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

Derleme Makalesi / Review Article

İstenmeyen E-postaların Tespiti için Kullanılan Yöntemlerin İncelenmesi

Review of the Methods Used for the Detection of Spam

E. Enes Eryılmaz*[1], Erdal Kılıç[2]

[1] Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun, enes.eryilmaz@bil.omu.edu.tr, ORCID: 0000-0003-1163-970X
[2] Ondokuz Mayıs Üniversitesi, Bilgisayar Mühendisliği Bölümü, Samsun, erdal.kilic@bil.omu.edu.tr, ORCID: 0000-0003-1585-0991

MAKALE BİLGİLERİ

Makale geçmişi:

Geliş: 6 Nisan 2020
Düzeltme: 6 Mayıs 2020
Kabul: 22 Mayıs 2020

Anahtar kelimeler:

İstenmeyen e-posta tespiti, yapay zekâ, makine öğrenmesi, derin öğrenme

ÖZET

İstenmeyen elektronik postalar alıcıya rızası dışında gönderilen ve genellikle kötü niyetli veya tanıtım amaçlı olan kişilerin başvurduğu bir yöntemdir. Elektronik postalar, kullanımının kolaylığı, maliyetlerinin ucuz olmasından dolayı propaganda, reklam, oltalama yapmak isteyen kişi veya topluluklar tarafından etkin bir biçimde kullanılmaktadır. Amaçlarını gerçekleştirmek isteyen kişi veya topluluklar hiç tanımadıkları e-posta hesaplarına gereksiz ve istenmeyen postalar gönderirler. Bu çalışmada, istenmeyen elektronik postaların filtrelenmesi için literatürde bulunan yöntemler incelenmiştir. Bu istenmeyen e-posta filtreleme yöntemleri temel olarak yapay zekâ tabanlı olmayan ve yapay zekâ tabanlı olan şeklinde iki ana başlık altında incelenmiştir. Yapay zekâ tabanlı olmayan yöntemlerin istenmeyen e-posta tespitinde etkili sonuçlar verdiği ancak literatürde bu yöntemleri atlayabilen tekniklerin olduğu görülmektedir. İstenmeyen e-posta tespitinde yapay zekâ tabanlı makine öğrenmesi algoritmaları kullanan sistemlerin popülaritesinin arttığı ve araştırmaların bu yönde ivme kazandığı görülmektedir. Özellikle derin öğrenme yöntemleri yüksek performansları nedeniyle spam tespitinde tercih edilmeye başlamıştır. Literatürde klasik makine öğrenme yöntemlerinden olan Bayes, Destek Vektör Makinesi, Yapay Sinir Ağı, Rastgele Orman, Çok Katmanlı Algılayıcı, K-En Yakın Komşu gibi algoritmalarının kullanıldığı spam tespit yöntemlerinde yüksek başarım sağladığı görülmektedir. Uzun Kısa Süreli Bellek ve Evrişimsel Sinir Ağı algoritmalarını kullanan derin öğrenme temelli spam tespit yöntemlerinin başarım oranlarını daha da artırdığı farklı veri kümeleri kullanılarak gösterilmiştir. Ayrıca spam tespit sistemlerinde bulunan açık problemler ve Türkçe özelinde bu çalışmaların hangi aşamada olduğu da bu çalışmada irdelenmiştir ve çeşitli öneriler yapılmıştır.

Doi: 10.24012/dumf.715638

ARTICLE INFO

Article history:

Received: 6 April 2020
Revised: 6 May 2020
Accepted: 22 May 2020

Keywords:

Spam e-mail detection, artificial intelligence, machine learning, deep learning

ABSTRACT

Spam e-mails are a method that is sent to the recipient without his consent and is generally used by people with malicious or promotional purposes. E-mails are actively used by people or communities who want to make propaganda, advertising, phishing because of their ease of use and low cost. People or communities who want to achieve their goals send spam to the e-mail accounts they never knew. In this study, the methods in the literature for filtering spam e-mails were examined. These spam filtering methods are mainly examined under two main headings: non-artificial intelligence-based and artificial intelligence-based. It is seen that non-artificial intelligence-based methods give effective results in detecting spam, but there are techniques in the literature that can bypass these methods. It is seen that the systems that use artificial intelligence-based machine learning algorithms in detecting spam have increased in popularity and research has gained momentum in this direction. Especially deep learning methods have been preferred for spam detection due to their high performance. In the literature, it is seen that it provides high performance in spam detection methods using algorithms such as Bayes, Support Vector Machine, Artificial Neural Network, Random Forest, Multilayer Perceptron, and K-Nearest Neighbour, which are classical machine learning methods. It has been demonstrated using different datasets that deep learning-based spam detection methods using Long Short Term Memory and Convolutional Neural Network algorithms further increase the performance rates. Besides, open problems found in spam detection systems and the stage of these studies in Turkish are also examined in this study and various suggestions have been made.

