Avrupa Bilim ve Teknoloji Dergisi
Sayı 16, S. 826-833, Ağustos 2019

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 16, pp. 826-833, August 2019

Research Article

Sahte Web Sitelerinin Sınıflandırma Algoritmaları İle Tespit Edilmesi

Adem Korkmaz[1*], Selma Büyükgöze[2]

[1] İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Enformatik Bölümü, İstanbul, Türkiye (ORCID: 0000-0002-7530-7715)
[2] Kırklareli Üniversitesi, Teknik Bilimler MYO, Bilgisayar Teknolojileri Bölümü, Kırklareli, Türkiye (ORCID: 0000-0002-6559-7704)

(İlk Geliş Tarihi 1 Temmuz 2019 ve Kabul Tarihi 2 Ağustos 2019)

(**DOI:** 10.31590/ejosat.598036)

ATIF/REFERENCE: Korkmaz, A. & Büyükgöze, S. (2019). Sahte Web Sitelerinin Sınıflandırma Algoritmaları İle Tespit Edilmesi. *Avrupa Bilim ve Teknoloji Dergisi*, (16), 826-833.

Öz
Günümüzde kimlik avı yapan sahte web sitelerinin sayısı oldukça artmıştır. Bu web sitelerinin amaçları genel anlamda kişilerin, kişisel bilgilerini ele geçirerek çıkar sağlamaktır. Sosyal medya hesaplarımızdaki kimlik ve parola bilgilerimiz, alışveriş sitelerindeki kimlik ve adres bilgilerimiz bize ait kişisel bilgilerimizdir. Bu tür bilgiler istenmeyen kişilerin eline geçmesi durumunda, tahmin bile edemeyeceğimiz kötü sonuçlar doğurabilmektedir. Ayrıca online bankacılık işlemlerimiz gibi finansal işlemlerimizin önemli bir kısmını internet ortamında yapıyor olmamız bu tür sitelerden korunmamız açısından önemli bir sorun teşkil etmektedir. Bu amaçla antivürüs yazılım firmaları, tarayıcılar, arama motorları daha iyi kullanıcı hizmeti ve memnunniyet sağlamak açısından bu tür zararlı sitelerden kullanıcılarını korumak için çalışmalar yapmaktadırlar. Ayrıca sahte web sayfalarının kullanıcıların önüne gelmeden tespit edilip engellenmesi günümüz yapay zeka çalışmalarınında önemli bir çalışma alanı olmaktadır. Hergün milyarlarca insanın gezindiği internet ortamında bu sahte sitelerden korunmasının en kolay yöntemi, sahte web sayfalarının otomatik olarak tespit edilip engellenmesi olacaktır. Makine öğrenmesi sınıflandırma algoritmaları ile bir sayfaya ait bilgilere bakarak sistem tarafından otomatik olarak sahte veya gerçek olarak tespit edilmesi yapay zeka çalışmalarının sunduğu önemli avantajların başında gelmektedir. Bu çalışma ile bir web sitesi adresine ait belirlenmiş 10 özellik kullanılarak; bu adresin sahte mi, yoksa gerçek bir adres mi olduğu tespit edilmeye çalışılmaktadır. Çalışmada kullanılan veriler Machine Learning Repository (UCI)'dan alınmıştır. Verilerin analizi Çapraz Endüstri Standart Süreç Modeli(CRISP-DM) baz alınarak gerçekleştirilmiştir. Veri setinde web sitelerinin durumunu belirleyen nitelik (Class, Kimlik Avı=-1, Şüpheli=0 ve Meşru=1) olarak etiketlenmiştir. Çalışma da RStudio kullanılarak R programlama dili ile analizler yapılmıştır. Kullanılan sınıflandırma algoritmaları Rastgele Orman (RF), Destek Vektör Makineleri (SVM), J48, K-En Yakın Komşu (KNN) ve Naive Bayes algoritmalarıdır. Yapılan değerlendirmeler sonucunda Rastgele Orman algoritması ile en yüksek doğruluk performansı elde edilmiştir.

Anahtar Kelimeler: Sahte site, Kimlik avı, Makine Öğrenmesi.

Detection of Fake Websites by Classification Algorithms

Abstract
Nowadays, phishing web sites have been increased. The purpose of these sites is to obtain benefits by acquiring personal information of people in general. Our identity and password information in our social media accounts and identity and address information on shopping sites are our personal information. If such information is received by unwanted people, it can have bad unpredictable consequences. In addition, the fact that we carry out a significant portion of our financial transactions such as our online banking transactions on the internet constitutes an important problem in terms of protection from such sites. For this purpose, antivirus software companies, browsers, search engines are working to protect users from such harmful sites in terms of providing better user service and satisfaction. In addition, the detection and prevention of fake web pages before the users is an important area of work in today's artificial intelligence studies. The easiest method of protecting these fraudulent sites in the internet environment where billions of people are browsing every day will be to detect and block fake web pages automatically. Machine learning classification algorithms

[*] Sorumlu Yazar: İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Enformatik Bölümü, İstanbul, Türkiye, ORCID: 0000-0002-7530-7715, korkmazadem@hotmail.com

are automatically identified as fake or real by the system by looking at the information of a page and this is one of the important advantages offered by artificial intelligence studies. With this study, using 10 properties determined for a website address; it is attempted to determine whether this address is a fake or a real address. The data used in this study were taken from Machine Learning Repository (UCI). Data analysis was performed based on the Cross Industry Standard Process Model (CRISP-DM). In the data set, it is labeled as the attribute that determines the status of websites (Class, Phishing = -1, Suspicious = 0 and Legitimate = 1). The study was also done by using RStudio analysis with R programming language. The classification algorithms used are Random Forest (RF), Support Vector Machines (SVM), J48, K-Nearest Neighbor (KNN) and Naive Bayes algorithms. The highest accuracy performance was obtained by Random Forest algorithm.

