YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.org.tr/ybs

Yayın Geliş Tarihi: 25.12.2024 Cilt: 11, Sayı: 1, Yıl: 2025, Sayfa: 31-44
Yayına Kabul Tarihi: 13.03.2025 ISSN: 2148-3752
Online Yayın Tarihi: 30.06.2025

MOBİL CİHAZLAR İÇİN MAKİNE ÖĞRENMESİ TABANLI URL GÜVENLİK ANALİZİ

Furkan AYDIN[1], Mesut POLATGİL[2]

[1, 2] Bilişim Sistemleri ve Teknolojileri Bölümü, Şarkışla Uygulamalı Bilimler Yüksekokulu, Sivas Cumhuriyet Üniversitesi, Sivas, Türkiye

ÖZET

Bu çalışmada, bireylerin cihazlarına ulaşan bağlantılar hakkında, tıklama öncesi bilgi sahibi olabilmeleri adına bir mobil uygulama hazırlanmıştır. Uygulama, Dart-Flutter programlama dili kullanılarak hazırlanmıştır. Geliştirilen optik karakter tanıma (OCR) teknolojisi, mobil uygulamaya entegre edilmiştir. Optik karakter tanıma teknolojisi sayesinde, kullanıcılar herhangi bir bağlantıya tıklamadan önce, cihazlarına ulaşan bağlantıların ekran görüntülerini uygulamaya yükleyerek bağlantı metnini uygulamaya tanıtabilmektedir. Uygulamaya yüklenen görüntü formatındaki bağlantı metni, optik karakter tanıma teknolojisi kullanarak dijital metne dönüştürülmektedir. Dijital metin, analiz edilmek üzere hazırlanmış olan flask tabanlı uzaktan sunucuya gönderilmektedir. Uzaktan sunucu içerisinde ISCX-2016 veri setine uygulanan makine öğrenmesi modelleri mevcuttur. Yüklenen URL metinleri, makine öğrenmesi modelleri ile analiz edilmektedir sonrasında analiz sonucu kullanıcıya iletilmektedir.

Anahtar Kelimeler: Makine Öğrenmesi, URL Güvenliği, Siber Güvenlik, Mobil Cihaz

MACHINE LEARNING-BASED URL SECURITY ANALYSIS FOR MOBILE DEVICES

ABSTRACT

This study presents a mobile application designed to provide users with pre-click information about URLs appearing on their devices. The application was developed using the Dart-Flutter programming language and integrates Optical Character Recognition (OCR) technology. With this technology, users can upload screenshots containing URLs to the application before clicking on them. The OCR system extracts the URL text from the image and converts it into a digital format. The extracted digital text is then sent to a remote Flask-based server for analysis. The server hosts machine learning models trained on the ISCX-2016 dataset to classify and assess the URLs. Once the analysis is completed, the results are communicated back to the user, enabling them to make informed decisions about the links they encounter.

Keywords: Machine Learning, URL Security, Cybersecurity, Mobile Device.

1. GİRİŞ

Teknolojinin hızla gelişmesi ile teknolojik cihazların gelişmiş versiyonları kullanıma sunulmaktadır. Teknolojik cihazlar insan yükünü hafifletmede ve günlük işlerimizi yerine getirmekte oldukça yeterlidir. Örneğin bireyler bankacılık işlemlerini, alışverişlerini, çalışmalarını, diğer bireylerle

iletişimlerini teknolojik cihazlar vasıtasıyla gerçekleştirebilmektedir. Gün geçtikçe teknolojik cihazlar hem yazılım hem de donanım alanında geliştirilmekte ve sürekli olarak yenilenmektedir. Teknolojik cihazların gelişmesi sırasında cihazlarda güvenlik açıkları meydana gelmiştir. Güvenlik açıkları, cihazların sistemindeki zayıflığa verilen isimdir. Bu zayıflıklardan yararlanmak isteyen kötü amaçlı kişiler tarafından, cihaz kullanıcılarına yönelik gerçekleştirilen saldırılara siber saldırı adı verilmektedir. İnternetin gelişimi ile birlikte, saldırılacak olan potansiyel sistem sayısı da fazlasıyla artmıştır. Siber saldırılara neden olan pek çok faktör bulunmaktadır. İnternet tasarımında mevcut olan zayıflıklar, internetin çalışması yönünde hazırlanan sistemlerin birçoğunun açık ve şifresiz olması, yönetim eksikliği gibi faktörler, sistemin donanım ve yazılım kısmında mevcut olan hatalar ve önemli sistemlerin çevrimiçi erişim hakkına sahip olması gibi faktörlerden ötürü siber saldırılar gerçekleşebilmektedir (Clarke ve Knake, 2015). Bu tür saldırılardan korunmak adına iki adet yöntem mevcuttur. Bunlardan ilki tamamen güvenli bir sistem oluşturmaktır fakat bu tarz bir sistem oluşturmak oldukça zordur çünkü kriptografik yöntemlerin kırılabilmesi veya sistem kullanıcılarının şifrelerini unutabilmesi gibi birçok neden ile bu yöntem pratik açıdan mümkün olmamaktadır. İkinci yöntem ise siber saldırıların tespitini sağlayarak sonrasında gerekli önlemleri almaktır (Şenkaya ve Adar, 2014). Kurumlar, siber saldırılardan korunmak ve bu saldırıları erken tespit edebilmek adında ciddi yatırımlar yapmaktadırlar. Yine de dünya üzerinde bulunan pek çok özel ve devlet kurumları siber saldırıların odağı olabilmektedir (Gökçe vd., 2014). Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA) tarafından 2013 yılına ait bir çalışmada, Vergi Dolandırıcılığı, Kurumsal Hesapların Devri, Kimlik Hırsızlığı, Hassas verilerin çalınması, Fikri Mülkiyet Hırsızlığı olmak üzere beş adet siber suç listelenmiştir (AICPA, 2013).

Bireyler sanal ortamda barındırdıkları fotoğrafları, kişisel verileri ve kimlik bilgilerini tıpkı gerçek hayatta olduğu gibi korunmak zorundadır. Bu korunmanın sağlanması adına etkili uygulamalara ihtiyaç duyulmaktadır (Kumar vd., 2005). Bireyler, verilerinin korunması konusunda bilinçlenmeli ve olası saldırılara karşı kendini güvende hissetmelidir. Bireylere sanal ortamda güvenlik sağlayabilmek adına mobil cihazlarda ve bilgisayarlarda, güvenlik uygulamaları geliştirilmiştir. Sanal ortama en çok giriş yapılan cihazlardan bir tanesi de mobil cihazlardır. Mobil cihazlar, kendisinden daha büyük olan bilgisayarların yaptıkları çoğu işlemi yerine getirebilen cihazlardır. Bilgisayarlara göre daha küçük ve taşınabilir olmasından ötürü küçük bilgisayarlar olarak değerlendirilebilmektedir (Liyanage vd., 2016).

Mobil cihazlar, insan yaşamını birçok yönden kolaylaştırarak günlük işlerin daha verimli ve pratik bir şekilde yürütülmesine katkı sağlasa da çeşitli güvenlik zafiyetleri barındırması nedeniyle riskler içermekte ve endişelere yol açmaktadır. Gittikçe artan mobil cihaz kullanıcısı sayısıyla paralel olarak, olası mağdurların da sayısı artmaktadır. Mobil cihazlar da güvenlik kapsamında korunması gereken cihazlardır. Çünkü bireyler, çeşitli iletişim uygulamaları kullanarak diğer insanlarla iletişime geçebilir, bankaların hazırladıkları uygulama üzerinden online bankacılık işlemlerini gerçekleştirebilir, cihaz kamerası üzerinden fotoğraf ve video çekebilir ve bunları cihazında depolayabilir, sağlık ve devlet kurumlarındaki ve gerektiği durumlarda T.C. kimlik numaralarını kullanarak işlemlerini gerçekleştirebilirler. Bu nedenle bireyler olası siber saldırılara karşı bilinçlenmeli ve verilerini güvende tutmalıdır. Siber saldırıların hedefi haline gelen bireylerin en değerli verileri arasında kimlik bilgileri, Türk vatandaşları için e-Devlet hesap bilgileri, sağlık ve hastane kayıtları, pasaport ve ehliyet bilgileri, mobil bankacılık uygulamalarında kullanılan hesap ve kredi kartı bilgileri, çalıştıkları kuruma ait konum ve detaylar, maaş bilgileri, harcama geçmişi ile çeşitli uygulama ve web sitelerinde kullanılan kullanıcı adı ve şifreler yer almaktadır.

