Dicle University Journal of Engineering (DUJE)
web: http://dergipark.gov.tr/dumf

Research Article

Siber Zorbalık Tespit Yöntemleri Potansiyel Uygulama Alanları ve Zorluklar

Enver YAZĞILI [1*], Muhammet BAYKARA [2]

[1] Munzur Üniversitesi, Tunceli MYO, Bilgisayar Teknolojileri Bölümü, Tunceli
enveryazgili@munzur.edu.tr, 0000-0001-8459-3488
[2] Fırat Üniversitesi, Yazılım Mühendisliği Bölümü, Elazığ
mbaykara@firat.edu.tr, 0000-0001-5223-1343

ARTICLE INFO

Makale geçmişi:

Geliş: 26 Şubat 2020
Düzeltme: 29 Haziran 2020
Kabul: 30 Ağustos 2020

Anahtar Kelimeler:

Bilgi güvenliği, siber zorbalık, siber suç, siber güvenlik

ÖZET

Dünya genelinde sosyal medya kullanıcılarının karşılaştığı sorunların başında gelen siber zorbalık gün geçtikçe daha da artmaktadır. İnsanlar arasında yaygınlaşan İnternet kullanımı, siber zorbalığın uygulama alanlarının da artmasına neden olmuştur. Siber zorbalar, İnternet üzerinden yapacakları zorbalıkların tespit edilememesi veya tespit edilse dahi yasal bir yaptırım uygulanmayacağı düşüncesiyle geleneksel zorbalığa oranla daha fazla zorbalık yapmaktadırlar. Artan siber zorbalık suçları, kurbanlarına psikolojik baskılar yaşatarak toplumdan dışlanmaları ve hatta intiharın eşiğine gelmelerine neden olmaktadır. Bu ve buna benzer sorunların önüne geçilmesi için siber zorbalığın anlık tespit edilmesi gerekir ancak bu oldukça güçtür. Bu problemin tespit edilmesi için literatürde çeşitli çalışmalar gerçekleştirilmiştir. Bu çalışmada öncelikle siber zorbalık ve türleri, tespit için kullanılan makine öğrenmesi yöntemleri ve algoritmaları ile literatürde yapılan çalışmalar sunulmuştur.

ARTICLE INFO

Article history:

Received: 26 February 2020
Revised: 29 June 2020
Accepted: 30 August 2020

Keywords:

Information security, cyberbullying, cyber crime, cyber security

Abstract

Cyberbullying, which is one of the problems faced by social media users worldwide, is increasing day by day. It puts psychological pressure on its victims, causing them to be excluded from the society and even to the brink of suicide. In order to prevent these and similar problems, cyberbullying must be detected. Although cyberbullying detection is very difficult, many methods have been developed for its detection. The widespread use of the internet among people caused cyber bullying the application areas to increase . Cyber bullies; They bully more than traditional bullying with the thought that their bullying on the internet cannot be detected or even with the thought that there will be no legal sanction. Various studies have been carried out in the literature to identify this problem. In this study first of all cyberbullying definition, types, legal regulations in the international arena and in turkey, used in detection methods machine learning methods and algorithms, studies in the literature and generally presented implementation steps used in the detection method.

Doi: 10.24012/dumf.859651

* Enver YAZĞILI
✉ e-mail
enveryazgili@munzur.edu.tr

Please cite this article in press as E. Yazğılı, M. Baykara, "Siber Zorbalık Tespit Yöntemleri Potansiyel Uygulama Alanları ve Zorluklar", DUJE, vol. 12, no.1, pp. 23-35, January 2021.

Giriş

Bilgi teknolojilerindeki gelişme ve iletişim araçlarının kullanıcı yaşamlarına çok hızlı yerleşmesi, sosyal medya platformlarının, paylaşım sitelerinin ve ağların gelişimine ve çeşitliliğine zemin hazırlamıştır. Dünya genelinde yapılan araştırmalarda 2018'de nüfusun %42'sinin sosyal medya araçlarını/platformlarını kullandığı, 2019'da ise bu sayının %3'lük dramatik bir artış göstererek %45'e ulaştığı belirtilmiştir [1].

Sosyal medya uygulamaları (Facebook, YouTube, WhatsApp, FB Messenger, Instagram, Twitter gibi), çok yönlü hizmetler sunması (iletişim, eğlence, ticaret, iş, eğitim gibi), bunun yanında kullanıcılar tarafından çeşitli kişisel verilerini paylaşabilecekleri zeminler oluşturması yönüyle kullanıcılarına sayısız avantajlar sunmaktadır. Ancak kişisel bilgilerin izinsiz başka kişilerin eline geçmesi ve bu kişilerin farklı amaçlarla bu bilgileri kullanımları veya paylaşımları sonucunda çeşitli sorunlar ortaya çıkmıştır [2-5].

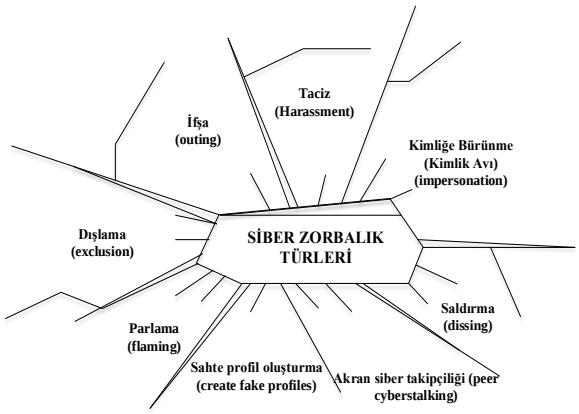
Bu çalışmada literatürde siber zorbalık tespitinde yapılan çalışmalar sunulmaktadır. Daha sonra siber zorbalık ve türleri, siber zorbalık tespitinde kullanılan makine öğrenmesi yöntemleri sunulmuştur. Son kısımda ise sonuç başlığı ile öneriler ve gelecek çalışmalarla ilgili fikirler sunulmuştur.

Siber Zorbalık

Sosyal medya kullanıcıları yaşamlarının en az bir anında siber zorbalık yapmış, siber zorbalığa maruz kalmış veya izleyicisi olmuştur. Kullanıcı davranışlarının, internet ortamında değişkenlikler göstermesine bağlı olarak siber zorbalıklar farklı şekillerde uygulanmakta ve tanımlanmaktadır. Amerika Birleşik Devletleri (ABD) Ulusal Suç Önleme Konseyi zorbalığı, *"İnterneti, cep telefonlarını veya diğer cihazları başka bir kişiye zarar vermek, utandırmak amacıyla metin, resim göndermek için kullanma süreci"* şeklinde tanımlamıştır. Ülkemizde ise Bilgi Teknolojileri ve İletişim Kurumu, *"Siber zorbalık, elektronik ortamda bir birey veya grubun, diğerlerine yönelik kasıtlı biçimde gerçekleştirdiği aşağılama, iftira, dedikodu, taciz, tehdit, utandırma ve dışlama gibi rahatsızlık verici eylemleri ifade eder"* şeklinde siber zorbalığı tanımlamıştır [6].

Siber Zorbalık Türleri

Siber zorbalığın uygulama alanının geniş olması ve uygulama şeklinin de kişilere bağlı olması nedeniyle literatürde birçok farklı siber zorbalık türü yer almaktadır. Ancak en çok kabul gören ve karşılaşılan türleri Şekil 1'de gösterilmiştir [5], [7-9].