Keywords: Fake site, Phishing, Machine Learning.

1. Giriş

Teknolojinin hızla gelişmesiyle birlikte internet hayatımızın vazgeçilmez bir parçası olmuş ve çoğu zaman hayatımızı kolaylaştırmıştır. Eskiden bankaya gidip yaptığımız işlemlerimizi artık evden ya da iş yerimizden internet aracılığıyla halledebilir hale gelmiş durumdayız. Faturalarımızı ödeyebilir, hesabımızdan para aktarabilir, döviz işlemlerimizi bile yapabiliriz. Ayrıca internetteki web siteleri aracılığıyla alışveriş de yapabilmekteyiz. Ancak bu işlemlerimizi yaparken güvenliğimize ne kadar dikkat ediyoruz? Öncelikle internet kullanım oranlarımıza bir bakalım.

We are Social ve Hootsuite tarafından hazırlanan "Digital in 2018 Western Asia" istatistiklerine göre Dünya'da 4,02 milyar internet kullanıcısının 5,14 milyarı ise mobil internet kullanıcısından oluşmaktadır. Bu da demek oluyor ki; Dünya popülasyonun %53'ü internet kullanırken; bu oranın %68'i ise mobil interneti kullanmaktadır. Verilen sonuçlarda bir önceki yıla göre mobil internet kullanım oranı ise %4 oranında 218 milyon kişi artmıştır. Türkiye'de ise nüfusun %67'sine tekabül eden 54.33 milyon kişinin internet kullanıcısı, mobil kullanıcı sayısının 51.45 milyon olduğu verilmektedir (Kemp, 2018). Bu durum bize internet ve mobil internetin hayatımızda ne kadar önemli bir rolü olduğunu göstermektedir.

Phishing ya da oltalama/yemleme bazı yerlerde ise e-tuzak, kimlik avı gibi kelimelerinin karşılığına bakıldığında banka şifresi, kredi kartı bilgileri, mail şifresi, kullanıcı şifresi gibi tamamen kişisel bilgilerin çalınması için yapılan bir elektronik aldatmaca işlemidir. Genellikle sosyal mühendislik yöntemi kullanılarak e-posta veya anlık mesaj halinde kullanıcıya yapılan bir dolandırıcılık türüdür (Sönmez, 2017). Bankalardan gelen şifre yenileme linki ya da alışveriş sitelerinden gelen cazip postalara tıkladığınızda bire bir aynı tasarım ile yapılmış; ancak orijinal siteyle alakası olmayan başka bir web sitesine yönlendirilirsiniz ve gerekli olan teknik bilgiye sahip değilseniz; bilgilerinizi bu siteye girdiğinizde hesaplarınıza ya da bilgilerinize ulaşıp sizi dolandırabilirler. Eğer dikkatli olunmazsa hem maddi hem de manevi olarak büyük zarar verebilirler.

Phishing ile kredi kart numaranızı ve kartınızın güvenlik kodunu (CVC), şifrelerinizi, hesap parolalarınızı, hatta banka hesap numaranızı çalabilirler. Bunun için rastgele kullanıcılara, rastgele mailler atılmaktadır. Bu yöntem genellikle e-posta ile olmaktadır. Hesabınızın çalındığına dair gelen bir e-posta, şifrenizin yenilenmesinin gerektiğine dair gelen bir mail, dikkatli olmadığınız takdirde sizi kimlik avının eşiğine getirebilmektedir.

Phishing'den korunmak için yapılabileceklere bakıldığında;

- İlk olarak kimden geldiğini bilmediğimiz mailleri açmamak,
- Bankaların bize şifre yenilemesi ya da kullanıcı bilgileri soran mail atmayacağını bilmek ve o linklere tıklamamak,
- Yarışmadan büyük meblağlar kazanıldığına dair gelen postaları açmamak,
- Yurtdışı bankalardan, adınıza ait hesapta büyük miktarda para olduğuna dair gelen mailleri dikkate almamak,
- Kısaltılmış internet sitesi adreslerini açmamak,
- İşlemleri online yaparken bulunduğumuz internet sitesinin güvenli olup olmadığını kontrol etmek, https:// protokolünün uygulanmasına dikkat etmek,
- SSL sertifikasının olup olmadığına bakmak (sayfanın altındaki kilit işareti),
- Arkadaşlarımızdan gelmiş olsa bile bilmediğimiz internet sitesi adreslerine girmemek,
- Linklere tıklamak yerine tarayıcıya kendimiz o internet adresini yazmak,
- İnternet adresi sayılardan oluşuyorsa ya da çok uzunsa bu durumda o internet adresinden kuşkulanmak ve siteyi açmamak,
- Kullandığınız cihaza ve bağlandığınız kablosuz ağa dikkat etmek (ücretsiz olan ya da şifresiz ortak alan kablosuz ağlarından giriş yapmamak),
- Kullanıcı şifrelerinizi sık sık değiştirmek,
- Her bir hesabınız için karmaşık (güvenlik seviyesi yüksek, sayı ve karakterlerden oluşan) şifreler belirlemek,
- Kullandığınız bilgisayar ya da akıllı telefonun işletim sistemini güncel tutup, antivirüs ile güvenliğini sağlamak, sayılabilir.