Mobil cihazlara yönelik birçok saldırı türü bulunmaktadır ve bu saldırılara yönelik mobil cihaz kullanıcılarının dikkat etmesi gereken bazı temel güvenlik kuralları mevcuttur. Örneğin, mobil cihazlara erişim sağlamak için güçlü şifreler oluşturulmalı, cihazlara yönelik özel olarak geliştirilen antivirüs yazılımları kullanılmalı ve zararlı yazılım içerebilecek uygulamalardan korunmak amacıyla yalnızca güvenilirliği kanıtlanmış uygulamalar yüklenmelidir. Ayrıca, e-posta veya kısa mesaj yoluyla iletilen bağlantılara tıklamaktan kaçınılmalı, Bluetooth ve Wi-Fi gibi kablosuz bağlantılar yalnızca gerekli durumlarda etkinleştirilmeli, işletim sistemi düzenli olarak güncellenmeli ve çalınma veya kaybolma durumlarına karşı "Find My Phone" gibi güvenlik önlemleri aktif hale getirilmelidir. Bunun yanı sıra, telefon numarası gibi kişisel bilgiler yalnızca güvenilir platformlarla paylaşılmalıdır (Özcan, 2009).

Mobil cihazlara yönelik yapılan saldırılarda büyük bir çoğunluk yüzdesine sahip saldırı türü, tehlikeli içerik bulundurabilecek olan URL'lerdir. URL'ler, protokol, dosya yolu ve alan adı olmak

üzere üç adet bölümden oluşur (Köksal vd., 2021). Bireylere e-posta, mesaj gibi yollarla ulaşan bu zararlı bağlantılar, tıklanması halinde bireylere maddi ve manevi anlamda zarar verebilmektedir. Truva atları, kimlik avları gibi kötücül yazılım araçları, saldırmayı hedefleyen bir biçimde URL'leri bir araç olarak kullanmaktadır (Arslan, 2021). Her gün birçok kötü niyetli URL adresi oluşturulmaktadır. Bu sebeple, ağ saldırılarının önüne geçmek ve ağ güvenliğini sağlamak amacıyla web linklerinin belirlenmesi gerekmektedir (He vd., 2021). URL'ler web sitelerine dair önemli zengin bilgileri taşımakta olup sınıflandırma amacı ile kullanılabilmektedirler. Domain adresleri birçok sözcüksel ifadeyi ve ayırıcıyı içerisinde barındırır. Örneğin; nokta (.), taksim (/), soru işareti (?) gibi ifadeler barındırır. URL'ler bir IP adresini temsil etmektedir. Zararlı olmayan bir domain adresi genellikle bağlantılı olduğu kuruluşu temsil etmektedir (Arslan, 2021).

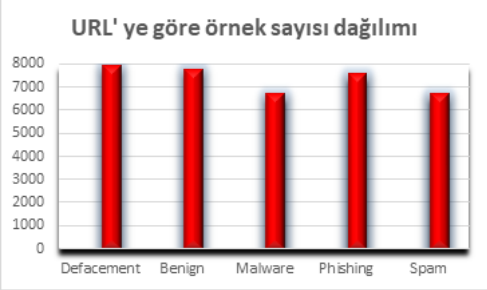
Çalışmada, bireylerin cihazlarına ulaşan bağlantılara tıklamadan önce sorgulayabilmeleri adına bir mobil uygulama hazırlanmıştır. Uygulama, Dart-Flutter programlama dilleri kullanarak hazırlanmış olup, olası maddi ve manevi zararın önüne geçilmesi hedeflenmiştir. Uygulamamızda, zararlı ve zararsız URL'lerden elde edilmiş olan 80 adet öznitelik barındıran ISCX-2016 veri seti kullanılmıştır. Veri setine makine öğrenmesi metotlarından olan yapay sinir ağları, rastgele orman algoritması ve k-en yakın komşu algoritmaları uygulanarak doğruluk olasılığının artırılması sağlanmıştır. Bu çalışmada önerilen yaklaşım, mobil uygulama ve flask tabanlı uzaktan sunucu üzerinden URL sorgulama işlemini gerçekleştirebilmesi sayesinde literatürde yer alan çalışmalardan farklıdır ve bu özellikler çalışmamıza özgünlük sağlamaktadır.

2. VERİ SETİ

Bu çalışmada, Kanada Siber Güvenlik Enstitüsü tarafından oluşturulan ISCX-2016 veri seti kullanılmıştır. Söz konusu veri seti, literatürde birçok akademik çalışmada güvenlik analizleri ve siber tehdit tespiti amacıyla yaygın olarak kullanılmaktadır. ISCX-2016 veri setinde, farklı siber tehdit türlerini içeren beş farklı URL kategorisi yer almaktadır. Bu kategoriler; spam, kötü amaçlı yazılım (malware), zararsız (benign), kimlik avı (phishing) ve web sitesi tahrifatı (defacement) olarak sınıflandırılmaktadır. Spam URL'ler, kullanıcıları istenmeyen reklam içeriklerine yönlendiren bağlantılardır. Kötü amaçlı yazılım (malware) içeren URL'ler, zararlı yazılımlar dağıtarak cihazlara yetkisiz erişim sağlamayı veya sistemlere zarar vermeyi amaçlamaktadır. Zararsız (benign) URL'ler, herhangi bir tehdit unsuru içermeyen güvenli bağlantılardır. Kimlik avı (phishing) URL'leri, kullanıcıların kişisel bilgilerini ele geçirmek amacıyla güvenilir web siteleri gibi görünen sahte sayfalara yönlendiren bağlantılardır. Web sitesi tahrifatı (defacement) URL'leri ise, saldırganlar tarafından ele geçirilerek içeriği değiştirilmiş veya zarar verilmiş web sitelerine ait bağlantılardır (Mamun vd., 2016).

Veri seti içerisinde Defacement türünde 7930, Benign türünde 7781, Malware türünde 6712, Phishing türünde 7586, Spam türünde ise 6698 adet bağlantı örneği bulunmaktadır (Şekil 1).

Şekil 1. ISCX-2016 Veri Seti URL Dağılımları (Arslan, 2021)



Veri seti içerisinde 80 adet öznitelik bulunmaktadır. Bu özniteliklerden bazıları; Karakter süreklilik oranı, URL uzunluğu, TLD (Top Level Domain), Ldl getArg, token, harf ve sembol sayımı, Spchar URL.