Şekil 1. Sosyal ağlarda karşılaşılan siber zorbalık türleri

Taciz

Taciz (Harassment), hedef kişiye uygun olmayan, hakaret içerikli farklı formlardaki mesaj türlerinin kasıtlı bir şekilde gönderilmesi durumudur [10-12].

İfşa

İfşa (Outing), hedef kişiye ait özel bilgilerin, sırların, uygunsuz veya utanç verici bilgilerin ya da görsellerin telefon, e-posta, sosyal medya platformları üzerinden herkese açık şekilde yayınlanması, başkalarına gönderilmesidir [10-12].

Dışlama

Hedef kişinin online gruplardan veya form sitelerinden kasıtlı bir şekilde çıkarılması veya kısıtlanması durumudur [11], [12].

Kimliğe Bürünme

Kimliğe bürünme veya kimlik avı (Impersonation), hedef kişi veya kişileri aşağılamak, kötü göstermek veya arkadaşlık ilişkilerine zarar vermek amacıyla hedefin kimliğine veya başka birinin kimliğine bürünerek paylaşımlarda bulunma veya mesajlar gönderilmesi eylemidir [6], [11], [12].

Saldırma

Saldırma (Dissing), hedef kişi hakkında doğru olmayan, yıpratıcı ve acımasız sözlerin veya bilgilerin üçüncü şahıslara gönderilmesi, dedikodu ve söylenti çıkarılması durumudur [10-12].

Parlama

Parlama (Flaming) diğer adıyla kışkırtma, sosyal medya kullanıcıları arasında aşağılayıcı ve düşmanca etki oluşturma durumudur [10-12].

Sahte profil oluşturma

Sahte profil oluşturma (Create fake profiles), sahte bir web sitesi, blog veya online grup oluşturularak bu platformlar üzerinden hedef kişileri aşağılamak, utandırmak ve güvenliklerine saldırmak amacıyla yalan ve kötü niyetli haberler, bilgilerin yayılması durumudur [11], [12].

Akran siber takipçiliği

Siber zorbalık türlerinden taciz ile benzerlik gösteren bu tür (Peer Cyberstalking), tacizin daha şiddetli formudur. Bu zorbalık türü, hedef kişinin iletişim teknolojileri kullanılarak takip edilmesiyle başlar ve hedef kişinin sadece taciz edilmesiyle kalmaz, kurban tehdit edilir, korkutulur ve her an zarar verilecekmiş gibi siber saldırılarda bulunulur [11], [12].

Siber zorbalık farklı türlerde karşımıza çıksa da genel olarak her yaş gurubu için ciddi tehditler oluşturmaktadır. Kurbanlar hakaret içerikli, rahatsız ve taciz edici yorumlardan hayati tehlikelere yol açacak içerikteki mesajlara her geçen gün daha fazla maruz kalmaktadır. Bu içeriklerin çok hızlı bir şekilde geniş kitlelere yayılabilmesi, sosyal ağların kurbanlar için endişe verici alanlar haline gelmesine neden olmuştur [13].

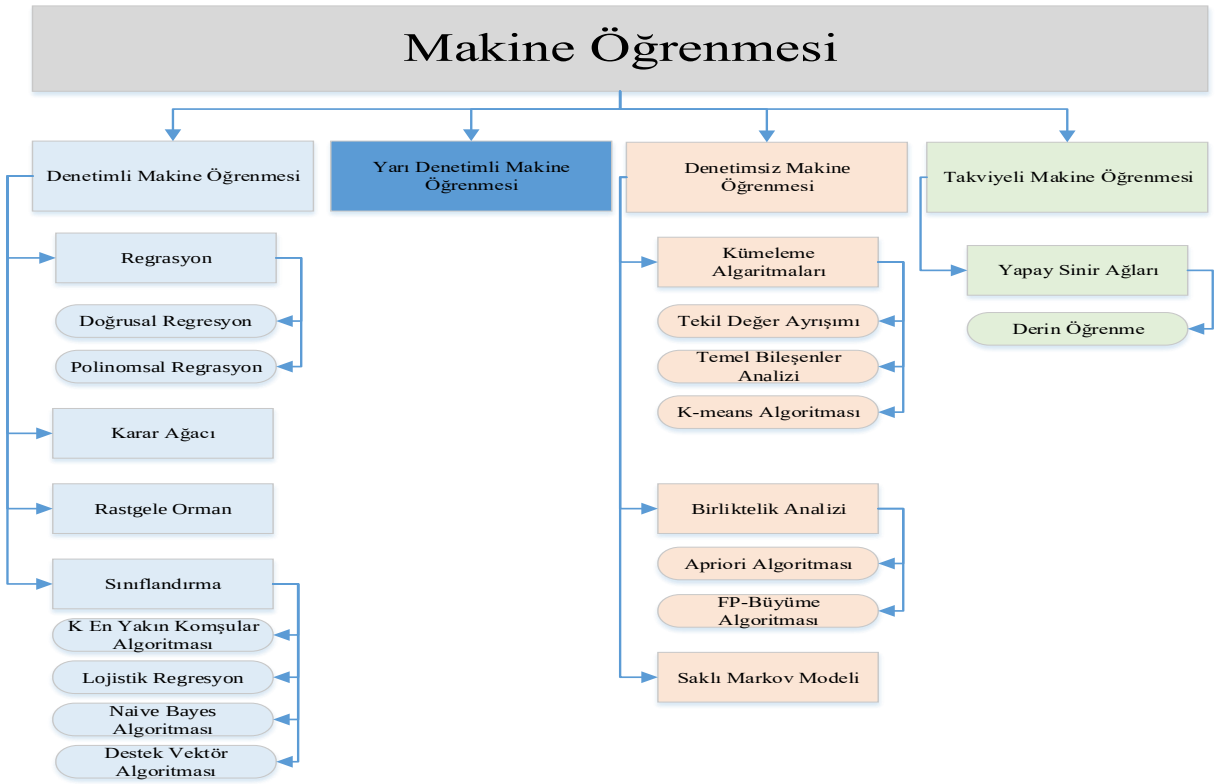
Siber Zorbalık Tespitinde Kullanılan Makine Öğrenmesi Yöntemleri

Siber zorbalık tespitinde büyük veri kullanımının yaygın olması, bu veriler arasında birden fazla özelliğin bulunması ve özellikler arasında da doğru ilişkilerin kurulabilmesi nedeniyle hedef verilerin tespitinde iyi bir tahmin yürütülebilmesi gerekmektedir. Makine öğrenmesi (MÖ) yöntemleri bu yönüyle siber zorbalık tespitinde sıkça başvurulan yöntemlerin başında gelmektedir.

1959 yılında Amerikan bilgisayar bilimcisi Arthur Samuel tarafından makine öğrenmesi, *"bilgisayarın açıkça programlanmadan öğrenme yeteneği"* şeklinde ifade edilmiştir.

Temel olarak makine öğrenmesi, istenen veya kabul edilebilir bir aralıktaki çıkış verilerini tahmin edilebilmek için alınan giriş verilerini analiz eden çeşitli algoritmalar kullanır. Söz konusu algoritmalar, gelen her yeni veri ile daha iyi sonuç elde etmek ve zamanla "zeka geliştirmek" için yeni algoritma adımlarını öğrenir ve bu adımları günceller [14].

Bir başka değişle makine öğrenmesi, problemin çözümüne yönelik o probleme ait giriş verilerini modelleyen algoritmalardır. Modellenen her algoritma en yüksek performansı elde etmek için oluşturulur. Bu yönüyle birçok makine öğrenmesi yöntemi geliştirilmiştir. Makine öğrenmesi türleri ve algoritmaları Şekil 2'de gösterilmiştir [15].