Phishing yapmanın tek yolu e-postalar değildir. Keylogger ya da Screenlogger adı verilen uygulama yazılımları ile bilgisayarınızda yazdığınız her karakter (keeylogger), işaretlediğiniz her alan (screen-logger) karşı tarafa gönderilir. Böylece size ait olan kişisel bilgileriniz çalınabilir. Bu yazılımlar ise siz farkında olunmadan truva atı aracılığıyla e-posta olarak gelmiş, ya da bir program içinde saklanmış olarak bilgisayarlarınıza kurulmuş olabilir.

Durumu daha iyi analiz edebilmek için; Kaspersky Lab 2018'in 3. Çeyreği saldırı istatistiklerine bakıldığında 246.695.333 tekil URL şüpheli bileşenler içermekte olup, 305.315 kişinin banka hesaplarından bu şekilde para alındığı raporlanmıştır (Chebyshev vd., 2018). Intel Security 2015'te, phishing uygulamasıyla ilgili bilgileri test etmek ve phishingi tespit etme yeteneğini ölçmek için ilginç bir çalışma yayınlamıştır. Bu çalışma için, Intel Security, kişisel verileri çalmak amacıyla hangi e-postaların kimlik avı kullandığını ve hangilerinin yasal e-postalar olduğunu tespit etmeleri için 10 e-posta sunmuştur. Araştırmanın verileri 144 ülkeden toplanmış ve 19.000 kişi araştırılmıştır. Sonuçta, insanların %97'sinin kimlik avı e-postalarını tanımlayamadığını göstermektedir (Paganini, 2015).

Durumun ciddiyeti bu çalışma sonucunda netleşmiş görünmektedir. Her 100 kişiden üç kişi sadece bu postaları ayırt edebilmekte ve bu tuzağa düşmemektedir. Bu durumda geri kalan 97 kişi phishing için potansiyel kurban haline gelmektedir.

Kimlik avından korunabilme yollarından bahsettikten sonra bir web sitesinin gerçek mi yoksa sahte mi olduğunu anlayabilmenin kişilere zarar vermeden bir yolu var mı diye bakıldığında, makine öğrenmesi yoluyla bu işin antivirüs firmaları tarafından da bu şeklide yapıldığı görülmektedir. Makine öğrenmesi, bilgisayarların gerçekleştirdikleri eylemleri daha doğru bir hale getirmek üzere değiştirmesi veya uyarlamasıdır (Marshland, 2015). Kimlik avı hırsızlığı (Phishing) gerçekleştiren web siteleri konusunda kullanıcıları henüz bir hırsızlık gerçekleşmeden uyarabilmek için bu metod kullanılabilir. Literatürde de bu amaçla yapılan çeşitli uygulamalar mevcuttur.

Chiew vd. (2019) UCI'den almış oldukları eğitim seti ile Hibrit Topluluk Özellik Seçimi (HEFS) metodu kullanarak birçok makine öğrenmesi yöntemi denemiş ve Random Forest algoritması ile eldeki özelliklerin sadece %20.8 kullanılarak phishing postalarını %94.6 doğruluk oranıyla bulmuşlardır. Sahingoz vd. (2019) çalışmalarında; 7 farklı sınıflandırma algoritması kullanarak 36.400 normal, 37.175 adet phishing postası arasından, Random Forest algoritması ile %97.98 doğruluk oranıyla kimlik avı yapan postaları bulmuşlardır. Aksu vd. (2019) çalışmalarında derin öğrenme kullanılarak, web sitelerinin sinir ağları ile gerçek olup olmadığı işaretlenmiş ve sınıflandırma yöntemleri olarak Vektör Makinesi, Karar Ağacı Ve Yığılmış Otomatik Kodlayıcılar (stacked automatic encoders) kullanmışlardır. Çalışma sonucunda, derin öğrenme tekniklerinin bir parçası olan yığılmış otomatik kodlayıcılar ile %86 başarı oranına ulaşılmıştır. Kalaycı (2018), çalışmasında makine öğrenmesi yöntemlerinin karşılaştırılmasını gerçekleştirmiş olup, 9 farklı özellik içeren 1.353 örnekten oluşan bir veri kümesinden yararlanmıştır. Rastgele Orman (RF) daha başarılı olsa da çapraz doğrulamanın kullanıldığı durumda çok katmanlı algılayıcı daha yüksek bir başarım elde etmiştir. Koşan vd. (2018) çalışmalarında Phishing Websites adlı veri seti kullanılmış ve RF ve PRISM algoritmalarının doğruluk oranında yüksek başarı gösterdiği ortaya çıkmıştır. Fette vd. (2007) çalışmalarında PILFER adlı makine öğrenmesi yaklaşımını kullanarak 860 phishing postası ve 6.950 gerçek posta arasından kimlik avı yapan sitelerin doğruluk oranını %92 olarak bulmuştur. Miyamoto vd. (2008) çalışmalarında kimlik hırsızı web sitelerinin sınıflandırılması için 9 makine öğrenme tekniği kullanmış olup, 1.500 gerçek, 1.500 sahte e-posta arasından %83 ile RF algoritmasının en yüksek başarımı vermiştir. Basnet vd. (2008) Phishing Corpus (2006) ve Spam Assassin (2006) veri setlerini kullanarak 4.000 posta içerisinden 973 phishing postasını %97.99 doğruluk oranı ile Biased Support Vector Machine (BSVM) ile bulmuşlardır.

2. Materyal ve Metot

Web sitelerinin sahte veya gerçek mi olduklarının tespitine yönelik yapılan bu çalışmada, veri madenciliği projelerinin daha az maliyetli, daha güvenilir, daha tekrar edilebilir, daha kolay yönetilebilir ve daha hızlı bir duruma getirmeyi amaçlayan Endüstri Çapraz Standart Süreç Modeli (CRISP-DM) ile analiz süreçleri gerçekleştirilmiştir.