* Sorumlu yazar / Correspondence
Ersin Enes ERYILMAZ
✉ enes.eryilmaz@bil.omu.edu.tr

Please cite this article in press as E. E. Eryılmaz, E. Kılıç , "İstenmeyen E-postaların Tespiti için Kullanılan Yöntemlerin İncelenmesi", DUJE, vol. 11, no. 3, pp. 977-987, September 2020.

Giriş

Elektronik posta (e-posta ya da e-mail), internet üzerinden gönderilen dijital mektuptur. Ucuzluğu ve kolaylığı nedeniyle tercih edilen e-mail ile her gün dünyada milyarlarca e-posta gönderilmektedir.

Spam e-mail ise istenmeyen, önemsiz, gereksiz e-posta anlamına gelir. Genellikle, talep etmeyen çok sayıda alıcıya bir reklam veya alakasız içeriği olan bir mesajın gönderildiği anlamına gelir.

2017 yılında dünya çapında her gün yaklaşık 269 milyar, 2018'de 281 milyar, 2019 yılında 293 milyar e-posta gönderilmiş ve alınmıştır. Bu sayının 2023 yılında günlük 347 milyardan fazla e-postaya çıkacağı tahmin edilmektedir. Akıllı telefonlarla birlikte her ne kadar yeni tür mesajlaşma uygulamaları ortaya çıksa da e-posta kullanımı her geçen yıl artmakta bundan sonraki yıllarda da artmaya devam edeceği görülmektedir [1].

E-posta kullanıcısı sayısının 2017 yılında 3.7 milyar olduğu, 2020 yılında 4 milyar olacağı ve 2023 yılında 4.3 milyar olacağı öngörülmektedir [2]. Tüm e-postaların sayısının günlük 14.5 milyar olduğu ve en yaygın spam türünün reklamcılıkla ilgili (%36.5) olduğu bilinmektedir. İkinci en yaygın spam türü, tüm istenmeyen e-postaların %31,7'sini oluşturan yetişkinlerle ilgili içeriktir. Mali konularla ilgili mesajlar üçüncü sırada yer alır ve tüm spam e-postalarının yaklaşık %26.5'ini oluşturur. Gönderilen her 12.5 milyon spam e-posta için yalnızca bir kişi yanıt verse de spam göndericiler günde yaklaşık 7.000$ kazanmaktadır. Böylelikle spam, işletmelere her yıl 20.5 milyar dolarlık bir maliyet getirdiği değerlendirilmiştir [3].

2012 yılında toplam e-postaların %69'u istenmeyen e-posta olurken bu oran 2018'de toplam e-postaların %55'ine denk gelmektedir. Her ne kadar istenmeyen e-posta oranı düşmüş olsa da tüm e-postaların yarısından fazlasının hala istenmeyen e-posta olduğu tespit edilmiştir [4]. Bu durum istenmeyen elektronik postaların tespiti ve sınıflandırma işlemlerinin yapılmasında yıllara göre başarılı sonuçlar alınmasına rağmen aynı şekilde çalışmalara devam edilmesi gerektiğini göstermektedir.

Mevcut spam tespit yöntemleri çoğunlukla spam göndericilerin sürekli olarak getirdiği yenilikçiliğin gerisinde kalmakta, bundan dolayı da spam tespit yöntemleri de güncel yeni teknikler kullanılarak sürekli olarak geliştirilmektedir.

Bu nedenle, bu gelişmelerin zaman içinde nasıl ilerlediği ve değiştiği, bu değişimlerde ne tür yöntemler ve veriler kullandığı, başarımlarının nasıl değiştiği, bu yöntemlerin temel problemlerinin neler olduğu ve Türkçe özelinde bu çalışmaların hangi aşamada olduğu bu çalışmanın temel motivasyonu olmuştur.

Gözden geçirme çalışmasının bundan sonraki kısımlarında kronolojik olarak bu yöntemlerden bahsedilmiş, çözümler eleştirisel olarak değerlendirilmiş ve daha fazla iyileştirmenin nasıl yapılabileceğine dair öneriler verilmiştir.

Spam Tespit Sistemleri

Spam tespit sistemleri yapay zekâ tabanlı olan ve olmayan şeklinde iki ana grupta incelenebilir.