Şekil 2. Makine öğrenmesi türleri ve algoritmaları

Denetimli Makine Öğrenmesi

Denetimli makine öğrenmesinde, makineye örnekler verilerek öğrenme sağlanır. Yani algoritmaya bilinen girdi ve bu girdilere karşılık gelen çıktılar verilerek, algoritmanın girdiler ve çıktılar arasındaki ilişkiyi öğrenmesi daha sonra gelecek olan yeni girdiler için istenilen değerlere en yakın çıktıları elde etmesi hedeflenmektedir [15].

Regresyon

Regresyon analizi, bağımlı ve bağımsız değişkenlerin birbirleriyle olan ilişkilerini inceleyen modelleme tekniği veya tahmin yöntemidir. Bu teknikte veri noktalarına, veri dağılımına bağlı olarak bir eğri veya doğru uygulanmaktadır. Buradaki amaç veri noktaları ile çizilecek eğri/doğru arasındaki farklarının minimum seviyede olmasıdır.

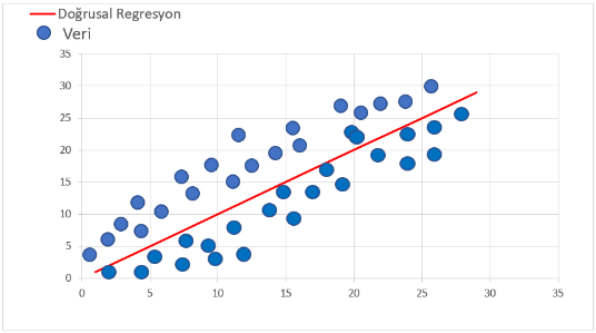
Regresyon analizinde çeşitli teknikler kullanılmaktadır. Bu tekniklerden en sık kullanılanları;

- Lojistik Regresyon
- Doğrusal Regresyon
- Polinomsal Regresyon
- Ridge Regresyon
- Lasso Regresyon
- ElasticNet Regresyon

Siber zorbalık ile ilgili çalışmalarda genel olarak doğrusal ve polinomsal regresyon yöntemlerinin kullanıldığı görülmüştür. Bu sebeple bu kısımda Doğrusal ve Polinomsal regresyon türleri açıklanmıştır [16].

Doğrusal Regresyon

Tahmin edilecek veriler ile değişkenlerin arasında doğrusal bir ilişki olduğunda doğrusal regresyon algoritması kullanılmaktadır.

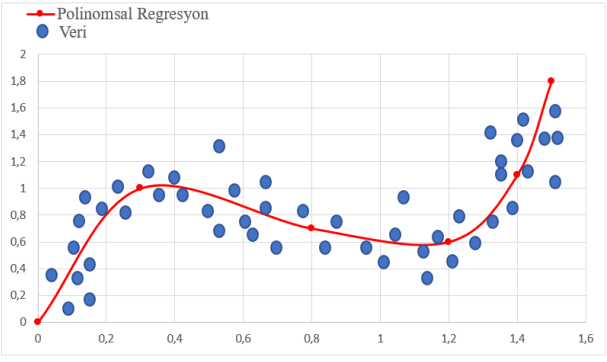


Şekil 3. Doğrusal regresyon veri ilişkileri

Burada önemli olan çizilecek doğrunun bütün değişkenler ve sonuçlar için hata payını en aza indirgeyecek şekilde çizilmesidir. Doğrusal Regresyon algoritması bu durumu başarılı şekilde yapmaktadır. Bu yöntem siber zorbalık tespitinde belirlenen farklı özelliklerin birbirleriyle ilişkilendirmelerinde kullanılmaktadır [17].

Polinomsal Regresyon

Veriler arasında doğrusal bir ilişkinin olmaması durumunda problemin çözümüne yönelik polinomsal bir algoritma kullanılması gerekir. Örnek olarak eldeki veriler Şekil 4'teki gibi polinomsal bir dağılım gösterdiği varsayılsın. Bu durumda eldeki verilerin dağılımına uygun veriler arasına polinomsal bir eğrinin çizilmesi gerekir [18].

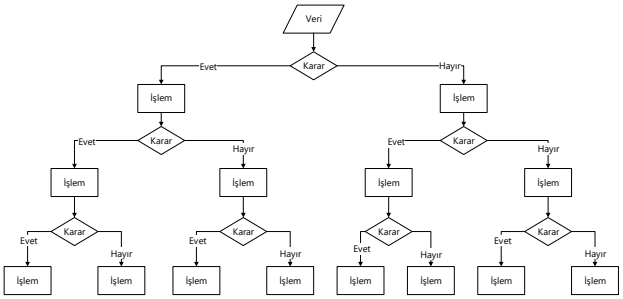


Şekil 4. Polinomsal regresyon veri ilişkileri

Karar Ağacı

Bu algoritma yapısal olarak bir ağaca benzemektedir. Ağacın yaprakları sınıf etiketlerini, yapraklara giden dallar da özellik ile ilgili işlemleri ifade etmektedir. [18].

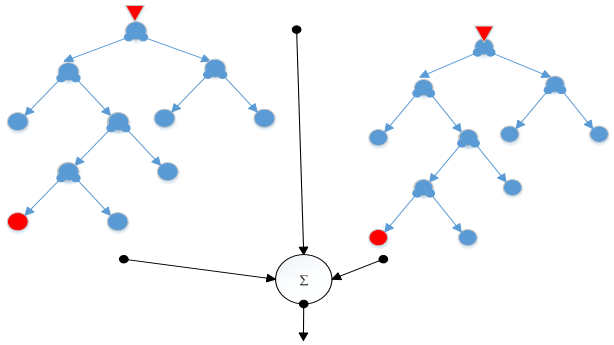
Karar ağaçları tepeden aşağıya inen bir yapıya sahiptirler. Bu yapının oluşturulmasındaki temel amaç, büyük veri kümelerini çeşitli karar kurallarına tabi tutarak daha küçük kümelere bölümlemektir. Karar ağacı modelleri, çok büyük veri kümelerine uygulanabilmesi, bir modelin güvenirliğini birçok istatistiksel testlerle gerçekleştirebilmesi, kullanılacak verilerde çok fazla ön işleme gerek duymaması yönüyle siber zorbalık tespitinde tercih edilmektedir [19]. Şekil 5, bir karar ağacı yapısını göstermektedir.



Şekil 5. Karar ağacı yapısı

Rastgele Orman

Kısaca Rastgele Orman (RO), sınıflandırma yapılırken birçok karar ağacı üreterek sınıflandırma oranını yükselten ve daha doğru tahminler elde etmek için onları birleştiren bir algoritmadır. Rastlantısal olarak seçilen karar ağaçları bir araya gelerek karar ormanını oluşturur. Rastgele Orman algoritması çok fazla sayıda değişken, kayıp veri, etiketlenmiş sınıflara sahip ve dengesiz bir dağılım gösteren veri setlerinde iyi sonuçlar vermesi yönüyle siber zorbalık tespitinde kullanılmaktadır. RO'ın en büyük avantajı, sınıflandırma ve regresyon problemlerinde kullanılabilmesidir. Basit bir Rastgele Orman yapısı Şekil 6'de gösterilmiştir. [20].