2.1. Problemin Tanımlanması

Çalışmada internet kullanıcıların sıklıkla karşılaştıkları oltalama (Phishing) sitelerinin gerçek veya sahte oldukları tahmin edilmeye çalışılmıştır. Bu doğrultuda kullanıcıların karşılaşacakları web sitelerinin durumunun tespiti için makine öğrenmesi algoritmalarının kullanımı ve bu algoritmaların performans ölçütlerinin karşılaştırılması amaçlanmaktadır. Bu kapsamda Machine Learning Repository (UCI)'da erişime açılmış, 1.353 web sitesine ait veri bulunmaktadır (Abdelhamid vd., 2014). Bu araştırma, web sitelerin durumuna göre sitenin sahte içerikli bir web sayfası veya gerçek bir web sayfası olduğunu ortaya koyacak en yüksek performansa sahip sınıflandırma algoritmasını bulmayı amaçlamaktadır. Elde edilen en yüksek performansa sahip algoritma ile gelen web sayfaları temel özelliklerine göre filtreleme işlemi yapılarak zaman, maliyet ve en az zararla işletmenin durumu atlatması öngörülmektedir.

2.2. Veriyi Anlama

Çalışmada kullanılan veri seti, ücretsiz veri ambarlarından Machine Learning Repository (UCI)'den elde edilmiştir. 2016 yılında UCI'ye bağışlanan bu veri seti Phish Tank arşivi ve Yahoo'dan PHP'de geliştirilen bir script dosyası ile toplanmıştır. Elde edilen veriler 1.353 örnek ve 10 niteliğe sahiptir (Abdelhamid, vd., 2014). Verilerin 548'i meşru site, 702'si kimlik avı ve 103 URL ise şüphelidir. Veri setinin niteliklerine ait özellikleri Tablo 1'de verilmiştir. Nitelikler incelendiğinde hepsinin kategorik verilerden oluştuğu görülmektedir. Veri setindeki 9 nitelik tahmin etmek için, 1 nitelik ise sonuç sınıfını vermekte olup veri setinde kayıp değer sayısı ise 0'dır.

Tablo 1. Veri seti nitelik değerlerinin özellikleri

Öznitelik Adı (Tahmin Edici Nitelikler)	Açıklama	Veri Tipi
Farklı Bir Pencere (SFH)	SFH "" about: blank\"" ya da Boş mu → Kimlik Avı SFH "Farklı Bir Etki Alanını" İfade Ediyor → Şüpheli Otherwise → Meşru	Kategorik
Açılır Pencere (popUpWindow)	Sağ Tuş Devre Dışı → Kimlik Avı Sağ Tuş Uyarı Veriyor → Şüpheli Aksi takdirde → Meşru	Kategorik
Sertifika Durumu (SSLfinal_State)	HTTPS var ve Sertifikalı ve Sertifikanın Yaşı ≥ 2 Yıl → Meşru HTTPS var ve Sertifika Yok → Şüpheli Aksi takdirde → Kimlik Avı	Kategorik
Siteki Url Yüzdesi (Request_URL)	İstek URL'sinin Sayfanın <22% → Meşru İstek URL'sinin Sayfanın ≥22% ve <% 61 → Şüpheli Aksi halde → özellik = Kimlik Avı	Kategorik
Farklı Siteye Link (URL_of_Anchor)	Çapa URL'sinin Yüzdesi <31% → Meşru Çapa URL'sinin Yüzdesi ≥31% And≤67% → Şüpheli Aksi takdirde → Kimlik Avı (a href="JavaScript ::void(0)")	Kategorik
Web Trafiği (web_traffic)	Web Sitesi Sıralaması <150.000 → Meşru Web sitesi sıralaması> 150.000 → Şüpheli Aksi takdirde → Kimlik Avı	Kategorik
Link Uzunluğu (URL_Length)	URL uzunluğu <54 → özellik = Meşru URL uzunluğu ≥54 ve ≤75 → özellik = Şüpheli Aksi halde → özellik = Kimlik Avı	Kategorik
Site İsminin Yaşı (age_of_domain)	Domain Yaşı≥6 ay → Meşru Aksi takdirde → Kimlik Avı	Kategorik
URL içerisinde IP olması (having_IP_Address)	URL bilgisinde içinde bir IP Adresi varsa → Kimlik Avı Aksi halde → Meşru	Kategorik
Sınıf (Class)	Kimlik Avı, Şüpheli ve Meşru	Kategorik

2.3. Veriyi Hazırlama

Veri seti incelendiğinde tüm verilerin kategorik verilerden oluştuğu ve verilerin değer aralığının ise (-1,1) arasında olduğu görülmektedir. Veriler için bu şekilde herhangi bir normalizasyon işlemine gerek görülmemektedir.

2.4. Model Kurma

Bu çalışmada, web sayfası bilgilerinden oluşan veri setinden elde edilen deneyime bağlı olarak hedef niteliğin doğruluğunu tespit edecek en iyi algoritmanın elde edilmesi gerekmektedir. Bu doğrultuda Rastgele Orman (RF), Destek Vektör Makineleri (SVM), J48, K-En Yakın Komşu (KNN) ve Naive Bayes (NB) algoritmalarının kullanılması ile elde edilen performans ölçütlerinin karşılaştırılması ve en iyi performansı sağlayan algoritma tespit edilmeye çalışılmıştır. Kullanılan bu algoritmalar, sınıflandırma algoritması ve danışmanlı öğrenmeyi kapsayan kategorik veri setimize uygun olduğu için bu çalışmada kullanılmıştır.