Yapay zekâ tabanlı olmayan spam tespit sistemleri

Bu sistemlerin çoğu bağımsız yazılım programları veya çevrimiçi tabanlı çözümler gibi farklı platformlarda kullanılabilen yaygın istenmeyen e-posta önleme çerçeveleridir. Bunlar, sunucu yetkilendirme sistemleri, işbirlikçi yöntemler, sezgisel filtreleme ve içeriğe dayalı yaklaşımlar olarak sıralanabilir [5].

Sunucu yetkilendirme - kimlik doğrulama sistemleri

SPF (Gönderen politikası çerçevesi), DKIM (Alan adı anahtarlarıyla tanımlanmış e-posta) ve DMARC (Alan adı esaslı ileti kimlik doğrulaması, raporlama ve uyumluluk), posta sunucusunun kimliğini doğrulamanın ve ISS'lere, posta hizmetlerine ve gönderenlerin e-posta gönderme konusunda gerçekten yetkili olduğu diğer alıcı posta sunucularına kanıtlamanın yoludur [6].

SPF ve DKIM daha geniş bir şekilde benimsenirken, DMARC potansiyel kimlik avı e-postalarını yakalamak için ciddi bir yol olsa da, yaygın olarak benimsenen bir politika değildir. Açık anahtar şifrelemesine dayanan kriptografisi

yavaş olduğundan hızlandıracak şifreleme yöntemlerinin bulunmasına ihtiyaç vardır.

İşbirlikçi modeller

Ortak çalışmaya dayalı spam filtreleme modelleme stratejilerinde bir mesaj başka bir kullanıcı tarafından alınır ve değerlendirilir. İşbirliğine dayalı modeller, bu kararların erken yakalanması, kaydedilmesi ve sorgulanması sürecini sergiler. Kriptografik hash, bulanık hash, dağıtılmış checksum clearinghouse (DCC), gri liste, DNS kara liste-beyaz liste ve sosyal güven temelli çözümler de işbirlikçi modeller arasındadır [5].

İmza tabanlı teknikler, bilinen her spam ileti için benzersiz bir özet imza değeri oluşturur. İmza oluşturma teknikleri, yasal bir e-posta iletisinin, spam iletisiyle aynı karma değere sahip olmasını istatistiksel olarak imkânsız hale getirir [7]. Message Digest 5 (MD5) kriptografik hash için yaygın seçeneklerden biri olsa da spam göndericiler, karma algoritmaları kırabilecek araçlar geliştirmede başarılıdırlar. Bu yüzden SHA-3 gibi güncel hash algoritmalarının kullanımı yaygınlaşmalıdır.

DCC fikri, e-posta alıcılarının aldıkları postaları karşılaştırabilmeleri durumunda, istenmeyen toplu postaları tanıyabilmek için ortaya atılmıştır. DCC bir iletinin spam olup olmadığına karar vermez. Sadece bir iletinin kaç kopyasının alındığını bildirir [8].

Gri liste yaklaşımı ise tanınmayan bir göndericiden gelen herhangi bir e-postayı geçici olarak reddeden bir spam önleme yöntemidir. Bu yöntemde açık problem ise, spam e-posta yeniden gönderilerek bu yaklaşım etkisiz kılınabilir [9].

DNS (Alan Adı Sunucusu) kara listesi merkezi bir veri tabanında spam oluşturucu olarak tanımlanan posta sunucusu IP'lerinin tutar. Spam, genellikle alan adları veya web sitelerine göre kara listeler oluşturularak tespit edilir [10]. Kara Listelerle ilgili sorunlar spam göndericilerin kaynak adresini sık sık değiştirmeleri ve kara liste güncelleme problemidir [11].

Beyaz liste, yalnızca onaylanmış yasal yöneticiler tarafından yönetilen posta sunucularının bir listesini tutma veya iyi niyetli kullanıcılardan gelen içeriği kabul etme uygulamasıdır. Farklı organizasyonlar, kullanıcıları daha kolay tanıyabilmek için kendi beyaz listelerine sahiptir [5]. Beyaz listeden olan bir sunucu spam gönderici durumuna dönüşebilir. Spam kaynaklarını listesini tutan Spamhaus projesi bu probleme çözüm olmaya çalışmaktadır.

Güvene duyarlı bir işbirliğine dayalı spam azaltma sisteminde e-posta sınıflandırma işlevselliği olmayan düğümlerin, bir ana bilgisayarın spam göndericisi olup olmadığını sorgulamasını sağlar [12]. Önerilen çerçeve tam olarak spam gönderen botları tanımlayamaz. Burada güven oluşturan ara sunucu sayısı artırılabilir.