Şekil 6. Rastgele orman yapısı

Sınıflandırma

Sınıflandırma, makine öğrenme algoritması ile gözlemlenen verilerden bir sonuç çıkararak bu verilerin kategorilere ayrılması ve daha sonra gelecek olan yeni verilerin hangi kategoriye ait olduğunun tespit edilmesi işlemidir. Kısaca kullanılan veriler etiketlenebilir, kategorilere ayrılabilir veya belli gruplara ayrılabilir ise bu teknik kullanılabilir. Sosyal medya platformlarında elde edilen cümlelerin gözlemlenerek "siber zorbalık içeren" veya "siber zorbalık içermeyen" cümleler olarak iki sınıfa ayrılması ve daha sonra anlık cümlelerin gözlemlenmesi ve bu iki sınıftan hangisine ait olduğunun tespit edilmesi sınıflandırmaya örnek olarak verilebilir [15].

K En Yakın Komşular Algoritması

Bu algoritma (K-Nearest Neighbors-KNN) sınıflandırılmak istenen yeni verinin daha önceki verilerden k tanesine olan yakınlığına bakan bir algoritmadır. Sınıflandırma esnasında test örnekleri ve eğitim örnekleri birbirleri ile karşılaştırılır. Bu karşılaştırmalarda komşuluk mesafesi için genel olarak öklid bağıntısı kullanılmaktadır. Tahminler, komşu örneklerin oy çoğunluğuna dayanmaktadır. Yüksek k değerlerine aşırı uyma eğiliminde olmasından dolayı dikkat edilmesi gerekmektedir. Bu yöntemin siber zorbalık tespitinde kullanılmasının temel nedeni, eğitim aşaması kısmının olmaması ve gürültü verilerine karşı dayanıklılık gösterebilmesidir [18].

Lojistik Regresyon

Lojistik Regresyon, eldeki verilere dayanarak meydana gelecek bir olayın olasılığının tahmin edilmesidir. Burada bağımlılığı birden fazla olan bir değişkenin sonuçları 0 ve 1'e indirgenerek gösterilmektedir. Genel olarak siber zorbalık kategorilerinin ayırımı veya ilişkilendirilmesi durumlarında kullanılmaktadır [17].

Naive Bayes Sınıflandırma Algoritması

Diğer algoritmalarla karşılaştırmak için temel seviye sınıflandırıcı olarak önerilen iyi bilinen bir istatistiksel öğrenme algoritmasıdır. Naive Bayes (NB), belirli bir sınıf için girdilerin birbirinden bağımsız olduğunu varsayarak sınıf koşulu olasılıklarını tarafsız tahmin eder. NB, sınıfları koşullu marjinal yoğunlukları bulmak için ayırıcı sınıflar problemini azaltır, bu da belirli bir örneğin olası hedef sınıflardan biri olma olasılığını temsil eder. NB, birbirleri ile ilişkili girdiler içermedikçe diğer algoritmalara karşı iyi performans göstermektedir. Bu algoritma diğer sınıflandırma algoritmalarına göre daha sade olması ve daha iyi sonuçlar elde etmesi yönüyle siber zorbalık tespitlerinde sıkça kullanılmaktadır [18].

Destek Vektör Makinesi

Destek Vektör Makineleri (Support Vector Machine: SVM) teorisi, iki sınıfa ait verilerin en uygun şekilde birbirlerinden doğrusal/doğrusal olmayan şekilde ayrılabilen sonsuz sayıda çizginin olduğunu varsayar. Bu algoritma, büyük veri kümelerinde çok hızlı sonuçlar elde etmesi, verilerin ayrımını doğrusal veya doğrusal olmayan şekilde yapabilmesi ve sonsuz sayıdaki bu ayrımların içerisinden en iyisini seçme yeteneğine sahip olması nedeniyle siber zorbalık tespitinde en çok kullanılan algoritmaların başında gelir [18].

Yarı Denetimli Makine Öğrenmesi

Bu yapıda etiketli ve etiketsiz veriler birlikte kullanılmaktadır. Verilerdeki etiketler anlamlı bilgiler içerdiğinden algoritma, etiketli veriler ile etiketsiz veriler arasındaki farklılığı anlamlandırarak veri çözümlemesi gerçekleştirmektedir. Bu sayede algoritma,

etiketsiz verilere etiket eklemeyi öğrenebilmektedir. Kısaca etiketlenmiş veri sayısının az olduğu ve tahmin edilecek veri sayısının çok olduğu durumlarda bu yöntem kullanılmaktadır [15].

Denetimsiz Makine Öğrenmesi

Denetimli Makine Öğrenmesinden farklı olarak bilinen girdi ve buna karşılık gelen çıktılar yoktur. Algoritma sadece girdi verilerini analiz ederek veriler aralarında bir ilişki bulmaya çalışır. Daha sonra tespit edilen ilişkiler aracılığıyla girdiler yakınlık durumuna göre gruplara ayrılır. Bu sayede gelen yeni girdiler yakınlık durumuna göre belirlenen guruba alınır. Siber zorbalık tespitinde veri ön işleme, özellik sayısını düşürme, veri kümesini birden çok bileşene ayırma gibi özelliklerinden dolayı Denetimsiz Makine Öğrenmesi tercih edilmektedir [15].

Kümeleme Algoritmaları

Kümeleme algoritmaları, belirlenmiş özellikler dikkate alınarak benzer özellikteki verilerin aynı gruba alınması işlemini gerçekleştirir. Burada özelliklerin tespit edilmesi ve grup ayrımının yapılabilmesi için her bir veri kümesinin analizinin yapılması gerekir. Siber zorbalık tespitinde verilerin zorbalık unsuru taşıma durumlarına bağlı olarak uygun kümelere ayrılmasında kümeleme algoritmaları kullanılmaktadır [15].

Tekil Değer Ayrışımı

Tekil Değer Ayrışımı (TDA), bir matrisin çarpanlarına ayrılma türlerinden biridir. Matris çözümlemelerinde terim sayısının teorik olarak bilinmediği durumlarda kullanılır. Verilen bir matristeki problemleri belirleyip nümerik cevaplar bulmaya yarar. Burada öncelikle matris 3 parçaya ayrılır daha sonra bu parçalar kullanılarak aynı matrisin elde edilmesi sağlanır. Google arama motorunun kullandığı PageRank algoritması, yüz tanıma modellemeleri, bilgi getirimi/çıkarımı, boyut azaltma, gen analizleri, veri sıkıştırma gibi birçok alanda temel adım olarak kullanılmaktadır [20].

Temel Bileşenler Analizi

Bu analiz yöntemi bir boyut azaltma işlemidir. Birbirleri ile ilişkili çok sayıdaki değişken içerisinde fazla olanların çıkarılarak veri kümelerinin küçültülmesine ihtiyaç duyulması durumunda kullanılmaktadır. Buradaki hedef büyük veri kümesinin basitleştirilmesiyle elde edilecek sadeleştirilmiş veri kümesinde daha doğru gözlem yapabilmeyi ve veriler arasındaki ilişkiyi daha iyi çözümleyebilmeyi sağlamaktır. Bu metot yüz tanıma, görüntü sıkıştırma, örüntü tanıma gibi birçok alanda yaygın olarak kullanıldığı gibi siber zorbalık tespitinde de veri kümelerini azalmak için kullanılmaktadır [21].