2.4.1. Öğrenme yöntemi

Çalışmada mevcut etiketlenmiş girdi değerlerine dayanılarak çıktı değerlerinin tahminini gerçekleştirilmiştir. Yani geçmiş tecrübelerden geleceğe yönelik öngörülerde bulunulmuştur. Bu öğrenme türü danışmanlı (denetimli) öğrenme olarak adlandırılmaktadır (Aydın ve Özkul, 2015). Veri setindeki yüksek sayıda girdi vektörüne sonlu sayıdaki ayrık kategorilerden birinin atanması durumu sınıflandırma olarak ifade edilmiştir (Balaban ve Kartal, 2015). Bu çalışmada da kimlik avı sitelerinin durumları mevcut verilerden analiz edilerek "Kimlik Avı=-1" "Şüpheli=0" ve "Meşru=1" sınıflandırması ile tahmin edilmeye çalışılmıştır.

2.4.2. Model performans değerlendirme yöntemleri

Bu araştırmada model performans değerlendirme yöntemlerinden k-kat çapraz geçerleme yöntemi tercih edilmiştir. K sayısı araştırmalarda çoğunlukla 5 ya da 10 olarak tercih edilmektedir. Bunun için eğitim seti 5 parçaya bölünmüştür. Bu yöntem ile her defasında bir parça test, diğerleri eğitim veri seti olarak alınıp 5 defa bu süreç tekrar edilmiştir. Süreç tamamlandığında ise ortaya çıkan performans değerlendirme ölçütlerinin ortalaması alınmış ve bu ortalama model performansı olarak kabul edilmiştir (Balaban ve Kartal, 2015).

2.4.3. Model performans değerlendirme ölçütleri

Bu çalışmada model performans değerlendirme ölçümü için ikili sınıflandırmaya dayalı performans değerlendirme ölçütleri tercih edilmiştir. Çalışmanın veri setinde hedef niteliğin bulunması yani danışmanlı öğrenmenin kullanıldığı bir sınıflandırma probleminin mevcudiyeti sebebi ile doğruluk, kappa ve f-ölçütü kullanılmıştır. Makine öğrenmesinde sınıflandırma metodu ile oluşturulan modelin

başarısını ölçmek için bu ölçütler sıklıkla kullanılmaktadır. Modellerin performans sonuçlarının tespitinde çoğunlukla, gerçek sınıfların ve tahmin sınıfların değerlerini bulunduran hata matrisinde faydalanılmaktadır (Şirin, 2017).

Kontenjans tablosu/karmaşıklık matrisi gerçek değerlerin bilindiği bir test veri kümesinde bir sınıflandırma modelinin performansını tanımlamak için sıklıkla kullanılan bir tablodur. Elde edilebilecek olası sonuçlar Gerçek Pozitif (TP), Yanlış Pozitif (FP), Yanlış Negatif (FN) ve Gerçek Negatif (TN) elemanlarından oluşmaktadır (Dataschool, 2014).

Tablo 2. Kontenjans Tablosu

		Tahmin Sınıfları	
		Yes	*No*
Gerçek Sınıflar	*Yes*	True Positive (TP)	FalsePositive (FP)
	No	False Negative (FN)	True Negative (TN)

Tablo-2'deki verileri kullanılması ile model performans ölçütlerinin hesaplanması aşağıdaki gibidir (Aydemir, 2018):

- Doğruluk–Hata Oranı (Accuracy-Error Rate): Model performansının ölçülmesinde kullanılan en geçerli ve basit yöntem, modele ait doğruluk oranıdır. Doğru sınıflandırılmış örnek sayısının (TP +TN), toplam örnek sayısına (TP+TN+FP+FN) oranıdır. Hata oranı ise bu değerin 1'e tamlayanıdır. Diğer bir değişle yanlış sınıflandırılmış örnek sayısının (FP+FN), toplam örnek sayısına (TP+TN+FP+FN) oranıdır.

$$Doğruluk = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

- F-Ölçütü (F-Measure): Kesinlik ve duyarlılık ölçütleri tek başına anlamlı bir karşılaştırma sonucu ortaya koymak için yeterli değildir. Her iki ölçütü birlikte değerlendirmek daha doğru sonuçlar verir. Bunun için f-ölçütü (F) tanımlanmıştır. F-ölçütü, kesinlik (K) ve duyarlılığın (D) harmonik ortalamasıdır.

$$F\text{-}Measure = \frac{2 * Kesinlik * Duyarlılık}{(Kesinlik + Duyarlılık)} \quad (2)$$

- Kappa İstatistiği: Landis ve Koch (1977) çalışmasında kappa istatistik değerinin 0,4'ün üzerinde olması durumunda ölçümün tesadüfi olmadığını, uyum kabul edilebileceğini, kappa istatistik değerinin 0,6 ile 0,8 arasında olmasının önemli bir derecede uyum olduğunu göstermektedir. Kappa istatistiği 0,8 ile 1 arasında olması ise neredeyse mükemmel bir uyumun olduğunu gösterdiğini söylemektedir.

$$Kappa = \frac{Topla\ Doğruluk - Rastgele\ Doğruluk}{(1\text{-}\ Rastgele\ Doğruluk)} \quad (3)$$

