 0.001 belge frekansı uygulanarak belge frekansı değeri altında kalan nitelikler çıkarılmıştır. Daha sonra nitelik seçimi adımı gerçekleştirilmiş ve bu adımda Chi2 nitelik seçme algoritması kullanılmıştır. Son olarak makine öğrenme algoritmalarının uygulanarak sınıflandırma performansları karşılaştırılmıştır.

Önişleme adımında 2 farklı özellik kullanılarak 4 farklı kombinasyonun etkileri araştırılmıştır. Bu adımda kelimenin kökünü alıp/almama, etkisiz kelimeleri çıkarma/çıkarmama şeklinde kriterler uygulanmıştır. Bu kriterler içerisinde en etkili sonucu tespit edebilmek için SGD sınıflandırıcısı uygulanmıştır ve çıkan sonuçlara göre kelimenin kökünü almadan, etkisiz kelimeleri çıkartarak yani 01 yöntemi seçilmiştir.

Bu işlemler gerçekleştirildikten sonra nitelik çıkarımı ve Chi2 nitelik seçme algoritması uygulanarak farklı sınıflandırma algoritmalarının performansları ve süre performansları ölçülmüştür. Naive Bayes, J48, LibSVM, RBFClassifier, SGD, SMO, K-NN, HoeffdingTree, RandomTree, LWL, MultiClassClassifier, RandomForest, RBFNetwork, REPTree, Dld4jMlpClassifier, VotedPerceptron, DecisionTable algoritmalarından RBFClassifier ve SGD algoritmalarının doğruluk değerleri birbirine yakın çıkmıştır fakat bir sınıflandırıcı için sadece doğruluk değeri değil sürelerininde değerlendirilmesi gerektiği için en hızlı ve en doğru sonucun SGD sınıflandırıcısının verdiği gözlemlenmiştir.

6. ÖNERİLER

Bu çalışmada kullanılan veri setine gerçekleştirilen işlemler sonucunda etkisiz kelimelerin çıkarılmasının sınıflandırıcıların performansı için olumlu bir etki oluşturduğunu söyleyebiliriz. Kullanılan sınıflandırıcılardan SGD ve RBFClassifier algoritması daha doğru sonuç vermiştir fakat RBFClassifier, yavaş bir algoritma olduğu için farklı bir örneği gerçekleştirmek açısından daha fazla zaman gerektirebilir. Bu nedenle SGD algoritmasının en doğru sonucu ve en hızlı sonucu verdiğini söyleyebiliriz.

KAYNAKLAR

[1] **Gökler, R.** , 2009. Okullarda Akran Zorbalığı, *Uluslararası İnsan Bilimleri,* cilt 6, no.2, s. 511-537.

[2] **Hinduja**, **S. P. J. W.,** 2008. Cyberbullying: An exploratory analysis of factors related to off ending and victimization, *Deviant behavio,* volume 29, no. 2, p.129-156.

[3] Children and parents:Media use and attitudes report, ofcom, 2018.

[4] Pearson Student Mobile Device Survey 2015, pearson, 2015.

[5] **Çürük**, **E.,** 2018. Sosyal Ağlardaki Siber Zorbalığın Yapay Zeka Algoritmaları İle Tespiti Ve Sınıflandırılması, s. 25, 2018.

[6] Hirsch, M. Larissa, 2014. Cyberbullying, https://kidshealth.org/en/parents/cyberbullying.html.

[7] **Y. E. N. Ç. Adem Peker**, 2012. Boyun eğici davranışlar ile siber zorbalık ve siber mağduriyet arasındaki ilişkide cinsiyetin aracılığının incelenmesi, Uluslararası İnsan Bilimleri Dergisi.

[8] Russell, B. , 2017. Cyberbullying and Social Media, https://www.hastac.org/blogs/bahatiakili/2017/12/02/cyber-bullying-and-social-media.

[9] Social Media Fact Sheet, 2018. https://www.pewinternet.org/fact-sheet/social-media/.

[10] **Bingöl**, **T. T. N. ,** 2014. Siber zorba ve mağdur olma ile algılanan sosyal destek, Akademik Bakış Uluslararası Hakemli Sosyal.

[11] What to do if you're being bullied on a social network, https://www.bullying.co.uk/cyberbullying/what-to-do-if-you-re-being-bullied on-a-social-network/

[12] **Label, D. t.** , 2014. The, Wireless Report: Key Cyber Bullying and Sexting Statistics.

[13] **Juvonen, G. E.** , 2008. Extending the school grounds?—Bullying experiences in cyberspace.

[14] **TOPCU UZER, İ. T. Ç.** , 2017. Siber Zorbalığı Önleme ve Müdahale Programları: Ulusal Bir Alanyazın Taraması, *Eğitim Fakültesi Dergisi,* cilt 1, no. 17, s. 4.

[15] **Smith, P. K.** , 2012. Cyberbullying: Challenges and opportunities for a research program, *Research Gate,* volume 9, no. 5, p. 554.