K-Means Algoritması

Veri madenciliğinde en çok kullanılan algoritmalardan biri olan K-Means algoritması kümeleme algoritmalarının da en eskilerinden biridir. Bu algoritma istatistiksel olarak benzer özellikteki verileri aynı kümeye yerleştirir ve bu algoritmada bir veri sadece bir kümeye ait olabilir. Algoritmanın temel amacı, oluşturulan "K" adet kümenin her birinin mümkün olduğunca birbirinden farklı olmasını ve her kümede bulunan verilerin de birbirine en yakın olmasını sağlamaktır [22], [23].

Birliktelik Analizi

Veri madenciliğinde kullanılan ilk tekniklerden biri olan bu analiz yöntemi, farklı olayların birlikte gerçekleşme olasılıklarının çözümlenmesi işlemidir. Temel mantık, belirli bir veri kümesindeki geçmiş verilerin analiz edilmesi ve bu veriler içerisinde sık sık birlikte ortaya çıkan özellik-değer koşullarını gösteren ilişkilendirme kurallarının tespit edilmesidir. Siber zorbalık tespitinde, bir arada kullanılan kelime çiftlerinin belirlenmesinde ve yorumlanmasında bu analiz yöntemi kullanılmaktadır [24], [25].

Apriori Algoritması

Apriori algoritması temelde tekrarlayan bir özelliğe sahiptir. Hareket bilgilerini içeren veri tabanında sık rastlanan öge kümelerini tespit etmekte kullanılmaktadır. Bu algoritmaya göre k adet elemana sahip bir küme minimum destek

değerlerini sağlıyor ise, bu kümeye ait alt kümelerin her biri de minimum destek değerlerini sağlar. Birliktelik analizinin ilk adımında kullanılan Apriori algoritması, sık geçen öğeler madenciliğinde kullanılan en yaygın ve eski algoritmadır [24], [25].

FP-Büyüme Algoritması

FP-Büyüme Algoritması, verileri FP-Tree (Frequent Pattern Tree) denilen ve sıkıştırılmış bir ağaç yapısına sahip veri tabanında tutmaktadır. Bu veri tabanı oluşturulurken iki tarama gerçekleşir. Bu taramaların ilkinde yapıdaki nesnelerin tümünün destek değerleri hesaplanır. Daha sonraki tarama işleminde ise ağacın veri yapısı oluşturulur. Bu algoritmanın en önemli özellikleri, aday kümeler üretilmeden yaygın kümeleri test edebilmesi, yüksek boyutlu veri kümeleri üzerinde hızlı çalışabilmesi ve sisteme ait kaynakları verimli bir şekilde kullanabilmesidir. Algoritma, "böl ve yönet" yaklaşımına göre büyük veri kümelerini daha küçük kümelere ayırmaktadır. Bu yönüyle FP-Tree yapısı asıl veri kümesinden küçük olmalıdır. Siber zorbalık tespitinde FP-Growth algoritması kullanılarak benzer kelimelerin frekans değerleri hesaplanır ve bir desen oluşturulur. Oluşturulan bu desende kelimelerin birliktelik ilişkileri belirlenir [24], [26].

Saklı Markov Modeli

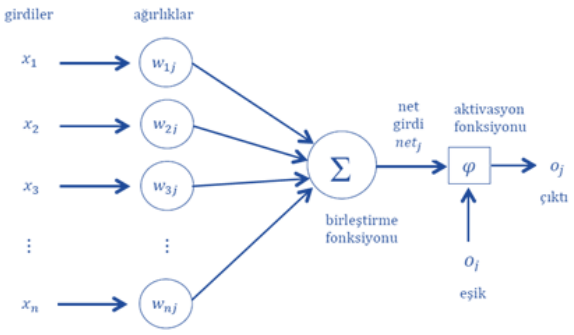
Saklı Markov Modelinde, durumlar dışarıdan doğrudan gözlemlenemez, yalnızca her durum için o duruma ait gözlem çıktıları izlenebilir. Her bir durum için ele alınan gözlem çıktıları toplanarak bir gözlem dizisi elde edilmektedir. Saklı Markov Modelinde sistemde oluşan gözlemlerin tümü zamandan bağımsızdır ve mevcut durumların olayların her birine ilişkin olasılıkları, dağılım değerine bağlı olarak ortaya çıkmaktadır. Saklı Markov Modelinde, sistemin herhangi bir anında hangi durumda olduğu bilinmemektedir, ancak söz konusu durumun etkilediği gözlemler tespit edilebilmektedir [27].

Takviyeli Makine Öğrenmesi

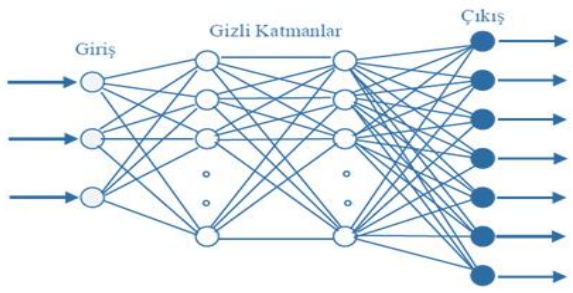
Takviyeli (pekiştirmeli) öğrenme, en yüksek ödüle erişmek için hangi seçimlerin yapılması gerektiğini geçmiş deneyimlere dayanarak tespit eden (öğrenen) bir yaklaşımdır. Bu algoritmanın klasik yöntemlerden farkı, ön bilgiye ihtiyaç duymamaları yani doğru girdi/çıktı eşleşmelerinin verilmediği ve kesin yöntemlerin verimsiz kaldığı durumlar için kullanılmalarıdır [14], [15].

Yapay Sinir Ağları

Yapay sinir ağları insan sinir sistemini örnekleyen matematiksel bir modeldir. Bu modelde amaç insan sinir hücrelerinin veriyi depolama, kullanma ve işleme gibi özelliklerini taklit edecek, onun gibi karar verme ve muhakeme yeteneğine sahip olabilecek, birbirleri ile bağlantılı yapay sinir hücrelerinden (nöronlardan) meydana gelen bir yapı oluşturmaktır. Bu hücrelerin her birinin temel elemanları Şekil 7'de gösterilmiştir. Bu yapay sinir hücrelerinin katmanlar halinde birleşmesi ile yapay sinir ağı oluşur. Bu katmanlar ise girdi, çıktı ve her ikisi arasında bulunan gizli katmanlardan oluşmaktadır (Şekil 8). Girdi/Çıktı katmanlarındaki nöron sayıları, bağımlı/bağımsız değişken sayılarına bağlı olarak belirlenirken, gizli katmanda bulunacak katman sayıları ve nöron sayıları, kullanıcı tarafından en iyi sonucu elde edecek şekilde belirlenmektedir.