2.1 Konu ile İlgili Çalışmalar

ISCX-2016 veri setine dair çalışmalar incelendiğinde (Uçar vd., 2019), veri seti üzerinde LSTM, CNN ve İkili sınıflandırma metotları kullanmıştır. LSTM (Uzun kısa süreli bellek) metodunda %91,13, CNN (Evrişimli Sinir Ağları) metodunda ise %95,37 oranında bir doğruluk tespiti sağlanmıştır. (Dawn

vd., 2019) ise yapmış oldukları çalışmada lexical ve host tabanlı 32 adet özniteliği çıkarmıştır. Bu özniteliklere ExtraTree ve Adaboost sınıflandırma yöntemlerini kullanarak, ExtraTree yönteminde %91, Adaboost yönteminde ise %90 oranında bir doğruluk tespiti sağlanmıştır. Powell vd. (2019), yapmış oldukları çalışmada, veri seti üzerinde karar ağacı ve EkstraTree kullanarak %99 oranında doğruluk oranına ulaşmıştır. Kapil vd. (2019), veri seti içerisinde bulunan 80 adet öznitelik içerisinden 47 tanesini seçerek bu özniteliklere J48, Random Forest (Rastgele Orman), Bayes-Net, Lazy ve İkili Sınıflandırma yöntemlerini kullanmıştır. Elde edilen sonuçlar incelendiğinde J48 yöntemi ile %94,4, RF ile %96,1, BayesNet ile %92,1, Lazy ile %95,4'lük bir doğruluk oranı elde edilmiştir. Wang vd. (2020) ise yapmış oldukları çalışmada veri seti üzerinde Naive Bayes algoritmasını kullanarak ikili sınıflandırma metodu oluşturmuştur. Öznitelik seçme algoritması kullanılmıştır. Kullanılan algoritma sonucunda seçtikleri üç adet özelliği kullanarak oluşturdukları model, %90,18 oranında bir doğruluk tespitine sahiptir. Deebanchakkara vd. (2019), yapmış oldukları çalışmada veri seti üzerinde Random Forest algoritmasını kullanarak %97,0'lık bir doğruluk oranına ulaşmışlardır. Arslan (2021), yapmış olduğu çalışmasında, veri seti üzerinde Doc2vec yapısında, LR (lojistik regresyon), SVM (destek vektör makineleri), LDA (Doğrusal Ayırma Analizi), Adaboost, KNN (k-en yakın komşu), Random Forest, ExtraTree sınıflandırma yöntemlerini kullanmıştır. Lojistik regresyon yönteminde %98,9, LDA yöntemiyle %97,5, Adaboost yöntemiyle %96,3, KNN yöntemiyle %98,9, RF yöntemiyle %98,8, SVC yöntemiyle %98,8, ExtratTree yöntemi ise %98,8 oranında bir doğruluk tespitine sahiptir. Veri seti dışında gerçekleştirilen diğer çalışmalar incelendiğinde, Akar (2023), çalışmasında spam URL'leri tespit etmek adına büyük ölçekli bir veri setine en popüler 8 makine öğrenmesi yöntemini uygulamıştır. Lojistik Regresyon yöntemi ile %79,89, Karar Ağaçları yöntemi ile %93,55, Random Forest algoritması ile %94,16, Naive Bayes yöntemi ile %76,59, KNN yöntemi ile %91,84, XGBoost yöntemi ile %91,1, Adaboost yöntemi ile %82,36, Gradient Boosting yöntemi ile %85,91 doğruluk oranı elde etmiştir. Odeh vd. (2021) gerçekleştirmiş oldukları çalışmada, pudding tarafından hazırlanan "URL- Spam ve Spam olmayan" adlı veri setini kullanmıştır. Veri seti, yaklaşık 148.300 adet URL içermektedir ve bunların üçte biri spam URL olarak işaretlenmiştir. Veri setine uygulanan makine öğrenmesi yöntemlerinden elde edilen sonuçlar incelendiğinde, Random Forest yöntemi ile %97,55, Bagging yöntemi ile %98,64, Stacking yöntemi ile %98,45, MultinomialNB yöntemi ile %73,05, BernoulliNB yöntemi ile ise %77,75 doğruluk oranı elde edilmiştir.

Literatür çalışmaları, URL sınıflandırma konusunda gerçekleştirilmiştir. Bu çalışma, URL'lerin mobil cihazlar üzerinden anlık olarak sorgulanabilmesini sağlamaktadır. URL sınıflandırma işleminin mobil cihazlar üzerinden anlık olarak sorgulanması, bu çalışmayı diğer çalışmalardan ayıran bir özellik olmuştur.

3. YÖNTEM

Çalışmada ISCX-2016 veri seti içerisinde bulunan 80 adet öznitelikten model performansına katkı sunmayan 40 tanesi çıkarılmış geriye kalan 40 öznitelik kullanılmıştır. Öznitelik sayısı 40'a düşürülerek daha verimli bir model eğitimi sağlanmış ve modelin aşırı öğrenmeden kaçınarak daha genelleştirilebilir sonuçlar vermesi sağlanmıştır. Seçilen 40 öznitelik, URL sorgulama işleminde kullanılması en gerekli olanlar arasından belirlenmiştir. ISCX-2016 veri seti içerisinde 7781 tanesi zararsız ve 28.917 tanesi zararlı olan 36.698 adet URL mevcuttur. Bu URL'ler defacement, benign, spam, phishing ve malware olmak üzere beş adet kategoriye ayrılmıştır. Tablo 1'de kategoriler içerisindeki URL'lerin kayıt sayısı verilmiştir. Veri seti üzerinde, yapay sinir ağları, rastgele orman algoritması ve k-en yakın komşu yöntemleri kullanılarak her üç yöntem için de doğruluk oranları hesaplanmıştır.

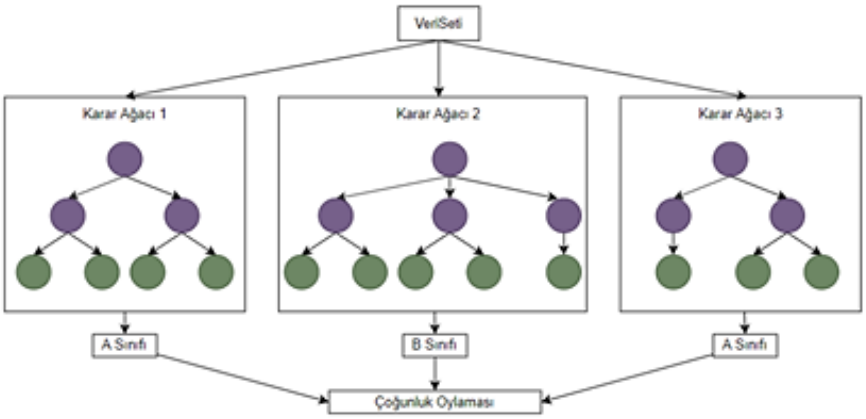
Tablo 1: URL türüne göre kayıt sayıları (Köksal vd., 2021)

URL Türü	Kayıt Sayısı
Benign	7781
Defacement	7931
Phishing	7577
Spam	6698
Malware	6711

3.1 Rastgele Orman Algoritması

Rastgele orman algoritması, karar ağacına bağlı olarak gerçekleşmektedir. Verilerin aşırı öğrenilmesi probleminin ortadan kalkmasına yardımcı olmaktadır. Rastgele orman algoritması, çeşitli karar ağaçları yoluyla karar ağaçlarını farklı gözlem modelleri sayesinde eğiterek çeşitli modellerin oluşmasına olanak tanır. Bu sebeplerden ötürü uygulamamızda kullanılmasına karar kılınmıştır. Rastgele orman algoritması kullanarak oluşturduğumuz model %97 doğruluk oranına sahiptir. Şekil 2'de rastgele orman algoritmasının çalışma mantığına dair bir görsel verilmiştir.