İşbirlikçi modeller spam tespitinde etkili sonuçlar vermesine rağmen kriptografik özet ve bulanık özet fonksiyonlarının zayıf noktaları olabileceği, kara liste - beyaz liste veri tabanları güncelleme sorunu, güven belirleyen sunucuların bir şekilde pasifize olması ihtimali bu modellerin başarımlarına olan güveni sarsabilmektedir. Yukarıdaki problemi çözmek için literatürde kural tabanlı sezgisel filtreleme yaklaşımları ile düzenli ifade oluşturulması önerilmektedir.

Sezgisel filtreleme modelleri

Kural tabanlı olan statik spam e-posta filtrelemede düzenli ifade (regex) tabanlı filtre sistemleri sezgisel filtreleme modelleri olarak bilinirler. Bu yapıdaki kurallar çoğunlukla düzenli ifadeler kullanılarak geliştirilirler. Eşleşen kuralların her biri için puanlar hesaplanır. Hesap sonucunda elde edilen toplam değerin, önceden belirlenmiş bir eşik değerin üstünde olup olmadığı kontrol edilir ve ilgili e-postanın gerçekten spam olup olmadığına karar verilir [13].

Sezgisel sistemler hızlı ve kolaydır, ancak dolandırıcıların kural setini ele geçirmeleri durumunda, filtreleme sisteminden kaçınmak için kolayca mesaj oluşturabilirler. Burada kural setinin şifrelenmesinin çözüm olabileceği düşünülmektedir.

Bu yöntemlerin yanında istenmeyen e-posta yakalamada daha etkili olan içeriğe bağlı yaklaşımlar da kullanılmaktadır.

İçeriğe dayalı yaklaşımlar

Bu sistemler öncelikle e-postanın gövdesinin veya içeriğinin incelenmesine dayanır. İçeriğe dayalı istenmeyen e-posta tespiti

yaklaşımlarında, üstbilgi veya alan adı bilgileri yerine e-postanın içeriğine en fazla önem verilir. Bunlar; içerik filtreleme sistemleri, bağlama duyarlı öneriler ve bulanık mantık tabanlı sistemlerdir.

Bu sistemlerde, ana bilgisayar mesajında bulunan metinlerindeki kalıpları bulmak için kapsamlı bir analiz yapılır, bunlar önceden tanımlanmış ve onaylanmış spam kalıplarıyla eşleştirilir ve bir puan kaydedilir. Puanlar eşik değeri ile karşılaştırıldıktan sonra spam veya spam değil kararı verilir [13]. Son derece etkili olmasına rağmen, sistem içerikte yazanları anlayamamaktadır. Yani gerçek amaçlanan mesaj ve tartışmanın arka planı dikkate alınmayabilir. Örneğin "virüs" kelimesi hakkında tartışma ve eğitsel mesajlar bulunan e-postanın spam olarak tanımlanması istenmeyen durumdur. İçeriğe dayalı filtreleme yaklaşımında bulunan bağlamsal sorunları ele almak için bağlam duyarlı çalışmalar yapılmıştır. Laorden vd., sözdizimsel ve iletilerdeki terimlerin temel anlamlarını açıklayabilmek için Word Sense Disambiguation (WSD) adında bir ön işleme adımı ekleyerek spam filtrelemede anlambilimin kullanımını araştırmıştır [14]. Uzun mesajlarda performans iyileştirilmesine ihtiyaç duymaktadır. Bunun için bulanık mantık tabanlı öneriler getirilmekte olup bu yünde çalışmalar artırılmalıdır.

Yapay zekâ tabanlı olmayan diğer yaklaşımlar
Ülke tabanlı filtreleme, eşler arası altyapı diğer spam tespiti yaklaşımlarıdır. Bazı e-posta sunucuları çoğu zaman belirli ülkelerden gelen e-posta akışlarını tamamen engeller, çünkü belirli coğrafi sınırlar genellikle büyük bir spam kaynağıdır [15]. Dünya genelinde spam hacminin payı ile 2019'un 3. çeyreğinde istenmeyen e-postalar için önde gelen kaynak ülkelerin oranı Statista'ya göre 2019 yılında spam oluşturma oranlarında ilk üç sırayı alan ülkeler Çin, ABD ve Rusya olup sırasıyla %20.43, %13,37 ve %5,60 oranlarında spam oluşturmuşlardır. Türkiye %2,42 ile 8. en çok spam oluşturulan ülkelerdendir [16].