Şekil 7. Yapay sinir ağlarındaki hücre yapısı

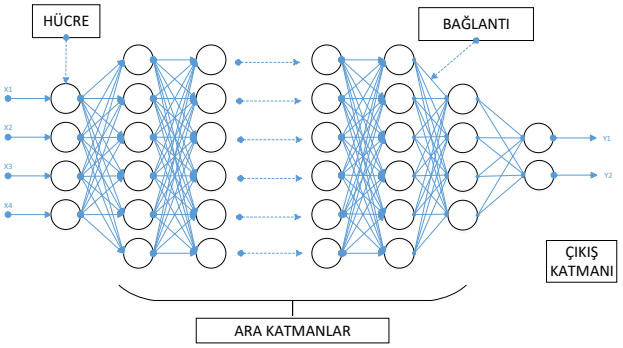


Şekil 8. Çok katmanlı yapay sinir ağının genel yapısı

Yapay sinir ağları, eldeki veri setinin yapısını öğrenerek, sonuca ulaşmak için genellemeler yaparlar. Genelleştirmeler, yapay sinir ağının ilgili olay örneklerle eğitilmesiyle ile gerçekleştirilir. Bu sayede benzer olaylara karşı gelebilecek çıkış verileri tespit edilir. Ağ üretmiş olduğu sonucu, ağa girdi olarak gelen bilgilerin kendi ağırlık değerleri ile çarpılıp toplanması sonucu oluşan yeni bilginin bir fonksiyon aracılığıyla işlenmesi ve bu işlenen bilginin de çıkış katmanından alınmasıyla elde etmektedir. Yapay sinir ağının her istenilen en iyi sonucu elde edebilmesi için bu ağırlıkları sürekli güncellemesi gerekir. Ancak bu ağırlık değerleri kullanıcı tarafından anlamlandırmaya ve yorumlamaya kapalı olduğu için yapay sinir ağları için bir dezavantaj olarak görülmektedir. Ağın en iyi sonucu nasıl elde ettiği tespit edilemediğinden, ağ kara kutu gibidir. Yapay sinir ağı içindeki bilgi, istenilen hedefe en yakın sonuç, kullanıcının belirlemiş olduğu katman ve nöronlarda gizlidir. Yapay sinir ağları deneyimleme ve örnekleme yaparak öğrenmeyi gerçekleştirir. Bu sayede girdiler arasındaki ilişkilerin tespitinin zor olduğu veya büyük veri kümelerinde doğrusal olmayan ilişkilerin modellenmesinde kullanılmaktadır. Yapay sinir ağları; görünün tanımlanması, doğal dil işleme, ses tanıma, büyük veri analizlerinde ve buna benzer birçok alanda kullanılmaktadır. Bu yönüyle siber zorbalık tespitinde de etkin olarak kullanılmaktadır [15].

Derin Öğrenme

Makine öğrenmesi sınıflarından biri olan derin öğrenme, verilere ait özelliklerin çıkarılması ve bu özelliklerin dönüştürülmesi amacıyla doğrusal olmayan birçok işlem katmanı kullanmaktadır. Birbirini takip eden her bir katmanın çıkış verisi bir sonraki katmana giriş verisi olarak aktarılır [28]. Derin öğrenme algoritmaları denetimli veya denetimsiz olabilir. Derin öğrenme ile verilere ait birçok özelliğin veya verileri temsil eden bilgilerin öğrenilmesi amaçlanmaktadır. Derin öğrenmede alt düzeydeki özelliklerin türetilmesiyle üst düzey özellikleri elde etmeye yönelik bir hiyerarşik temsili yapı oluşturulur [29]. Derin öğrenmede eldeki verileri en iyi şekilde temsil edecek özellikler manuel yerine, algoritmalar kullanılarak gerçekleştirilir. Derin öğrenmenin genel yapısı Şekil 9'da gösterilmiştir [30].



Şekil 9. Derin öğrenme genel yapısı

Örnek Uygulamalar

Altay ve Alataş Siber zorbalık tespitine yönelik doğal dil işleme teknikleri ile makine öğrenmesi yöntemlerinden Bayesyen lojistik regresyon, rassal orman algoritması, çok katmanlı algılayıcı, J48 algoritması ve destek vektör makineleri kullanılmıştır.Veri seti olarak hazır formspring verileri kullanılmış yapılan farklı sınıflandırma deneylerinde BLR ve RO algoritmalarının en iyi performansı verdiği tespit edilmiştir [5].

Siber zorbalık konularında sosyal medya kullanıcılarını bilinçlendirmek veya kullanıcıların mevcut bilgilerini tespit etmek için çeşitli anket çalışmaları yapılmıştır [7-9], [31].

Hussain ve diğ. Facebook'tan, Prothom-Alo haberlerinden ve YouTube'dan veriler toplayarak veri seti oluşturmuşlardır. Bu veri setinde ön işleme işlemlerini gerçekleştirmek için bir algoritma tasarlamışlar ve %75,5 başarı elde etmişlerdir. Daha sonra sınıflandırma için RO,

SVM ve Multinomial Naive Bayes (MNB) algoritmalarını kullanmış ve bu algoritmalardan SVM algoritmasının en iyi performansı verdiğini tespit etmişlerdir [32].

Al-Mamun ve Akhter, sosyal medya ortamlarından veri çekebilecek bir program geliştirmişlerdir. Java dilinde geliştirdikleri program aracılığıyla Facebook ve Twitter üzerinden Bengalce veriler çekilmiştir. Bu veriler NB, J48, SVM ve k-NN MÖ sınıflandırma algoritmalarına tabi tutulmuş ve SVM algoritmasının en iyi sonucu verdiği görülmüştür [33].

El-Halces, Arapça ve İngilizce yazılan spam e-postaların filtrelenmesine yönelik Twitter ve Facebook yorumları toplayarak elde ettikleri veri setlerine SVM, NB, k-NN ve YSA algoritmalarını uygulamıştır. Bu karşılaştırma sonuçları ile SVM algoritmasının saf İngilizce, NB algoritmasının saf Arapça veri setlerinde en iyi sonucu elde ettiğini tespit etmişlerdir [34].

Duygu analizi tespiti için yapılan bir çalışmada Arapça yazılmış olan Facebook yorumları SVM, NB ve Karar ağaçları algoritmaları kullanılarak sınıflandırmaya tabi tutulmuş, %73,4 doğruluk oranıyla SVM'nin en iyi sonucu verdiği tespit edilmiştir [35]. Duygu analizine yönelik bir başka çalışmada ise Twitter'dan alınan Arapça Tweetler üzerinde yazım ve lehçeler de dikkate alınarak NB, SVM ve k-NN algoritmalarına tabi tutularak karşılaştırma yapılmış ve NB algoritmasının en iyi sonucu verdiği tespit edilmiştir [36].

Sintaha ve Mostakim [37], Shekhar ve Venkatesan [38] Twitter'dan elde ettikleri veri setlerine farklı sınıflandırma algoritmaları uygulayarak bu algoritmaları karşılaştırmışlardır. İki çalışma sonucunda SVM algoritmasının en iyi sonucu verdiği tespit edilmiştir.

Zois ve diğ. AvOID algoritması tasarlayarak veri setindeki kelimeleri siber zorba/siber zorba olmayan gruba ayırmışlardır. Yapılan beş kat çapraz doğrulama ve deneyler sonucunda tasarladıkları algoritmanın çıkarılacak özellik sayısını %64 oranında azalttığını tespit etmişlerdir [39].

Venckauskas ve diğ. Litvanca haber portalı olan DELHİ'den topladıkları yorumlardan veri seti oluşturmuşlardır. Bu veri setine SVM algoritması uygulanmış, değerlendirme için ise Kazanan Her Şeye Sahip (WTA) metriği kullanarak adli tıp uzmanlarınca analizi yapılan şüpheli yazar listelerinin kısaltılmasını amaçlayan bir çalışma yapmışlardır [40].

Bu çalışmalar dışında sosyal medya platformlarının da siber zorbalık tespitine yönelik çalışmaları bulunmakta ve çözüme yönelik araştırmalarını devam ettirdikleri bilinmektedir [3], [38], [41-43], [44].