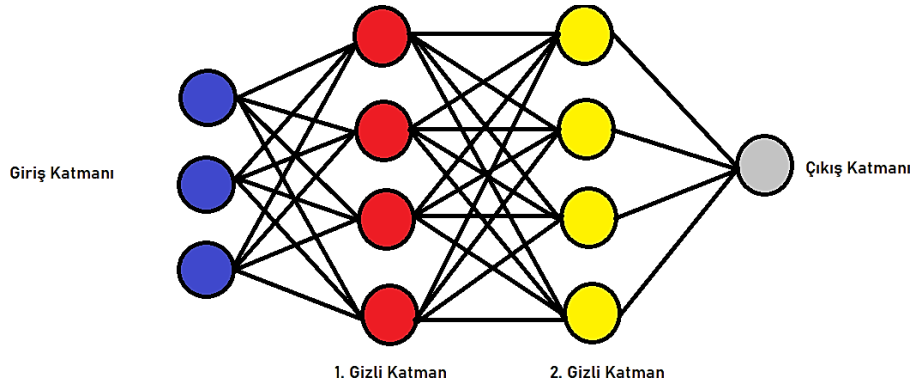
Şekil 2. Rastgele Orman Algoritması Temsili (Köksal vd., 2021)



3.2 Yapay Sinir Ağları

Yapay sinir ağları insan beyninin fonksiyonu olan öğrenme yönteminden yola çıkarak öğrenme, anımsama ve genelleme gibi yöntemler ile elde ettiği verilerden yeni verilerin oluşturulması gibi işlemlerin yerine getirilebildiği bir yöntemdir (Öztürk ve Şahin, 2018). Yapay sinir ağları, insan beynindeki nöronlardan esinlenmiştir. Yapay sinir ağları, tıpkı insan beynindeki nöronlar gibi birbirine bağlanmış pek çok ağdan oluşan matematiksel sistemlerdir. Şekil 3'te yapay sinir ağlarının modellerinden olan çok katmanlı algılayıcı modeline dair bir örnek verilmiştir.

Şekil 3. Genel Yapay Sinir Ağı Modeli (Yavuz, 2021)

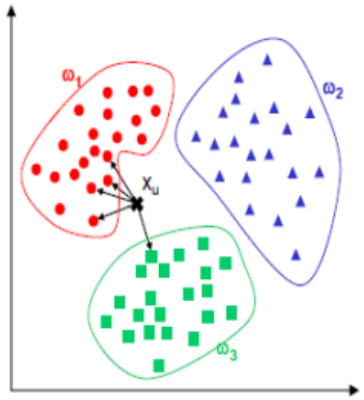


Yapay sinir ağları öğrenme, genelleme, eksik veri ile çalışma, fazla sayıda değişken kullanabilme gibi özelliklerinden ötürü çalışmada kullanılmasına karar verilmiştir. Bu yönleri sayesinde yapay sinir ağları, URL'lerin sınıflandırılması konusunda kolaylık sağlamaktadır. Yapay sinir ağları kullanarak hazırlanan model %88'lik bir doğruluk oranına sahiptir.

3.3 K-En Yakın Komşu

K-En yakın komşu algoritması, sınıflandırma ve regresyon yöntemlerinde kullanılır. Sınıflandırma amacı ile kullanılacağı zaman, k-en yakın komşu algoritması veri noktasını sınıflandırmak üzere etrafındaki en yakın k noktasını kullanır. Bu durumda en çok tekrar eden kategori, URL'nin tahmini kategorisi olarak belirlenecektir. Şekil 4'te k-en yakın komşu algoritmasının çalışmasına dair bir görsel verilmiştir.

Şekil 4. KNN Sınıflandırma Örneği (Gutierrez-Osuna, 2005)



K-En yakın komşu algoritması, veri seti içerisinde bulunan kategoriler içerisindeki bağlantıların benzerliklerine göre tahminlerin yapılmasını sağlar. Bireyler uygulamaya bir bağlantı yüklediğinde, k-en yakın komşu yöntemi ile sınıflandırılarak benzer olduğu bağlantıların bulunduğu kategoriye yerleştirilmesini sağlamaktadır. K-En yakın komşu algoritmasının kullanılması sonucunda %91 oranında sınıflandırılma başarısı sağlanmıştır.

Rastgele orman algoritması sonucunda elde ettiğimiz %97 doğruluk oranı, literatürle benzer bir sonuçtur. Bu çalışma, diğer çalışmaların birçoğunun aksine URL sınıflandırma işleminin mobil uygulama üzerinden çevrimiçi yapılmasını sağladığı için bu doğruluk oranı yeterli görülmüştür. Literatürde yer alan pek çok çalışma URL'lerin sınıflandırılmasına yönelik gerçekleştirilmiştir.

4. Mobil Uygulamanın Hazırlanması

Çalışmada kullanılan ISCX-2016-URL veri seti üzerinde, yapay sinir ağları, rastgele orman algoritması ve k-en yakın komşu yöntemleri kullanılarak her üç yöntem için de doğruluk oranı hesaplanmıştır. Analiz işleminin gerçekleşebilmesi için kullanıcının hazırlamış olduğumuz uygulamaya kendisine ulaşan bağlantı görselini yüklemesi gerekmektedir. Kullanıcı bağlantı görselinin fotoğrafını çekebilir veya ekran görüntüsü yoluyla uygulamaya yükleyebilir. Bağlantı metninin görsel olarak uygulamaya yüklenmesinin sebebi bireylerin kopyalama amacıyla dahi olsa bağlantıya temas etmemelerini sağlamaktır. Yüklenen görseldeki bağlantı metni Optik Karakter Tanıma yöntemi ile görselden ayıklanarak metne dönüştürülür. Ayıklanan bağlantı metni veri seti içerisinde sorgulanır ve bu sorgulama sonucu kullanıcıya bildirilir.

Hazırlamış olduğumuz sistemin işleyişini mobil uygulamamızın görsellerini kullanarak inceleme aşamasına geçelim. Şekil 5'te uygulamamızın ana sayfası gözükmektedir. Uygulamamızın arayüzü kullanıcılar tarafından kolayca anlaşılabilir bir şekilde tasarlanmıştır. Uygulamamızın ana sayfasında beş adet buton bulunmaktadır (Şekil 5).

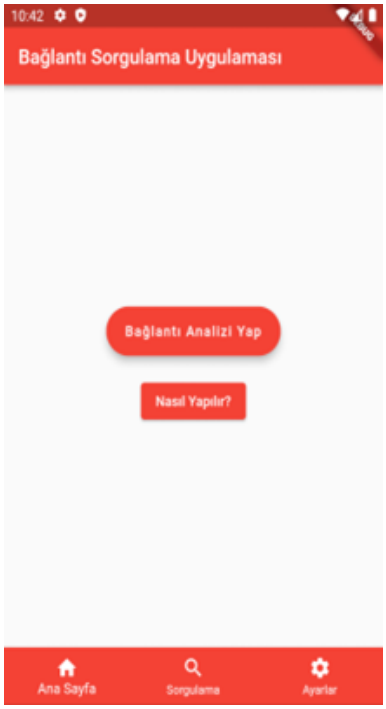
Ana sayfada bulunan "Bağlantı Analizi Yap" butonuna tıklandığında, bağlantının resminin çekilmesi gereken zamanlar için kameraya yönlendirme butonu ve eğer ekran görüntüsü alındıysa, ekran görüntüsünün sisteme yüklenmesi adına galeriye yönlendirme butonu bulunmaktadır (Şekil 6). Kullanıcının sisteme yüklediği resmi sonrasında yalnızca bağlantı metni gözükecek şekilde kırpması gerekmektedir. Çünkü OCR (Optik Karakter Tanıma) sistemi, eğer görselde, bağlantı metni dışında farklı bir yazı varsa onu da metin içeriğine dahil edecektir (Şekil 7). Kırpma işlemi gerçekleştikten sonra bağlantı, uzaktan sunucu içerisinde bulunan veri setinde analiz edilecektir. Bağlantı metni analiz süreçlerinden geçirildikten sonra kullanıcıya Zararlı Bağlantı, Zararsız Bağlantı, Bilinmeyen Bağlantı şeklinde üç adet bağlantı türünden hangisine ait olduğu bildirilecek ve güvenlik konusunda gerekli uyarılar yapılacaktır (Şekil 8).