[16] **Li, Q.** , 2007. New bottle but old wine: A research of cyberbullying in schools, *ScienceDirect*, volume 23, no. 4, pp. 6-7.

[17] **Li, Q.** , 2010. Cyberbullying in High Schools: A Study of Students' Behaviors and Beliefs about This New Phenomenon, *Journal of Aggression, Maltreatment and Trauma*, volume 19, no. 4, pp. 372-392.

[18] **Dadvar, F. d. J. R. O. D. T. M.** , 2012. Improved Cyberbullying Detection Using Gender Information, *12th -Dutch-Belgian Information Retrieval Workshop*.

[19] **Szuster, J. B. M. K. A.** , 2016. In search of a simple method: Is a human face an effective, automatic filter ınhibiting cyberbullying?, pp. 379-402.

[20] **Çürük, E.** , 2018. Sosyal Ağlardaki Siber Zorbalığın Yapay Zeka Algoritmaları İle Tespiti ve Sınıflandırılması, ss. 1-8.

[21] Shetty, B. , 2018. Supervised Machine Learning: Classification, 12 December. [Çevrimiçi]. Available: https://towardsdatascience.com/supervised-machine-learningclassification-5e685fe18a6d.

[22] Unsupervised Machine Learning, 2018. [Çevrimiçi]. Available: https://www.datarobot.com/wiki/unsupervised-machine-learning/.

[23] **Mohri, A. R. A. T. M**. , 2012 Foundations of machine learning.

[24] **Nguyen, K. S. T.** , 2013. Text Classification of Technical Papers Based on Text Segmentation, *Natural Language Processing and Information Systems, pp*. 278-284.

[25] **Deng, X. L. L.** , 2013. Machine Learning Paradigms for Speech Recognition: An Overview, *IEEE Transactions on Audio, Speech, and Language Processing*, volume 21, no. 5, pp. 1060-1089.

[26] **Siswanto, A. N. M. G. A.** , 2014. Implementation of face recognition algorithm for biometrics based time attendance system, *International Conference on ICT For Smart Society (ICISS)*.

[27] **Chen, X. H. Z.** , 2017. End-to-end learning for lane keeping of self-driving cars, *2017 IEEE Intelligent Vehicles Symposium (IV)*.

[28] **Yong, M. H. A. T. S. ,** 2008. Ranking Web Pages Using Machine Learning Approaches, *IEEE/WIC/ACM International Conference on Web*.

[29] **Wei, L. Q. D. J. W. Z. M. K. Z.** , 2010. "Research on the collaborative filtering recommendation algorithm in ubiquitous computing, *8th World Congress on Intelligent Control and Automation.*.

[30] **Kononenko, I.** , 2011. Machine learning for medical diagnosis: history, state of the art, *Artificial Intelligence in Medicine*, volume 23, no. 1, pp. 89-109.

[31] **Jordan, M.** , 2007. Statistical Machine Learning and Computational Biology, *IEEE International Conference on Bioinformatics and Biomedicine (BIBM 2007).*

[32] **Thangavel, P. B. A. S. S.** , 2017. Student placement analyzer: A recommendation system using machine learning, *4th International Conference on Advanced Computing and Communication Systems (ICACCS-2017).*

[33] Rouse, M. , 2018. text mining (text analytics), Mayıs. [Çevrimiçi]. Available: https://searchbusinessanalytics.techtarget.com/definition/text-mining.

[34] What is NLP Text Mining?, [Çevrimiçi]. Available: https://www.linguamatics.com/what-is-text-mining-nlp-machine-learning.

[35] About text mining, 2019. [Çevrimiçi]. Available: https://www.ibm.com/support/knowledgecenter/en/SS3RA7_18.2.1/ta_guide_ddita/textmining/shared_entities/tm_intro_tm_defined.html.

[36] R. Shaikh, Feature Selection Techniques in Machine Learning with Python, 28 January 2018. [Çevrimiçi]. Available: https://towardsdatascience.com/feature-selection-techniques-in-machine-learning-with-python-f24e7da3f36e.

[37] Text Classification, [Çevrimiçi]. Available: https://monkeylearn.com/text-classification/.

[38] What is Cyberbullying, 12 December 2018. [Çevrimiçi]. Available: https://www.ditchthelabel.org/what-is-cyberbullying/?gclid=CjwKCAjw27jnBRBuEiwAdjQXDOxji3m18XuRn2EN_G7mAxv9VkhXbr_PIu1q8qhejMNxGMpeGaDiTxoCvDgQAvD_BwE.

[39] U. F. P. Common Sense Media, Cyberbullying: What You Need to Know, 27 April 2015. [Çevrimiçi]. Available: https://www.understood.org/en/friends-feelings/child-social-situations/online-activities-social-media/cyberbullying-what-you-need-to-know.

[40] **G. T. Z. H. M. D. Başak Solmaz**, 2013. İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama, s. 26.

[41] H. We Are Social, Digital 2019: Global Internet Use Accelerates, 30 October 2019. [Çevrimiçi]. Available: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates.