İbrahim ve diğ. Siber zorbalık tespitinde kullanılan veri setlerindeki veri dengesizliği probleminin çözümüne yönelik bir çalışma gerçekleştirmişlerdir. Veri seti olarak Wikipedia verileri kullanılmış, çözüm için ise farklı veri büyütme tekniklerinden evrişimli sinir ağı (CNN), çift yönlü uzun kısa süreli bellek (LSTM) ve çift yönlü kapılı tekrarlayan üniteler (GRU) kullanılmıştır. Yapılan sınıflandırma işlemlerinde ise giriş verilerinde siber zorbalığın ve türünün tespit edilmesi işlemleri gerçekleştirilmiştir. Sınıflandırma işlemlerinde %87 başarı ile SVM algoritması en yüksek performansı verdiği tespit edilmiştir [45].

Tablo 1'de çalışmalarda kullanılan sınıflandırma algoritmaları, kullanılan dil, veri seti, veri setinin eğitim-test-doğrulama yönünden ayrıştırılmasına bağlı olarak elde edilen sonuçlara yer verilmiştir.

Tablo 1. Siber zorbalık tespitine yönelik yapılan bazı çalışmalar

Yapılan Çalışmalar	Çalışma Yılı	Kullanılan Sınıflandırma Algoritmaları	Kullanılan Veri Setleri	Veri Dağılımı Eğitim/Test/Doğrulama	Sonuçlar	Çalışılan Dil
[5]	2018	BLR, RO, Çok katmanlı Algılayıcı J48, SVM	Formspring.me	%70 / %30	BLR, RO	İngilizce
[32]	2018	SVM, RO, MNB	Twitter	%83.4 / %16.6	%75.5 SVM	Bengalce
[33]	2018	NB, SVM, J48, k-NN	Facebook / Twitter	%90 / %10	%95,4 SVM	Bengalce
[34]	2009	SVM, NB, k-NN, YSA	Facebook / Twitter		%98,32 SVM %92,42 NB	İngilizce Arapça
[35]	2013	SVM, NB, Karar Ağaçları	Facebook		%73.4 SVM	Arapça
[36]	2014	NB, SVM, k-NN	Twitter	%93 / %7	%76,78 NB	Arapça
[37]	2018	NB, SVM	Twitter	%80 / %20	%82,06 SVM	İngilizce
[38]	2018	NB, SVM	Twitter	%60 / %20 /%20	%89.54 SVM	İngilizce
[39]	2018	AVOID	Twitter	%50 / %50	%64 AvOID	İngilizce
[40]	2017	SVM	http://www.delhi.lt	%80 / %20	%95 SVM	Litvanca
[45]	2018	LSTM, GRU, NB, SVM	Wikipedia	%80 / %10 / %10	%87 SVM	İngilizce

Sonuçlar

Siber zorbalık üzerine yapılan çalışmaların incelenmesi sonucunda literatürde bu alanda birçok çalışma yapıldığı görülmektedir. Bu çalışmalar, kullanılan dil yapısı, veri seti, sınıflandırma algoritmaları veya veriler üzerinde gerçekleştirilen ön işlemler, eğitim test verilerinin dağılımına bağlı olarak farklılıklar göstermektedir. Bu çalışmalarda yukarıda yazılan etkenlere bağlı olarak sınıflandırma algoritmalarının performans değerlerinde değişkenliklerin görülmesiyle birlikte birçok dil yapısında yapılan sınıflandırmalarda SVM algoritmasının en iyi performansı sergilediği tespit edilmiştir [5, 32-34, 38-40, 45]. Arapça dil yapısında ise NB algoritmasının doğruluk oranının yüksek olduğu görülmüştür [34-36].

Her ne kadar bu alandaki çalışma sayısının fazla oluşu sevindirici olsa da siber zorbalık tespitinde yeterli sonuçlara ulaşılmadığı açıktır. Bu çalışmaların etkin sonuçlar verebilmesine yönelik iki öneri sunulmaktadır. Bunlardan birincisi siber zorbalık tespitlerinin anlık olarak gerçekleştirilmesidir. 2020 yılı itibariyle Microsoft firmasının bu yönde her sosyal medya platformuna uygulanabilecek bir çalışma gerçekleştirdiği açıklanmıştır ancak henüz uygulamaya geçilmemiştir. Diğer bir yaklaşım ise siber zorbalık tespiti için kelime analizlerinin yerine cümle bazında analizlerin yapılması yani kullanılan cümlelerin bir bütün olarak algılanarak siber zorbalık içerip içermemesine bakılmasıdır. Buna yönelik gelecekte siber zorbalık tespitinde daha sağlıklı ve verimli sonuçlar elde etmek amacıyla öncelikle kullanılacak veri kümelerinde duygu analizi yapılarak siber zorbalığın anlık tespit yöntemleri belirlenmesine yönelik çalışmalar gerçekleştirilmesi düşünülmektedir.

Kaynaklar

1. Dijilopedi, URL: https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/ (Erişim zamanı; Temmuz, 06, 2019).
2. Bertot, J. C. Jaeger, P. T. Hansen, D. "The İmpact Of Polices On Government Social Media Usage: Issues, Challenges, and Recommendations", Government information quarterly, vol. 29, pp. 30-40, 2012.
3. Patel, P. Kannoorpatti, K. Shanmugam, B. Azam, S. Yeo, K. C. "A Theoretical Review Of Social Media Usage By Cybercriminals", 2017 International Conference on Computer Communication and Informatics (ICCCI -2017), 5-7 January 2017, Coimbatore, India.
4. A. Aslan, B. O. Doğan, "Çevrimiçi Şiddet: Bir Siber Zorbalık Alanı Olarak "Potinss" Örneği", Marmara İletişim Dergisi, Marmara Journal of Communication, Yıl / Year: 2017, Sayı / Issue:

27, ss/pp: 95-119, ISSN: 1300-4050, DOI: 10.17829/midr.20172729524
5. Varol Altay, E. Alataş, B. " Detection of Cyberbullying in Social Networks Using Machine Learning Methods International Congress on Big Data", Deep Learning and Fighting Cyber Terrorism, Ankara, Turkey, 3-4 December 2018.
6. Aksaray, S. "Siber Zorbalık", Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt 20, Sayı 2, 2011, Sayfa 405-432
7. Žufić, J. Žajgar, T. Prkić, S. "Children Online Safety", 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 22-26 May 2017, Opatija, Croatia.
8. Ravichandran, K. Arulchelvan, S. "The Model of Multilayer perceptron Analysed the Crime News Awareness in India", 2017 International Conference on Advanced Computing and Communication Systems (ICACCS-2017), 06-07 January 2017, Coimbatore, India.
9. Weru, T. Sevilla, J. Oluku, J. Mutegi, L. Mberi, T. "Cyber-smart children, cyber-safe teenagers: Enhancing internet safety for children", 2017 IST-Africa Week Conference (IST-Africa), Windhoek, 2017, pp. 1-8.
10. Baştürk Akca, E. Sayımer, İ. "Cyberbullying, It's Tyeps And Related Factors: An Evaluation Through The Existing Studies", AJIT-e: Online Academic Journal of Information Technology 2017-Special Issue/Özel Sayı-Cilt/Vol: 8-Sayı/Num:30, http://www.ajite.org/?menu=pages&p=detailsofarticle&id=285. , Erişim Tarihi:06.01.2020.
11. Küçük, S. "Siber Zorbalik Ölçeği Türkçe Uyarlamasi", İstanbul Üniversitesi,Adli Tip Enstitüsü 2016 , Sosyal Bilimler Anabilim Dali Yüksek Lisans Tezi
12. Öztürk, E. "Cyberbullyıng Detectıon Usıng Text Classıfıcatıon For Turkısh Language", Çukurova Unıversıty Instıtute Of Natural And Applıed Scıences, Department Of Computer Engıneerıng Adana-2019
13. E. Baştürk Akca, İ. Sayımer, "Cyberbullying, It's Tyeps And Related Factors: An Evaluation Through The Existing Studies", AJIT-e: Online Academic Journal of Information Technology 2017-Special Issue/Özel Sayı-Cilt/Vol: 8-Sayı/Num:30,
14. Idlebundle, URL: http://www.idlebundle.com/regression-analysis/ (Erişim zamanı; Aralık, 25, 2019).
15. Atalay, M. Çelik, E. "Büyük Veri Analizinde Yapay Zekâ Ve Makine Öğrenmesi Uygulamaları", Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Cilt.9 Sayı.22 2017 - Aralık (s.155-172)
16. Çürük, E. "Sosyal Ağlardaki Siber Zorbalığın Yapay Zeka Algoritmaları İle Tespiti Ve Sınıflandırılması", Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Mersin Üniversitesi, 2018
17. Yavuz blog, URL: https://yavuz.github.io/dogrusal-coklu-dogrusal-polinomsal-regresyonlar/ (Erişim zamanı: Ocak, 03, 2020).
18. Aydın, C. "Makine Öğrenmesi Algoritmaları Kullanılarak İtfaiye İstasyonu İhtiyacının Sınıflandırılması", Avrupa Bilim ve Teknoloji Dergisi Sayı 14, S.169-175, Aralık 2018
19. Medium, URL: https://medium.com/@k.ulgen90/makine-örenimi-bölüm-5-karar-ağaçları-c90bd7593010 (Erişim zamanı; Aralık, 03, 2019).
20. Devhunter, URL: https://devhunteryz.wordpress.com/2018/09/20/rastgele-ormanrandom-forest-algoritmasi/ (Erişim zamanı; Aralık, 03, 2019).
21. Cömert, Z. "Temel Bileşenler Analizine Genel Bir Bakış", www.zafercomert.com, Erişim Tarihi:07.01.2020.
22. Şengöz, N.Özdemir, G. "Temel Bileşenler Analizi Ve K-Ortalama Kümeleme Yönteminin Birlikte Kullanımı: Bir Örnek Uygulama", Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Cilt.8 Sayı.15 2016 - Aralık (s.85-94)
23. Mustafaakca, URL: http://mustafaakca.com/k-means-kumeleme-algoritmasi/ (Erişim zamanı; Kasım, 15, 2019).
24. Erpolat, S. "Otomobil Yetkili Servislerinde Birliktelik Kurallarının Belirlenmesinde Apriori ve FP-Growth Algoritmalarının Karşılaştırılması", Anadolu Üniversitesi Sosyal Bilimler Dergisi, Cilt/Vol.:12 -Sayı/No: 1 (151-166)
25. VBO, URL: https://www.veribilimiokulu.com/associationrulesanalysis/ (Erişim zamanı; Kasım, 27, 2019).
26. Sivri, E. Ş. "Veri Madenciliği/E-Ticaret İçin Ürün Tavsiye Sistemi Geliştirilmesi", Yüksek Lisans Tezi Bilgisayar Mühendisliği Anabilim Dalı İstanbul - 2015
27. Ayaz, O.Alp, S. "Saklı Markov Modeli Kullanılarak İstanbul'daki Üniversite Öğrencilerinin GSM Operatör Tercihlerini

Etkileyen Faktörlerin Analizi", Çukurova Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 33(4), ss. 203-212, Aralık 2018

28. Haidar, B. Chamoun, M. Serhrouchni, A. "Multilingual Cyberbullying Detection System Detecting Cyberbullying in Arabic Content", 2017 1st Cyber Security in Networking Conference (CSNet), 18-20 October 2017, Rio de Janeiro, Brazil.
29. Alduailej, A. H. Khan, M. B. "The challenge of cyberbullying and its automatic detection in Arabic text", 2017 International Conference on Computer and Applications (ICCA), 6-7 September 2017, Doha, United Arab Emirates.
30. Şeker, A. Diri, B. Balık, H. H. "Derin Öğrenme Yöntemleri ve Uygulamaları Hakkında Bir İnceleme", Gazi Mühendislik Bilimleri Dergisi 2017, 3(3): 47-64
31. Karabatak, S. Namlı, A. Karabatak, M. "Perceptions of High School Students Regarding Cyberbullying and Precautions on Coping with Cyberbullying", 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 22-25 March 2018, Antalya, Turkey.
32. Hussain, M. G. Al Mahmud, T. Akthar, W. "An Approach to Detect Abusive Bangla Text", International Conference on Innovation in Engineering and Technology (ICIET), 27-29 December 2018.
33. Al-Mamun, A. Akhter, S. "Social Media Bullying Detection Using Machine Learning On Bangla Text", 10th International Conference on Electrical and Computer Engineering, 20-22 December 2018, Dhaka, Bangladesh.
34. El-Halees, A. "Filtering Spam E-Mail from Mixed Arabic and English Messages: A Comparison of Machine Learning Techniques", The International Arab Journal of Information Technology, vol. 6, no. 1, 2009.
35. Hamouda, A. E.-D. A. El-zahraa El-taher, F. "Sentiment Analyzer for Arabic Comments System", (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 4, no. 3, 2013.
36. Duwairi, R. M. Marji, R. Sha'ban, N. Rushaidat, S. "Sentiment Analysis in Arabic Tweets", 5th International Conference on Information and Communication Systems (ICICS), 2014.
37. Sintaha, M. Mostakim, M. "An Empirical Study and Analysis of the Machine Learning Algorithms Used in Detecting Cyberbullying in Social Media", 2018 21st International Conference of Computer and Information Technology (ICCIT), 21-23 December 2018.
38. Shekhar, A. Mathangi, V. "A Bag-of-Phonetic-Codes Modelfor Cyber-Bullying Detection in Twitter.", 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (2018): 1-7.
39. Zois, D. S. Kapodistria, A. Yao, M. Chelmis, C. "Optimal Online Cyberbullying Detection", 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 15-20 April 2018, Calgary, AB, Canada.
40. Venckauskas, A. Karpavicius, A. Damaševičius, R. Marcinkevičius, R. Kapočiūte-Dzikiené, J. Napoli, C. "Open Class Authorship Attribution of Lithuanian Internet Comments using One-Class Classifier", 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), 3-6 September 2017, Prague, Czech Republic.
41. Egitimpedia, URL: https://www.egitimpedia.com/instagramdan-siber-zorbaliga-karsi-yeni-onlemler/ (Erişim zamanı; Haziran, 23, 2019).
42. Burnap, P. Williams, M. "Cyber Hate Speech on Twitter: An Application of Machine Classification and Statistical Modeling for Policy and Decision Making", Policy & Internet, vol. 7, no. 2, pp. 223-242.
43. Alduailej, A. H. Khan, M. B. "The challenge of cyberbullying and its automatic detection in Arabic text", 2017 International Conference on Computer and Applications (ICCA), 6-7 September 2017, Doha, United Arab Emirates.
44. Arlı, K. "Instagram Siber Zorbalık İçin Yeni Önlemler Aldı", https://shiftdelete.net/instagram-siber-zorbalik-icin-yeni-onlemler-aldi (Erişim zamanı; Mayıs, 06, 2019).
45. Ibrahim, M. Torki, M. El-Makky, N. "Imbalanced Toxic Comments Classification Using Data Augmentation and Deep Learning", 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), 17-20 Dec. 2018, Orlando, FL, USA