Bağlantının Şekil 9'da görüldüğü gibi bilinmeyen bağlantı olarak tespit edilmesi durumunda kullanıcının yetkililerle canlı sohbet ortamından iletişime geçerek bağlantı sonucunu öğrenebilmesi adına 'Yetkiliye Bağlan' adında buton yerleştirilmiştir. Butona tıklanıldığında, kullanıcılar firebase tabanlı olarak kurulan sohbet kısmında, yetkililerle iletişime geçebilir, sohbet kısmına görsel yükleyebilir ve bağlantı sonucunu öğrenebilir (Şekil 10). Bu sayede eğer bağlantı sonucu 'bilinmeyen

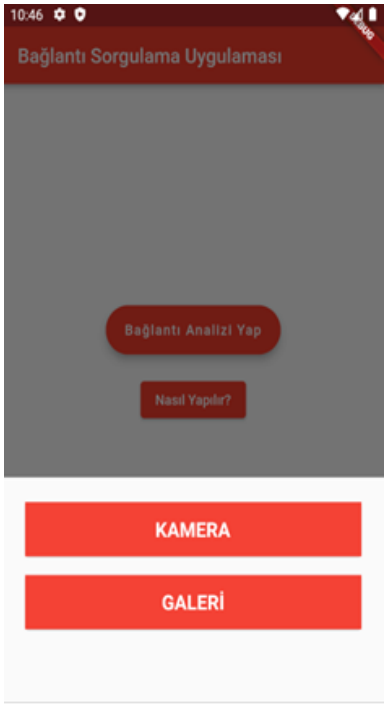
bağlantı' olarak tespit edilse dahi, kullanıcının yüklemiş olduğu bağlantıya dair net bir bilgi almasını sağlayan bir sistem entegre edilmiştir.

Uygulamanın anasayfasında sağ alt köşede bulunan "Ayarlar" butonuna tıklandığında Bildirimler, Sıkça Sorulan Sorular (SSS), Hakkımızda butonları bulunmaktadır (Şekil 11). Sıkça sorulan sorular sekmesine girildiği zaman uygulamaya dair kullanıcının sorabileceği soruların bulunduğu bir kısım bulunmaktadır. En sık karşılaşılan sorular ve cevapları bu kısımda derlenmiştir. Kullanıcılar bu kısımdan zararlı ve zararsız bağlantılara dair bilgi edinebilir, cihaz güvenliğini artırmaya yönelik ipuçlarından yararlanabilir (Şekil 12).

Şekil 5. Ana Sayfa

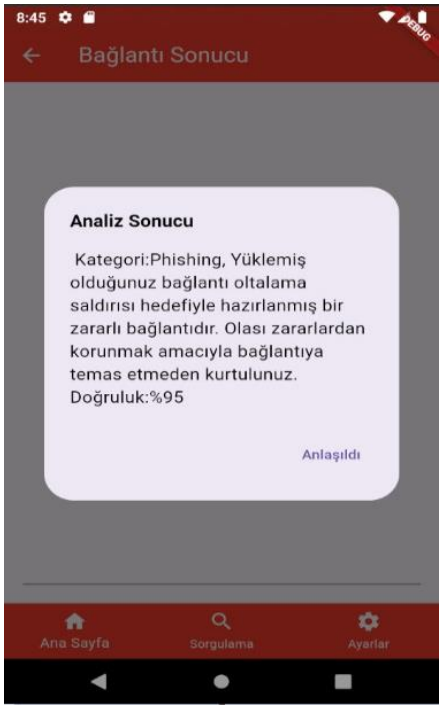


Şekil 6. Bağlantı Yükleme

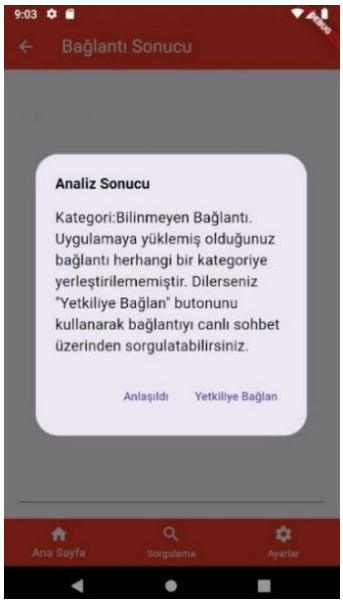


Şekil 7. Görüntü Kırpma

Şekil 8. Bağlantı Sonucu



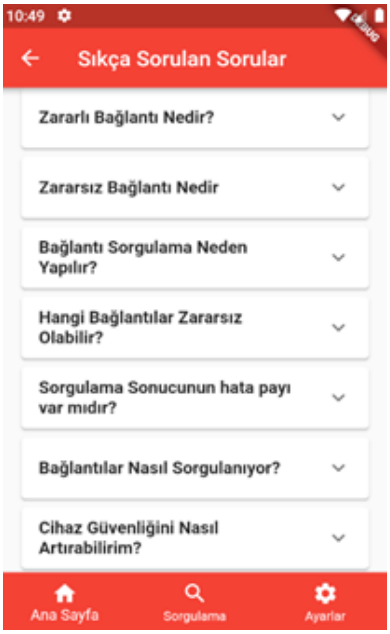
Şekil 9. Bilinmeyen Bağlantı Tespiti



Şekil 10. Yetkiliye Bağlanma

Şekil 11. Ayarlar Sekmesi

Şekil 12. Sıkça Sorulan Sorular

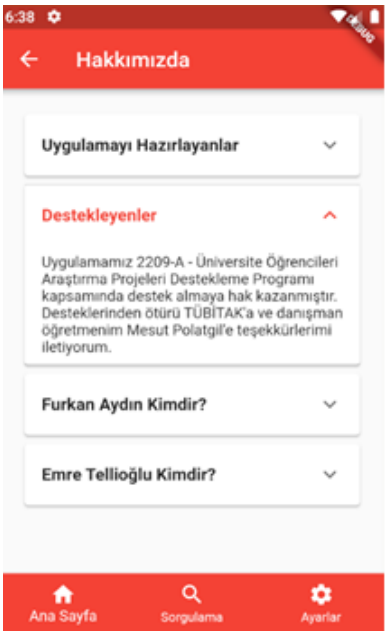


Sıkça Sorulan Sorular sekmesindeki soruların cevapları, soruya tıklandığı an kullanıcıya gözükmektedir. Örneğin "Zararlı Bağlantı Nedir" adlı soruya tıklandığında, kullanıcının zararlı bağlantılar hakkında bilgi sahibi olmasını sağlayacak bir cevap metni bulunmaktadır (Şekil 13).

Alt kısımdaki menüde bulunan üç adet butondan bir tanesi olan "Ana Sayfa" butonu, tıklandığı zaman kullanıcıyı anasayfaya yönlendirmeyi sağlar. Sorgulama butonuna tıklandığında ise kullanıcı hangi sayfada olursa olsun sorgulama işleminin başlamasını sağlar. Ayarlar butonundaki bir diğer işlev olan "Hakkımızda" butonuna tıklandığı zaman ise "Uygulamayı Hazırlayanlar", "Destekleyenler" ve "Furkan Aydın" kimdir olmak üzere üç adet bilgi kutucuğu bulunmaktadır. "Destekleyenler" kutusuna tıklandığı zaman proje süresince destek aldığımız TÜBİTAK'a ve Mesut Polatgil'e teşekkür metni bulunmaktadır (Şekil 14).