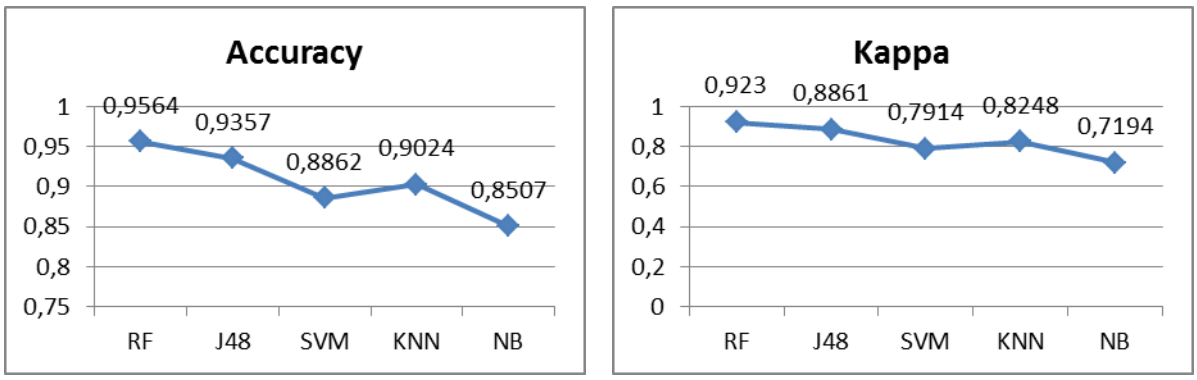
3. Araştırma Sonuçları ve Tartışma

Bu bölümde deneysel çalışmamızı oluşturan Rastgele Orman (RF), Destek Vektör Makineleri (SVM), J48, K-En Yakın Komşu (KNN) ve Naive Bayes (NB) algoritmalarının web sayfası bilgilerinden oluşan veri setinden oltalama amacıyla kullanılan web sayfalarının doğru tahmin edilebilmesine ait performans ölçütleri karşılaştırılmıştır.

Tablo 3. Sınıflandırma Algoritmalarına Ait Karşılık (Confusion) Matrisi

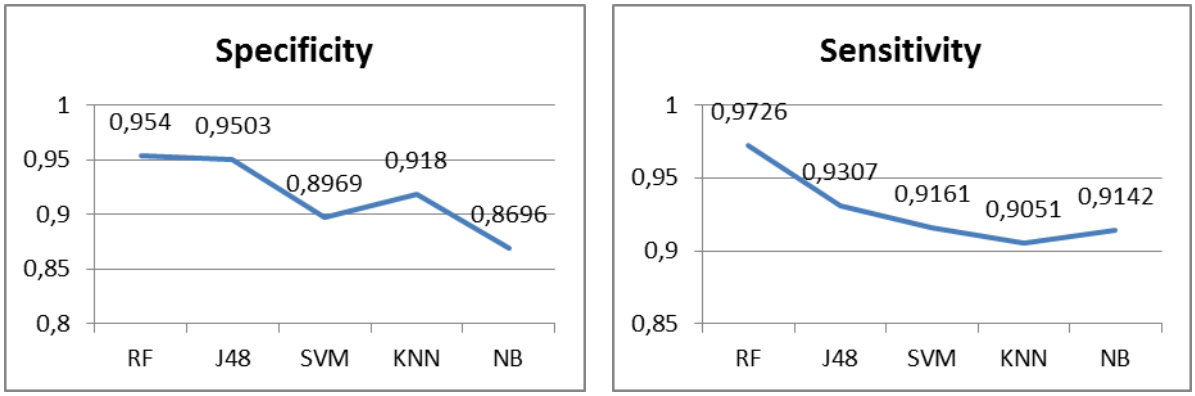
Algoritma	**Karşılık Matrisi**				
RF		Meşru	Kimlik Avı	Şüpheli	Toplam
	Meşru	533	35	2	570
	Kimlik Avı	10	660	0	670
	Şüpheli	5	7	101	113
J48		Meşru	Kimlik Avı	Şüpheli	Toplam
	Meşru	510	38	2	550
	Kimlik Avı	33	656	1	690
	Şüpheli	5	8	100	113
SVM		Meşru	Kimlik Avı	Şüpheli	Toplam
	Meşru	502	36	47	585
	Kimlik Avı	44	659	18	721
	Şüpheli	2	7	38	47
KNN		Meşru	Kimlik Avı	Şüpheli	Toplam
	Meşru	496	45	21	562
	Kimlik Avı	45	651	8	704
	Şüpheli	7	6	74	87
NB		Meşru	Kimlik Avı	Şüpheli	Toplam
	Meşru	501	52	53	606
	Kimlik Avı	47	650	50	747
	Şüpheli	0	0	0	0

Tablo 3'de modelin performans değerinin tespiti için en çok kullanılan yöntemlerin başında gelen Karşılık (Confusion) matrisi ile tüm algoritmalara ait sonuçlar gösterilmiştir. Tablo 3'de hedef niteliğimizi oluşturan sınıflara ait doğru ve yanlış tahminlerin değerlere ait verileri sunulmaktadır. Bu değerlere bağlı olarak algoritmaların performans ölçütleri karşılaştırılmıştır. Bu veriler incelendiğinde RF algoritmasının; *Meşru* sitelerden 10 tanesini kimlik avı ve beş tanesini ise şüpheli olarak gördüğü, *Kimlik Avı* sitelerinden 35 tanesini meşru, yedi tanesini şüpheli olarak gördüğü ve *Şüpheli* site kategorisindeki sitelerden yalnızca iki tanesini meşru olarak en az hata oranı ile tespit etmiştir.