Literatürde Bitcoin işlemlerinde kullanılan benzer iş kanıtı kavramına dayanan 'Bitmessaging' olarak bilinen farklı yaklaşımlarda vardır. Bu yöntemler BitMessage eşler arası iletişim protokolüne dayanır ve tamamen merkezi olmayan ve şifreli bir ağ kullanırlar. Bu tür yaklaşımı kullanan yöntemler, mevcut e-posta altyapısıyla henüz tam olarak uyumlu olmadığından, bazı ölçeklenebilirlik sorunları vardır [17]. Bu yüzden bu yöntem için farklı algoritmalar ve teknikler geliştirilmeye ihtiyaç vardır.

Şimdiye kadar açıklanan yapay zekâ tabanlı olmayan istenmeyen elektronik posta tespit sistemleri bağımsız yazılım programları olarak veya çevrimiçi tabanlı çözümler gibi farklı platformlarda kullanılabilen yaygın istenmeyen e-posta önleme çerçeveleridir. Bu çözümlerin yapay zekâ tabanlı sistemlerle birlikte kullanımı ile toplam gönderilen ve alınan istenmeyen e-posta sayısında önemli bir düşüş yaşanmıştır.

Yapay zekâ tabanlı olmayan sistemler bazı sunucularda tek başına çalıştığı, büyük sunucularda ise hem yapay zekâ tabanlı olmayan hem de yapay zekâ tabanlı olan sistemlerin birlikte çalıştığı bilinmektedir. Örneğin en büyük e-posta sunucularına sahip Google ve Microsoft SPF, DKIM, DMARC gibi yapay zekâ tabanlı olmayan sistemlerle makine öğrenmesi yöntemlerini birlikte kullanmaktadır. Fakat küçük çaplı sunucularda beyaz liste, kara liste, gri liste, içerik filtreleme yaklaşımları kullanılmaktadır. Bu sistemlerin birlikte kullanılması yani melez yapıların kullanımı daha iyi sonuçlar elde edilmesini sağlayabilecektir. Yapay zekâ tabanlı olmayan sistemler tek başına istenmeyen e-postalara engel olamadığından yapay zekâ tabanlı sistemler üzerinde çalışmalar günümüzde yaygın hale gelmiştir.

Yapay zekâ tabanlı spam tespit sistemleri

İstenmeyen e-postaların tespitinde kullanılan klasik yöntemlerin büyük veriyi işlemedeki başarı oranlarının tıkanması sonucu yapay zekâ tabanlı yeni bir istenmeyen e-posta tespit alanı doğmuştur. Literatürde bu tür sistemler biyolojik ilhamlı zekâya dayalı, makine öğrenmesi temelli ve makine öğrenmesinin bir çeşidi olan derin öğrenme temelli sistemler olarak karşımıza çıkmaktadır.

Biyolojik zekâya dayalı sistemler
Genetik algoritma (GA), NSA ve PSO tabanlı sistemler biyolojik ilhamlı zekâya dayalı sistemlerdir.

Spam için genetik algoritma ile düzenli ifade (regex) filtreleri geliştiren ve spam ve spam olmayanlar arasında ayrım yapan bazı testleri %94'ün üzerinde doğrulukla bulmasına rağmen bu tür yöntemler Fitness fonksiyonu her çalıştırıldığında, her mesajı incelemek zorunda kaldıkları için oldukça yavaştır [18]. Negatif Seçim Algoritması (NSA) ile Gerçek Pozitif ve Gerçek Negatif tespit oranının % 6 oranında artıran, %98.5 doğrulukla spam tespiti yapan bir yöntemler de vardır [19]. Ancak bu yöntemde veri sözlüğündeki kelimeler GA ile belirtilmeyen bir performans metriği ile test edilmiş olup yöntemin performansı genellikle standart diğer çalışmalarla karşılaştırılmamıştır [20, 21].

Bu çalışmalardaki temel problemler kullanılan veri kümelerinin çok küçük olması olup büyük veri temelli derin öğrenme kullanan yöntemler ile karşılaştırmak olası değildir. Ayrıca makine öğrenmesi algoritmalarına kıyasla biyolojik temelli yapay zekâya dayalı algoritmalarında spam tespitinde kullanılmasının performans açısından çok fazla kazanç sağlamadığı aksine düşük performans gösterdikleri görülmektedir.