Şekil 13. Soru Örneği

Şekil 14. Destekleyenler



Uygulamanın pek çok güvenlik açığı kapatılmıştır. Rate limiting (istek sınırlandırma) kullanılarak IP başına 10 saniyede bir sunucuya URL sorgulama isteği gönderilmesi sağlanmıştır. Bu sayede DDoS (dağıtılmış ağ saldırıları) saldırılarının önüne geçilmiştir. Sunucuya erişim yalnızca yetkili kişiler tarafından gerçekleştirilmektedir. XSS (siteler arası betik çalıştırma) saldırısının önüne geçilmesi adına gelen ve giden verilere encoding (karakter kodlaması) uygulanmıştır. Yetkili kişi ile gerçekleştirilen görüşmeler TLS (taşıma katmanı güvenliği) kullanılarak uçtan uca şifrelenmektedir. Konuşma esnasında karşıdaki kişinin saldırgan olması durumunda çok fazla mesaj göndermesi durumu sistemin çökmesine neden olabilmektedir. Bu durumun önüne geçilmesi adına Flask-Sınırlayıcı kullanılmıştır. Kullanıcılar 10 saniyede bir mesaj gönderebilmektedir. Bu sayede, olası bir sistem çökmesinin önüne geçilmiştir.

4.1 Uygulamanın Avantajları

Literatür çalışmaları incelendiğinde URL'lerin sınıflandırılması ve zararlı bağlantıların tespitine dair pek çok çalışma yer almaktadır fakat bu çalışmaların uygulanabildiği bir mobil uygulamanın hazırlanmasına dair tarafımızca hiçbir çalışmaya rastlanmamıştır. Çalışmada hazırlamış olduğumuz mobil uygulama ile bu eksikliğin giderilmesi amaçlanmıştır. Uygulamamız, bireylerin kendilerine ulaşan bağlantıları sorgulamayı alışkanlık edinmesi ve zararlı bağlantılar konusunda bilinçlenmesini sağlamak amacıyla hazırlanmıştır çünkü bağlantılar, sorgulanmadan tıklanması halinde eğer zararlı bir bağlantı ise bireyler birçok riskle karşılaşılabilmektedir. Kötü niyetli kişiler bağlantıya tıklayan bireylerin kimlik bilgilerine ulaşabilir, kart bilgilerini ele geçirebilir veya bireyleri elde ettikleri bilgiler doğrultusunda tehdit edebilir. Bireyler, bilgilerinin karşı tarafa geçmesi halinde endişe, korku ve kendilerine psikolojik hasar verebilecek birçok durumla baş başa kalabilir ve manevi duyguları zarar görebilir. Kart bilgileri, bankacılık işlemleri gibi önemli bilgilerin karşı tarafa geçmesi durumunda bireylerin maddi varlıkları çalınabilir veya elde edilen kart bilgileri ile bireyin izni olmadan satın alınmalar gerçekleşebilir. Bireyler uygulamamız sayesinde kendilerine ulaşan bağlantıları sorgulama alışkanlığı edinmektedir. Sorgulama alışkanlığı edinildiğinde bireyler, bağlantılarını sorgulayarak zararlı çıkması halinde erken tespitini sağlayacaktır ve bağlantıdan uzak durarak olası maddi ve manevi zararların önüne geçilecektir. Bağlantıların sorgulama amacıyla ekran görüntüsünün alınıp uygulamaya yüklenmesi gerekmektedir. Bu noktada ekran görüntüsünün yüklenmesindeki temel amaç, bireylerin kopyalamak için bağlantı metninin üzerine basılı tutması gibi herhangi bir temasa ihtiyaç kalmadan ekran görüntüsü üzerinden OCR tekniği ile bağlantı metninin uygulama tarafından çıkarılması sayesinde bireylerin bağlantıya minimum temas ile sorgulama işlemini gerçekleştirmelerini sağlamaktır.

5. BULGULAR

Bu çalışmada ISCX-2016 veri seti içerisinde bulunan 40 öznitelik, Python dili ve Numpy kütüphanesi kullanılarak makine öğrenmesi yöntemlerinden olan yapay sinir ağları, rastgele orman algoritması ve k-en yakın komşu yöntemleri uygulanmıştır. Bu yöntemler sayesinde bağlantının sorgulanması ve uygun bir kategoriye yerleştirilerek sınıflandırılması sağlanmıştır. Tablo 2'de uygulanan makine öğrenmesi yöntemleri ve doğruluk oranları verilmiştir. Makine öğrenmesi tüm kategorilere uygulanmıştır.

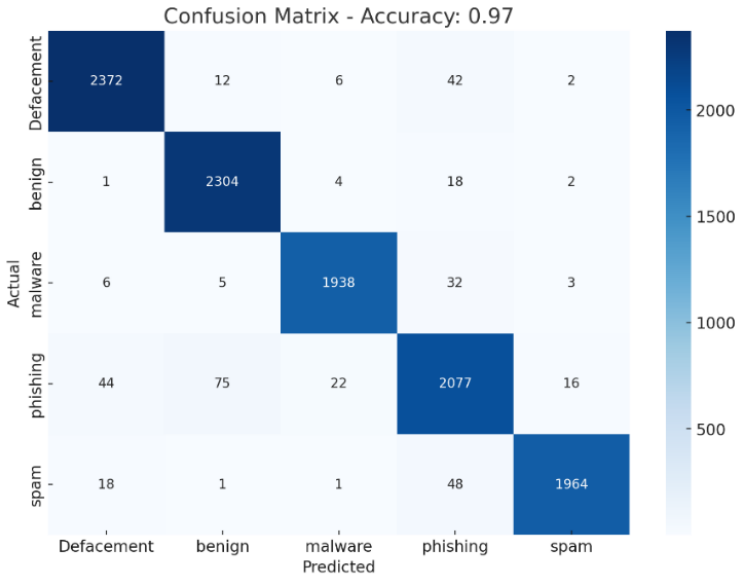
Tablo 2. Makine Öğrenmesi Yöntemleri ve Detayları

Algoritma	Doğruluk	Kesinlik	Duyarlılık	F1 skor	Süre
Rastgele Orman	%97	%98	%97	%97	20sn
KNN	%91	%93	%92	%91	15sn
YSA	%88	%87	%88	%87	35sn

Tablo 2'ye göre en yüksek doğruluk rastgele orman algoritması ile elde edilmiştir. Yaklaşık %97 gibi yüksek bir oranla sınıflandırma sağlanmıştır. En düşük başarı oranı ise yaklaşık %88 ile Yapay Sinir Ağları yöntemi ile elde edilmiştir. Süre bakımından ise 15 saniye ile en hızlı algoritma KNN olmuştur. Tabloda yer alan süreler eğitim süreleridir. KNN yöntemi sınıflandırma başarısı olarak %91 ile diğer modellere göre düşük bir oran elde etmiştir. Hem sınıflandırma başarısı hem de zaman yönünden incelendiğinde Rasgele orman algoritmasının daha iyi sonuç verdiği görülmektedir.

Rastgele orman algoritması, kesinlik, duyarlılık ve F1 skor metriklerinde en yüksek değerleri elde ederek diğer modellerden üstün performans göstermiştir. Bu nedenle analiz edilecek URL'ler uzaktan sunucuda ilk önce rastgele orman algoritması ile analiz edilecektir. Şekil 15'te modelin ürettiği karışıklık matrisi (confusion matrix), kategoriler arasındaki tahmin değerleri gösterilmiştir. Model, yüksek doğruluk oranı ile zararlı bağlantıların sınıflandırılmasında başarılı olmuştur. Çalışmamızın sonuçları, Deebanchakkara vd.'nin 2019 sonuçları ile uyumludur ve %97 doğruluk oranı ile güvenilir bir sınıflandırma sağlamaktadır.