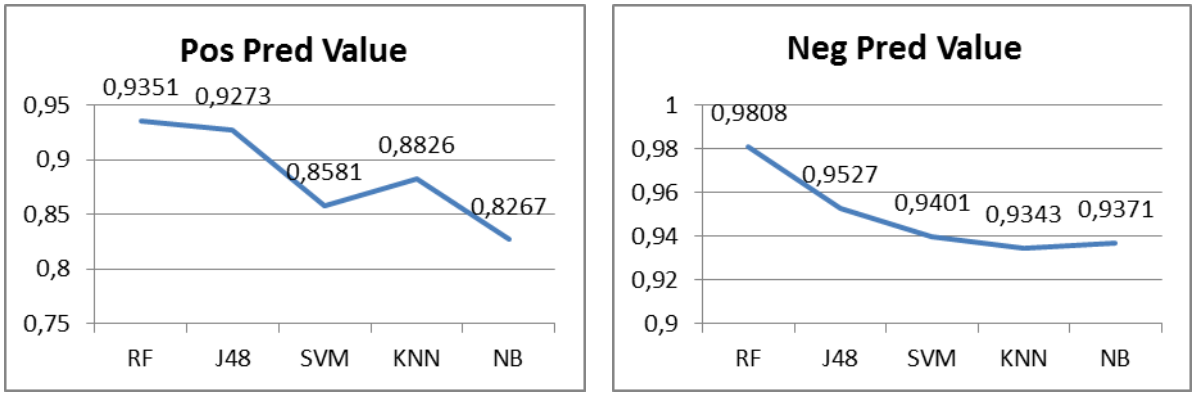
Şekil 1 - Çalışmada Kullanılan Algoritmaların Doğruluk (Accuracy) ve Kappa Ölçütleri

Şekil 1'deki veriler incelendiğinde hedef niteliğimizi oluşturan sınıflardan "Meşru" sınıfın baz alınarak yapılan değerlendirme de en yüksek doğruluk oranını RF algoritması ile elde edildiği, en düşük başarım oranının ise NB algoritması ile elde edildiği görülmektedir. Kappa istatistik değerleri incelendiğinde; 0,8 üzeri mükemmel bir uyum olduğunu gösteren aralık değeri baz alındığında RF ve J48 algoritmalarının en iyi sonucu verdiği görülmüştür.



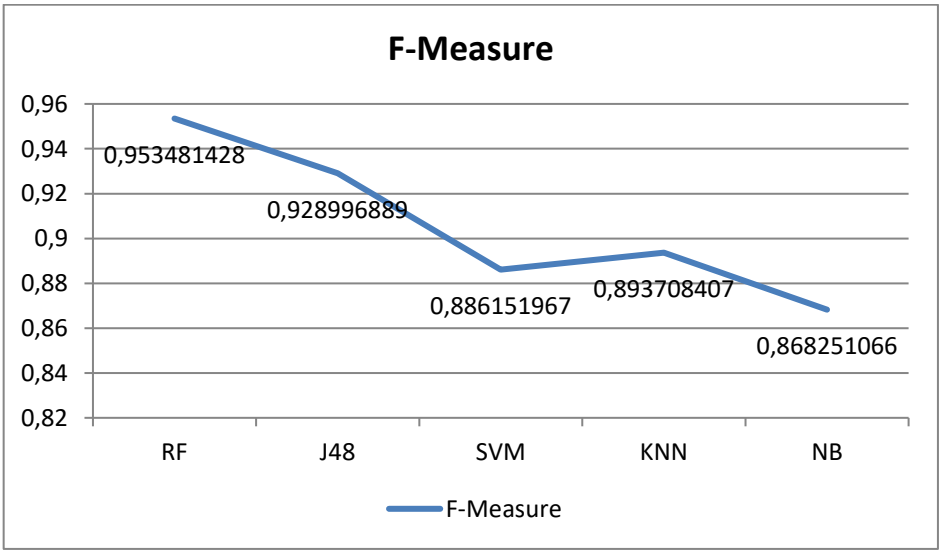
Şekil 2 - Çalışmada Kullanılan Algoritmaların Belirleyicilik (Specificity) ve Duyarlılık (Sensitivity) Ölçütleri

Şekil 2'de Belirleyicilik ve Duyarlılık verileri incelendiğinde hedef nitelik sınıfındaki pozitif ve negatif etiketlerin doğru tahmin edilmesinde RF algoritmasının her iki etiket grubunu da aynı tutarlıkla ve yüksek oranda doğru tahmin ettiği görülmektedir.J48 algoritması Belirleyicilik oranında aynı RF algortiması ile aynı başarımı sağlarken Duyarlılık oranında aynı başarımı sağlayamamaktadır.



Şekil 3 - Çalışmada Kullanılan Algoritmaların Pos. Pred. Value ve Neg. Pred. Value Ölçütleri

Şekil 3'de negatif etiketli ve pozitif etiketli sınıflara ait verilerin, ne kadar doğru olarak tahmin edildiğine ait veriler incelendiğinde karşılıklı olarak en tutarlı ve yüksek başarımlı olarak RF algoritması görülmektedir. Doğru kategorinin tespit edilmesinde J48 algoritması RF algoritması ile aynı tutarlılıkta başarım sağlarken yanlış kategorinin yespit edilmesinde aynı başarımı sağlayamadığı görülmektedir.



Şekil 4 - Çalışmada Kullanılan Algoritmaların F-Ölçütü Değeri

Şekil 4'de Kesinlik ve Duyarlılık verilerin harmonik ortalaması olarak verilen F-Ölçütü verileri incelendiğinde en yüksek başarım oranının RF algoritması ile sağlandığı anlaşılmıştır. RF algortimasını sırasıyla J48, KNN, SVM ve NB algoritmaları takip etmektedir.