[42] **GÖKÇE, M.** , Yeni Medya ve Sanal-Siber Zorbalık, *Academia*, s. 17.

[43] **Noviantho, S. I. ,. L. A. H.** , 2017. Cyberbullying classification using text mining, *1st International Conference on Informatics and Computational Sciences (ICICoS)*.

[44] **Dinakar, R. R. a. H. L. K.** , 2011. Modeling the Detection of Textual Cyberbullying, p. 15.

[45] **Kelly, A. K. L. E. Reynolds** , 2011. Using Machine Learning to Detect Cyberbullying, p. 37.

[46] **Sanchez, S. K. Huascar**, 2011. Twitter Bullying Detection, p. 6.

[47] **Zubiaga, D. S. R. M. V. F. A.** , 2015. Real-time classification of Twitter trends, p. 11.

[48] **Özgür, H. E. Atilla,** 2018. Saldırı tespit sistemlerinde genetik algoritma kullanarak nitelik seçimi ve çoklu sınıflandırıcı füzyonu, *Mühendislik Mimarlık Fakültesi Dergisi,* cilt 33, no. 1, s. 78.

[49] **Forman, G.** , 2003. An Extensive Empirical Study, *Journal of Machine Learning Research 3*, volume 1289, no. 1305, p. 3.

[50] **Ladha, T. D. L.** , 2011. Feature Selection Methods And Algorithms, *International Journal on Computer Science and Engineering*, volume 3, no. 5, p. 1788.

[51] **Yang, J. P. Y.** , 1997. A Comparative Study on Feature Selection in Text Categorization, *ICML '97 Proceedings of the Fourteenth International Conference on Machine Learning*, 1.

[52] **Budak, S. E. T. H.** , 2016. A Modified t-Score For Feature Selection, *Anadolu Üniversitesi Bilim ve Teknoloji Dergisi,* cilt 17, no. 5, s. 847.

[53] Bhardwaj, A. , 2017. Makine Öğreniminde Bilgi Kazancı Nedir?, 5 Kasım. [Çevrimiçi]. Available: https://www.quora.com/What-is-Information-gain-in-Machine-Learning.

[54] Feature Selection, 9 November 2017. [Çevrimiçi]. Available: https://pythonhosted.org/ibmdbpy/feature_selection.html.

[55] **Han, M. K. J.** , 2001. Data Mining Concepts and Techniques, Morgan Kaufmann.

[56] **Frank , M. A. H. I. H. W. Eibe**, 2016. The Weka Workbench.

[57] **McQueen, D. L. N. R. D. R. G. a. C. G. N.-M. Robert J.** , The WEKA machine learning workbench:Its application to a real world agricultural database.

[58] **Şeker, Ş. E.** , 2009. WEKA.

[59] **Dimitoglou, G.** , 2012. Comparison of the C4.5 and a Naive Bayes Classifier for the Prediction of Lung Cancer Survivability.

[60] **Youn , D. M. Seongwook**, 2007. A Comparative Study for Email Classification.

[61] **Brownlee, J.** , 2016. Naive Bayes for Machine Learning.

[62] **Kaur, A. C. Gaganjot**, 2014. Improved J48 Classification Algorithm for the, p. 13.

[63] **Chang, C.-J. L. Chih-Chung**, 2013. LIBSVM: A Library for Support Vector Machines, p. 1.

[64] **Jaiswal, M.** , 2017. What are the similarities and differences between multilayer perceptron (MLP) and radial basis function (RBF) networks?, 9 November. [Çevrimiçi]. Available: https://www.quora.com/What-are-the-similarities-and-differences-between-multilayer-perceptron-MLP-and-radial-basis-function-RBF-networks.

[65] **Rajamohana , D. K. U. K. R. Mrs. S. P.** , 2015. Sentiment Classification based on LDA using SMO Classifier, pp. 1053-1054.

[66] **Girosi, E. O. a. R. F. a. F.,** 1997. Improved training algorithm for support vector machines, *IEEE NNSP*.

[67] **Bonanseai L.** , 2009. 3D Hand gesture recognition using a ZCam and an SVM-SMO classifier, p. 23.

[68] **B. K. R. Ajay Kumar Mishra**, 2016. Study of Random Tree and Random Forest Data Mining Algorithms for Microarray Data Analysis, p. 5.

[69] **Englert, P.** , Locally Weighted Learning.

[70] **Rifkin, R.** , 2008. Multiclass Classification.

[71] **E. F. &. M. A. H. Ian H. Witten**, 2011. Data Mining Practical Machine Learning Tools and Techniques, Third Edition.

[72] **Freund Y. and Scharpie R.** , 1999. Large Margin Classification Using the Perceptron Algorithm, December, Volume 37, Issue 3, pp 277–296

[73] **Witten, F. E. M. H. I.H**, 2011. Data mining: practical machine learning tools and techniques., *Morgan Kaufmann,* p. 128.

[74] **R. D. Ignas Martišius**, 2013. Real-time training of Voted Perceptron for classification of EEG Data, *ResearchGate,* pp. 43-44.