Makine öğrenmesi temelli sistemler

Yapay sinir ağları (ANN), naïve bayes, bayes karar ağacı, rastgele orman, lojistik regresyon, destek vektör makinesi (DVM), adaboost, k-en yakın komşu (kNN) istenmeyen e-posta tespitinde en çok kullanılan makine öğrenmesi algoritmalarıdır. K-ortalama kümeleme, kendini düzenleyen harita tabanlı öneriler (SOM), temel bileşen analizi (PCA) tabanlı çerçeveler, birliktelik tabanlı öneriler de az da olsa kullanılmaktadır. Makine öğrenmesi tekniği kullanan çok sayıda spam tespit yöntemi, bunların kullandığı veriler ve spam tespit algoritmalarının performansları Tablo 1'de verilmiştir.

Tablo 1. Makine öğrenmesi tabanlı istenmeyen e-posta tespit sistemleri

Çalışmanın Adı	Kullanılan Veri kümesi	Kullanılan Yöntem /Başarısı En Yüksek Yöntem	Kullanılan Performans Metrikleri ve En Yüksek Değerleri (%)	Yöntemin Türü (Bilinen/ Yeni/ Melez)
Zhao ve Zhang. 2005 [22]	1518 adet e-posta içeren TE 943	Kaba Küme (RS), Naïve Bayes (NB) / RS	Doğruluk: 97.37 Hassasiyet: 86.58 Hatırlama: 96.99	Yeni
Altunyaprak. 2006 [23]	767'si spam olan 2387 adet Türkçe e-posta	Bayes	Hassasiyet: 84 Hatırlama: 93.2	Yeni
Norte Sosa. 2010 [24]	2200 e-posta	YSA	Doğruluk: 96.1	Yeni
Yumak. 2011 [25]	100 adet e-posta	Bulanık Mantık (BM), NB, / NB	Doğruluk: 81.8	Bilinen
Awad ve ELseuofi. 2011 [26]	SpamAssassin	Bayes, kNN, YSA, DVM, Yapay Bağışıklık Sistemi (AIS) ve RS / NB	Doğruluk: 99.46 Hassasiyet: 99.66 Hatırlama: 98.46	Bilinen
İdris ve Muhammed. 2012 [27]	Spambase	AIS	FP: 1.2	Bilinen
Bhagyashri ve Pratap. 2013. [28].	SpamAssassin	Bayes	Doğruluk: 90 Hassasiyet: 82.35 Hatırlama: 93.33	Bilinen
Ateş. 2014. [29]	Ergin vd. [30] tarafından oluşturulan 800 Türkçe e-posta veri kümesi ve İngilizce Lingspam_public veri kümesi	DVM, Gauss Karışım Modeli (GKM), NB. / Türkçe veri kümesinde NB, / İngilizce veri kümesinde doğrusal DVM	Doğruluk: 99 Doğruluk: 98.6	Bilinen
Sharma vd. 2014. [31]	TREC07	MLP, NB / MLP	Doğruluk: 93 Hatırlama: 93.2	Bilinen