Şekil 15. Confusion Matrix Sonuçları



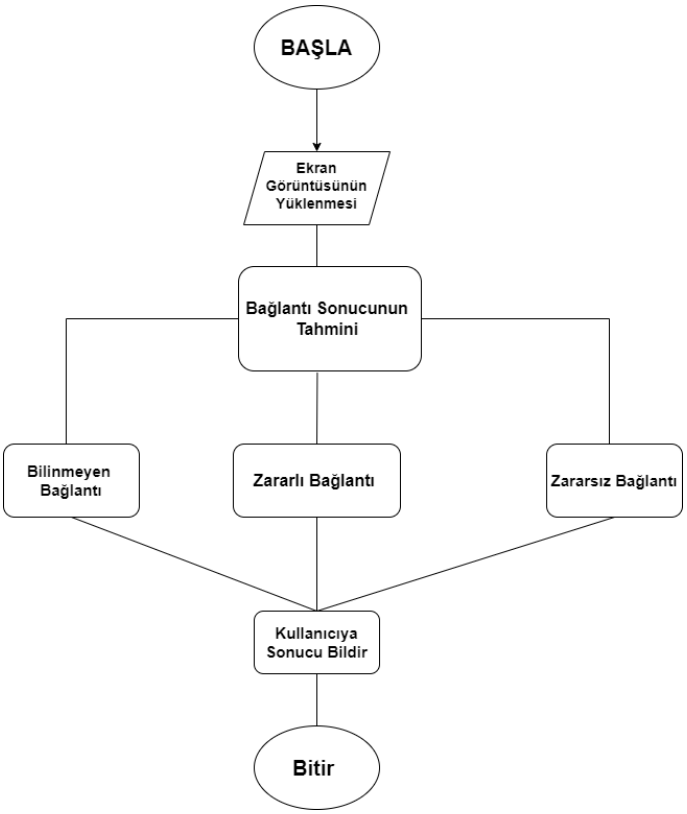
Tablo 3'te, uygulamış olduğumuz rastgele orman algoritması sonucunda veri setinde bulunan kategorilere göre elde edilen doğruluk oranları bulunmaktadır. Kategori düzeyinde kesinlik, duyarlılık ve F1 score değerleri bu tabloda bulunmaktadır.

Tablo 3. Rastgele Orman Algoritması Detayları

	Kesinlik	**Duyarlılık**	**F1 score**
Defacement	0,97	0,98	0,98
Benign	0,96	0,99	0,98
Malware	0,99	0,98	0,98
Phishing	0,94	0,93	0,93
Spam	0,99	0,97	0,98

Sorgulama işleminin mobil cihaz kullanıcısı bireyler tarafından da uygulanabilmesi adına Dart-Flutter dili kullanılarak mobil uygulama hazırlanmıştır. Mobil uygulamanın genel işleyişi, Şekil 15'te sunulan akış diyagramında ayrıntılı olarak gösterilmektedir.

Şekil 15: Mobil uygulamanın akış diyagramı



Tablo 4'te uygulamada gerçekleştirilen işlemler, kullanılan paketler ve bu işlemler sonucunda geçen ortalama süre bulunmaktadır. Elde edilen süreler mobil cihazda analiz edilmiştir, bu süreç cihaz, internet hızı gibi faktörlere göre değişebilmektedir.

Tablo 4. Uygulamada Kullanılan Yöntemler ve Detaylar

Yöntem	**Kullanılan paket, yazılım**	**Ortalama süre**
Görsel Seçme İşlemi	Image_picker	2 saniye
Kırpma İşlemi	Image_cropper	2 saniye
Bağlantı Metninin Çıkarılması	OCR	3 saniye
Analiz İşlemi	Flask sunucusu	4 saniye
Sonucun kullanıcıya bildirilmesi	Http isteği	3 saniye

Tablo 4'e göre kullanıcılar, kendilerine ulaşan bağlantıların ekran görüntüsünü alıp image_picker paketi sayesinde uygulamamıza yükleyebilmektedir. Kullanıcının seçtiği görselin ekrana düşmesi 1-2 saniye aralığında gerçekleşmektedir. Görsel kullanıcının ekranına düştükten sonra kullanıcı bu ekran görüntüsünü, yalnızca bağlantı metni gözükecek şekilde kırpmalıdır. Kırpma işlemi image_cropper paketi kullanılarak gerçekleştirilmektedir. Kırpılmış bağlantı metni sorgulanmak üzere Python dilinin flask kütüphanesi kullanılarak hazırlanan uzaktan sunucuya gönderilmektedir. Bağlantı metni uzaktan sunucuda makine öğrenmesi yöntemleri tarafından sınıflandırılmaya sokulmaktadır. Sınıflandırma sonucu yaklaşık olarak 4-5 saniye aralığında gerçekleşmektedir. Sonrasında bu sonuç 1-2 saniye aralığında düzenlenerek kullanıcıya dönüt olarak gönderilmektedir. Kullanıcının yüklediği görsel uzaktan sunucuya http isteği ile gönderilmektedir ve aynı şekilde kullanıcıya dönüt verilirken, http isteği üzerinden bu işlem gerçekleştirilmektedir.

6. TARTIŞMA

Bu çalışma, URL'lerin zararlı olma ihtimaline karşı erken tespitinin sağlanmasına odaklanmaktadır. Uygulama, Dart-Flutter dilinde hazırlanmıştır. Uygulama içerisinde görüntü yükleme sürecini hızlandırmak adına image_cropper, image_picker kütüphaneleri kullanılmıştır. Kötü niyetli URL'lerin tespitinin sağlanması sırasında ISCX-2016 veri seti içerisinde bulunan 80 adet özelliğin 40 adet özelliği kullanılmıştır. Veri setinde 1 zararsız 4 adet zararlı bağlantı kategorisi mevcuttur. Zararlı bağlantı tespiti sırasında veri setine makine öğrenmesi yöntemleri olan yapay sinir ağları, rastgele orman algoritması ve k-en yakın komşu yöntemleri uygulanmıştır. Bu yöntemler Python dilinde uygulanmış olup pandas, matplotlib ve scikit-learn kütüphaneleri kullanılmıştır. Kullanılan yöntemler sonucunda, k-en yakın komşu yönteminde ortalama %91 doğruluk oranı, yapay sinir ağları yönteminde ortalama %94 doğruluk oranı ve rastgele orman algoritmasında ise %97 doğruluk oranı elde edilmiştir. Rastgele orman modeli, (Köksal vd., 2021)'in çalışmasında kullandığı rastgele orman algoritması modelinden %2 daha düşük doğruluk oranına sahiptir. Kullanmış olduğumuz rastgele orman algoritması modeli, (Powell vd., 2019) tarafından kullanılan ve %90,18 doğruluk oranına sahip olan Naive Bayes modelinden 6,82 daha fazla doğruluk oranına sahiptir. Çalışmamızın diğer çalışmalardan farkı olarak URL sorgulanması işleminin mobil ortamda gerçekleştirilmesi işlemi örnek gösterilmektedir. Model hazırlarken kullanmış olduğumuz 40 özelliğin artırılması durumunda, daha yüksek doğruluk oranlarının elde edileceği düşünülmektedir. Hazırlamış olduğumuz uygulama yalnızca ekran görüntüsü alınabilecek şekilde ekrana sığan URL'leri analiz edebildiği için ekrana sığmayacak derecede uzun URL'lerin tespiti sağlanamamaktadır. Bu durum da uygulamamızın insanlığa yararını olumsuz etkilemektedir. Bu durumun çözülmesi adına kapsamlı araştırmalarda bulunup uzun URL'lerin analizini sağlayabilecek farklı bir yöntem bulunması halinde uygulamamıza entegre edilecektir. URL'lerin anlık analizini sağlayan uygulamamız, 15 saniye civarında analizi bitirip kullanıcıya bildirmektedir. Bu süre, bireyin internet hızı, cihaz donanımı gibi konular doğrultusunda daha da artabilmektedir. Bu duruma uygulama içerisinde kullanılan paketlerin ve anlık analiz durumunun sebep olduğu düşünülmektedir. Bu duruma çözüm olarak uygulama hızını artırma konusunda çalışmalar yapılacak olup analizin ve sonucun bildirilmesinin minimum süreye indirilmesi sağlanacaktır.