4. Sonuç

Yapılan çalışma UCI veri deposunda 2016 yılında paylaşılan kimlik avı tespiti amaçlı olarak kullanılan kimlik bilgilerini ele geçirmeyi hedefleyen web sayfalarına ait veriler kullanılmıştır. Çalışmanın amacı hedef web sayfalarının kimlik avı için kullanılıp kullanılmadığını daha önceden tespit etmektir. Kimlik avı amacıyla yapılan sahte web sayfalarının temel gayesi kullanıcıların e-finans ve gizli bilgilerinin elde edilerek çıkar sağlamak oluşturmaktadır. Bu açıdan bakıldığından günümüz bilgi trafiğinin büyük oranda internet ortamında olması bu bilgilerinin büyük oranda saldırı altında olmasına sebep olmaktadır. Bu açıdan kullanıcılara yönlendirilen web sayfalarının kimlik avı için kullanılıp kullanılmadığının tespit edilmesi kurum ve bireysel kullanıcılar için durumun en az zararla atlatılması açısından büyük önem kazanmaktadır.

Çalışmada web sayfalarının kimlik avı için olup olmadıklarını doğru sınıflandırmak için RF, J48, SVM, KNN ve NB algoritmaları analiz edilmiş ve en başarılı algoritma tespit edilmeye çalışılmıştır. Algoritmalardan elde edilen sonuçlar karşılaştırıldığında en başarılı sonuç RF algoritması ile elde edilmiştir. RF algoritması hem "Meşru" web sayfalarını, hem "Şüpheli" hem de "Kimlik Avı" web sayfalarını en iyi tahmin eden algoritma olmuştur. RF algoritması çok daha fazla kök ayrımlarını ayırt etmek de olduğundan kategorik verilerin analizinde daha iyi sonuçlar vermektedir. Kappa sonuçları da incelendiğinde tesadüfi olmayan sonuçlar ile mükemmel sonuçlar elde ettiği görülmektedir. Yapılan çalışmalar incelendiğinde benzer şekilde RF algoritmasının sahte web sayflarının tespit edilmesinde yüksek başarım sağladığı görülmektedir (Miyamoto vd., 2008; Kalaycı, 2018; Koşan vd., 2018;Sahingoz vd., 2019;).

Çalışmada elde edilen tüm performans ölçütleri birbirlerini teyit ederek aynı sonuçları vermektedir. Bu doğrulta elde edilen sonuçlarının tutarlı olduğu görülmektedir. Bu çalışmanın benzer çalışmalar için geçerli sonuçlar açısından yol gösterici olacağı düşünülmektedir.

Kaynakça

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based associative classification data mining. *Expert Systems with Applications*, *41*(13), 5948-5959.

Aksu, D., Turgut, Z., Üstebay, S., & Aydin, M. A. (2019). Phishing Analysis of Websites Using Classification Techniques. In *International Telecommunications Conference* (pp. 251-258). Springer, Singapore.

Aydemir, E. (2018). Weka ile Yapay Zekâ. *Seçkin Yayınevi, Ankara*.

Aydın, S., & Özkul, A. E. (2015). Veri madenciliği ve anadolu üniversitesi açiköğretim sisteminde bir uygulama. *Journal of Research in Education and Teaching*, *4*(3), 36-44.

Balaban, M. E., & Kartal, E. (2015). Veri Madenciliği ve Makine Öğrenmesi Temel Algoritmaları ve R Dili ile Uygulamaları. *Çağlayan Kitabevi, İstanbul*.

Basnet, R., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. In *Soft Computing Applications in Industry* (pp. 373-383). Springer, Berlin, Heidelberg.

Chebyshev V., Sinitsyn F., Parinov D., Kupreev O., Lopatin E., Liskin A., (2018). IT threat evolution Q3 2018. Statistics https://securelist.com/it-threat-evolution-q3-2018-statistics/88689/, Erişim Tarihi: 25.01.2019

Chiew, K. L., Tan, C. L., Wong, K., Yong, K. S., & Tiong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, *484*, 153-166.

Dataschool, (2014). Simple guide to confusion matrix terminology. http://www.dataschool.io/simple-guide-to-confusion-matrix-terminology/. Erişim Tarihi: 30.05.2018

Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web* (pp. 649-656). ACM.

Kalaycı, T. E. (2018). Kimlik hırsızı web sitelerinin sınıflandırılması için makine öğrenmesi yöntemlerinin karşılaştırılması. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, *24*(5), 870-878.

Kemp S. (2018). Digital in 2018: World's internet users pass the 4 billion mark https://wearesocial.com/blog/2018/01/global-digital-report-2018, Erişim tarihi: 25.01.2019

Koşan, M. A., Yıldız, O., & Karacan, H. (2018). Kimlik avı web sitelerinin tespitinde makine öğrenmesi algoritmalarının karşılaştırmalı analizi. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, *24*(2), 276-282.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *biometrics*, 159-174.

Marshland S. (2015). Machine Learning An Algorithmic Perspective. 2nd ed. New York, USA, *Chapman & Hall/CRC Press*,

Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2008, November). An evaluation of machine learning-based methods for detection of phishing sites. In *International Conference on Neural Information Processing* (pp. 539-546). Springer, Berlin, Heidelberg.

Paganini P., (2015). New Intel Security study shows that 97% of people can't identify phishing emails. http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html, Erişim Tarihi: 25.01.2019

Phishing Corpus (2006), http://monkey.org/~jose/wiki/doku.php?id=PhishingCorpus

Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Machine learning based phishing detection from URLs. *Expert Systems with Applications*, *117*, 345-357.

Sönmez, Ü. (2017). "Bilişim Sistemleri Aracılığıyla Dolandırıcılık Suçu". *Dicle Üniversitesi Adalet Meslek Yüksekokulu Dicle Adalet Dergisi*, 1(2), 47-68.

Spam Assassin (2006), http://spamassassin.apache.org/

Şirin, E., (2017). Hata Matrisini (ConfusionMatrix) Yorumlama. http://www.datascience.istanbul/2017/07/02/hata-matrisini-confusion-matrix-yorumlama/. Erişim Tarihi: 29.05.2018.