			Hassasiyet: 93	
Karthika ve Visalakshi. 2015. [32]	Spambase	kNN, NB, DVM ve Hibrid ACO-DVM / ACO-DVM	Doğruluk: 81.25 Hassasiyet:87.02 Hatırlama: 75.1	Yeni ve Melez
Renuka vd. 2015. [33]	Spambase	GA-Naïve Bayes, ACO-Naïve Bayes / ACO-Naïve Bayes	Doğruluk: 84 Hassasiyet: 89 Hatırlama: 78 F-ölçütü: 87	Yeni ve Melez
Tuteja ve Bogiri, 2016. [34]	100 spam olmak üzere 200 adet e-posta	K-ortalamalı Geri yayılımlı Sinir Ağı (BPNN)	Hassasiyet: 98.42 Hatırlama: 93.5	Melez
Palanisamy vd. 2016. [35]	Lingspam	Negatif Seçim Algoritması (NSA) kullanan PSO, DVM, NB, DFS-DVM / Negatif Seçim Algoritması (NSA) kullanan PSO	Doğruluk: 93.2	Melez
Zavvar vd. 2016. [36]	Spambase	PSO, SOM, k-ortalama, DVM / DVM	AUC: 93.07	Bilinen
Foqaha. 2016. [37].	Spambase	RBF, MLP ve YSA ve melez HC-RBFPSO / MLP	Doğruluk: 93.28	Melez
Sharma ve Suryawanshi. 2016. [38].	Spambase	Bayes, KNN, DVM / KNN	Doğruluk: 97.54 Hassasiyet: 97.72 Hatırlama: 93.52 F-ölçütü: 95.6	Bilinen
Alkaht ve Al Khatib. 2016. [39].	CSDMC 2010, SpamAssassin, Tarassul	Kendi kendini organize eden Küresel Sıralama Haritası ve İleri besleme algoritmalarının birleşimi ile Several Stage Neural Network (SNN)	Doğruluk: 95.40 Hassasiyet: 99.45 Hatırlama: 91.28 F-ölçütü: 95.19	Yeni
Rajamohana vd. 2017 [40].	Ott vd.[41] tarafından oluşturulan veri kümesi	Naïve Bayes Uyarlanabilir İkili Çiçek tozlaşma algoritması (ABFPA)	Doğruluk: 91.42	Yeni
Akinyelu ve Adevumi. 2017 [42].	2000 kimlik avı ve normal e-posta	Rastgele Orman (RF)	Doğruluk: 99.7 Hassasiyet: 99.47 Hatırlama: 97.5 F-ölçütü: 98.45	Bilinen
Yıldız. 2017. [43].	310 adet Türkçe e-posta	NB, DVM, YSA, Adaboost, J48, JRIP / Çok Terimli NB	Doğruluk: 96.31 Hassasiyet: 91 Hatırlama: 100 Kappa: 94	Bilinen
Şahin. 2018. [44].	55888 e-posta	12 klasik makine öğrenmesi algoritması / Naïve Bayes Kernel ve Doğrusal SVM	Doğruluk: 99.89 F-ölçütü: 99.81	Bilinen
Kale. 2018. [45].	Louis Dorard'ın 2013 yılında kendine ait 4.709 adet e-posta	Karar Ağaçları, Derin öğrenme, Gradient Boosted Tree (GBT), kNN, NB, RF ve Lojistik Regresyon / Çok terimli NB	Doğruluk: 95.5 Hassasiyet: 100 Hatırlama: 91 F-ölçütü: 95.8	Bilinen
Nazlı. 2018. [46].	Enron (300 e-posta)	DVM (Poly)	Doğruluk: 98.33	Bilinen
Al-Azzawi. 2018. [47].	Spambase	Kaotik ateş böceği algoritmasına dayanan sarmal öznitelik seçimli NB	Doğruluk: 95.14	Yeni
Salihi. 2019. [48].	355 spam gönderici olan 1183 Twitter'dan elde edilen veri kümesi	NB, J48, IBK, RF / RF	Doğruluk: 92.95 Hassasiyet: 92 Hatırlama: 88 F-ölçütü: 89	Yeni

Tablo 1 incelendiğinde veri kümesinin az olduğu spam tespit çalışmalarında başarım oranlarının yüksek çıktığı [23, 29, 34,43-46], Spambase açık veri kümesi üzerinde makine öğrenmesi tekniklerinin yoğunlaştığı [27, 32, 33, 36-38, 40, 47], doğruluk, hassasiyet, hatırlama performans metriklerinin yanında, F-ölçütünün de kullanıldığı görülmüştür [33, 38, 39, 44, 45, 48].

MLP, YSA'ya dayanan spam tespit algoritmalarında [26, 31, 37, 39] model eğitimlerinin zaman aldığı, Bayes, Naïve Bayes, DVM, YSA ve melez yaklaşımların başarım oranlarının ise yüksek olduğu tespit edilmiştir [22-26, 28, 29, 33, 35, 36, 43-47].

%99 civarı başarım oranı veren çalışmalarda veri kümelerinde bulunan e-posta sayılarının az olduğu görülmektedir [26, 29, 42]. N-gram ve Kelime Kümesi tekniği ile 50 özellik seçiminde veri kümesi fazla olsa da başarım oranının yüksek çıktığı görülmüştür [44]. SpamAssassin veri kümesini kullanan [26] nolu çalışmada 100 özellik üzerinden NB algoritması değerlendirme yapıldığında %99.46 başarım elde edilmiştir.

Görece daha küçük veriler üzerinde çalışan sistemlerde daha iyi çalışan DVM, Bayes, RF, MLP, YSA gibi makine öğrenmesi yöntemleri kullanmalıdır. Melez olarak farklı algoritma, öznitelik ve özellik seçimlerinin bir arada kullanıldığı makine öğrenmesi çalışmalarında genel olarak başarımın artacağı görülmektedir. Makine öğrenmesinin her aşamasında (öznitelik, özellik seçimi, doğal dil işleme, eğitim vb.) en iyi sonuçları veren yöntemlerin bir arada kullanılması daha başarılı sonuçlar üretecektir.