7. SONUÇ

Günümüzde siber saldırılar, özellikle zararlı URL'ler üzerinden gerçekleştirilen kimlik avı ve kötü amaçlı yazılım yayılımı gibi yöntemlerle bireyleri hedef almaktadır. Bireylerin bu tür tehditlere karşı bilinçlenmesi ve güvenli internet kullanımı için destekleyici araçlara sahip olması önem arz etmektedir. Bu çalışma, bireylerin mobil ortamda kendilerine ulaşan URL'leri analiz edebilmelerine olanak sağlayan bir mobil uygulama geliştirmeyi amaçlamıştır. Uygulamanın kullanıcı testi yapılmıştır. 140 kişiden geri bildirim alınmıştır. Kullanıcı testi süreci çeşitli bölümlerde öğrenim gören öğrenciler tarafından gerçekleştirilmiştir. Geri bildirimler doğrultusunda özellikle bilgilendirici kısım olması adına hazırlanan sıkça sorulan sorular sayfasının gerekli bilgileri taşıdığına dair olumlu dönüşler alınmıştır. Uygulamanın arayüzünün oldukça anlaşılır olduğu yönünde dönütler alınmıştır. Uygulama, yazılım alanında eğitim alan 20 öğrenci ile test edilmiş ve %85 oranında olumlu dönüşler alınmıştır. En sık eleştirilen kısım, uzun URL'lerin ekran görüntüsüne sığmamasıdır. Günümüzde pek çok akıllı telefonda scrolling screenshot özelliği bulunmaktadır. Bu özellik ekran görüntüsü alma özelliğini kaydırarak ekranın tamamının yakalanmasını sağlar. Bu sayede URL uzunluğunun ekrana sığmama sorunu çözülmektedir. Bu özelliği barındırmayan cihazları kullanan kullanıcılar ise, yetkiliye bağlanarak

kendilerine ulaşan URL metninin videosunu sisteme yükleyebilmektedir. Bu sayede URL, yetkililer tarafından incelenecek ve kullanıcıya gerekli dönüş sağlanacaktır. Gelecekte çalışmalarda kullanılan makine öğrenmesi yöntemlerine ek olarak LSTM ve DNN modellerinin eklenmesi değerlendirilecektir. Ayrıca analiz sürecinin kısalması adına gerekli optimizasyon yöntemlerinin araştırılması sağlanarak bireylerin daha hızlı bir şekilde URL sorgulama işlemini gerçekleştirmeleri hedeflenmektedir.

TEŞEKKÜR

Bu proje, TÜBİTAK 2209-A kapsamında 1919B012301687 numaralı proje ile destek almaya hak kazanmıştır. Bizleri desteklediği için TÜBİTAK'a teşekkürler ederiz.

KAYNAKÇA

Ada, S. ve Tatlı, H. S. (N.D.). Akıllı telefon kullanımını etkileyen faktörler üzerine bir araştırma.

AICPA (2013). "The top 5 cybercrimes", https://www.Aicpa.Org/Content/Dam/Aicpa/İnterestareas/Forensicandvaluation /Resources/Electronicdataanalysis/Downloadabledocuments/Top-5- Cybercrimes.Pdf.

Akar, F. (2023). Data correlation matrix-based spam URL detection using machine learning algorithms. Journal of Scientific Reports-A, (056): 56-69.

Arslan, R. S. (2021). Kötücül URL filtreleme için derin öğrenme modeli tasarımı. Avrupa Bilim ve Teknoloji Dergisi, (29): 122-128.

Deebanchakkarawarthi G., Parthan AS, Sachin L. ve Surya A. (2019). Classification of URL into malicious or benign using machine learning approach. International Journal Of Advanced Research in Computer And Communication Engineering, 8(2): 1-4.

Divya K., Anupriya A. B., Nidi M. ve Aditya J. (2019). Machine learning based malicious URL detection. International Journal of Engineering and Advanced Technology, 8(4): 1-5.

Dwan R. A. Jr. ve Tavares A. M. (2019). Predictive analysis: Machine learning model for URL classification. Yayınlanmamış Yüksek Lisans Tezi. Worcester Polytechnic Institute, Worchester.

Gökçe, K. G., Şahinaslan, E. ve Dinçel, S. (2014). Mobil yaşamda siber güvenlik yaklaşımı, 195(270.7): 349-1.

Gutierrez-Osuna R. (2005). Introduction to pattern analysis. Course Notes, Department Of Computer Science. Texas: A&M University.

He, S., Li, B., Peng, H., Xin, J. ve Zhang, E. (2021). An Effective cost-sensitive XGBoost method for malicious URLs detection in imbalanced dataset. IEEE Access, 9: 1-8.

ISCX-URL2016. "Legitimate And Phishing URL Dataset", https://www.unb.ca/cic/datasets/url2016.html, (2023, 10 Aralık).

Köksal, K., Doğan, B. ve Altıkardeş, Z. A. (2021). Topluluk sınıflandırıcı kullanarak zararlı URL tespiti. Veri Bilimi, 4(3): 113-122.

Kumar, V., Srivastava, J. ve Lazarevic, A. (2005). Managing cyber threats: Issues, approaches, and challanges. Springer.

Liyanage, M., Abro, A. B., Ylianttila, M. ve Gurtov, A. (2016). Opportunities and challenges of software-defined mobile networks in network security. IEEE Security & Privacy, 14(4): 34-44

Mamun, M. S. I., Rathore, M. A., Lashkari, A. H., Stakhanova, N. ve Ghorbani, A. A. (2016). Detecting malicious URLs using lexical analysis. In Network and System Security: 10th International Conference, NSS 2016, Taipei, Taiwan, September 28-30, 2016, Proceedings 10 (pp. 467-482). Springer International Publishing.

Odeh, O. H., Arram, A. ve Njoum, M. (2023). Classification of spam URLs using machine learning approaches. ArXiv preprint arXiv:2310.05953.

Özcan, S., Mayıs 2009, Yeni nesil şebekelere (NGN) düzenleyici yaklaşım ve Türkiye önerileri. Yayınlanmamış Uzmanlık Tezi. Bilgi Teknolojileri İletişim Kurumu

Öztürk, K. ve Şahin, M. E. (2018). Yapay sinir ağları ve yapay zekâ'ya genel bir bakış. Takvim-İ Vekayi, 6(2): 25-36.

Powell A, Bates D, Van Wyk C ve De Abreu D. (2019). A crosscomparison of feature selection algorithms on multiple cyber security datasets. Stellenbosch Universit.

R. A. Clarke ve R. K. Knake (2010). Cyber war-the next threat to national security and what to do about it, New York: Harpercollins Publishers.

Uçar E. ve Uçar M. (2019). A deep learning approach for detection of malicious URLs. 6. International Management Information Systems Conference: Connectedness And Cybersecurity.

Utku, A. ve Doğru, İ. A. (2016). Mobil kötücül yazılımlar ve güvenlik çözümleri. Gazi University Journal of Science GU J Sci Part C, 4(2).

Wang S, Wang Y. ve Tang M. (2020). Auto malicious websites classification based on naive bayes classifier. 2020 IEEE 3rd International Conference On Information Systems And Computer Aided Education (ICISCAE).

Yavuz, A. (2021). Derin öğrenme algoritmaları ile trafik işaret ve levhalarının tanımlanması. Yayınlanmamış Yüksek Lisans Tezi. Pamukkale Üniversitesi Fen Bilimleri Enstitüsü, Denizli.

Yeliz Şenkaya, Ö. G., ve Aadar, A. G. U. G. Siber Savunmada Yapay Zekâ Sistemleri Üzerine İnceleme.