Yukarıdaki çalışmalardan daha anlamlı sonuçlar çıkarmak için daha büyük e-posta veri kümelerine ihtiyaç duyulmaktadır. Ayrıca farklı performans ölçütlerinin spam algoritma performanslarını değerlendirirken bir arada kullanılmasının gerekli olduğu düşünülmektedir. Büyük veri ve son yıllarda merkezi işlemci biriminin (CPU) yanında grafik işlemci birimlerinin (GPU) hesaplama güçlerinin artmasıyla birlikte derin öğrenme tekniklerinin kullanımı daha yüksek başarım sonuçlar vermektedir.

Derin öğrenme temelli sistemler

Derin öğrenmede öznitelik ve özellik seçimini bir yöntem belirlemeden gizli sinir ağlarında yapılmaktadır. Normal ve istenmeyen etiketli veri kümesinde bulunan veriler veri vektörlerine dönüştürülerek, elde edilen bu veri kümesi eğitim ve test bölümlerine ayrılır. Kullanılacak derin öğrenme katmanları ile model eğitilir. Eğitimden sonra, sistemin performansı test kümesi adı verilen farklı bir dizi örnek üzerinde ölçülür. Derin öğrenme klasik yapay öğrenme yani makine öğrenmesi algoritmalarının yetersiz kaldığı bazı durumlarda insan performansına yakın çıktıların elde edilmesini sağlayabilmektedir. Geleneksel makine öğrenme teknikleri, doğal verileri ham formlarında işleme yetenekleriyle sınırlıdır. Derin öğrenmenin en önemli özelliği, özellik katmanlarının insanlar tarafından tasarlanmamasıdır.

Derin öğrenme, çoklu soyutlama seviyelerine sahip verilerin gösterimini öğrenmek için çoklu işleme katmanlarından oluşan hesaplama modellerine izin verir. Tipik bir derin öğrenme sisteminde, makineyi eğitmek için yüz milyonlarca ayarlanabilir ağırlık ve yüz milyonlarca etiketli örnek olabilir.

Literatürde derin öğrenme ile istenmeyen e-posta tespiti üzerine çalışmalar da görülmektedir. Bu, çalışmalarda kullanılan veri kümeleri, en başarılı yöntemler, kullanılan performans metrikleri, yöntemin türü, tespit algoritmalarının performansları, Tablo 2'de verilmiştir.

Tablo 2. Derin öğrenme tabanlı istenmeyen e-posta tespit çalışmaları

Çalışmanın Adı	Kullanılan Veri kümesi	Kullanılan Yöntem /Başarısı En Yüksek Yöntem	Kullanılan Performans Metrikleri ve En Yüksek Değerleri (%)	Yöntemin Türü (Bilinen /Yeni/ Melez)
Tyagi. 2016 [49]	PU1, PU2, PU3, PUA ve Enron-Spam	Yoğun MLP, Stacked Denoising Autoencoder, (SDAE), Derin İnanç Ağı (DBN) / DVM, SDAE	Doğruluk: 96.21 Hassasiyet: 96.78 Hatırlama: 95.57 F-ölçütü: 96.17	Bilinen

Shang ve Zhang. 2016 [50]	52934 görüntü içeren yeni bir spam veri kümesi	Tahmin Katmanında DVM kullanan CNN	Doğruluk: 82	Yeni ve Melez
Roy vd. 2016 [51]	Spambase	Derin DVM, YSA, DVM / Derin DVM	Doğruluk: 92.8 Hassasiyet: 91.4 Hatırlama: 89.9 F-ölçütü: 90.7 AUC: 97.3	Yeni
Seth ve Biswas. 2017 [52]	Toplanan 1521'den fazla spam resim ve Enron metin veri kümesi	Görüntü CNN, Metin CNN, Çoklu Öğrenme Modeli / Çoklu Öğrenme Modeli	Doğruluk: 98.11 F-ölçütü: 98	Yeni ve Melez
Yawen vd. 2018 [53]	Spambase	Derin Sinir Ağları (DNN), Naïve Bayes / DNN	Doğruluk: ~90	Bilinen
Ra vd. 2018 [54]	IWSPA-AP 2018	CNN, RNN, LSTM, MLP / Kelime Yerleştirme (Word Embedding) + LSTM	Doğruluk 99.1	Melez
Bagui vd. 2019 [55]	3416'sı kimlik avı e-postası olan 18366 etiketli e-posta veri kümesi	Naïve Bayes, DVM, Karar Ağacı, LSTM, CNN ve Kelime Yerleştirme / Kelime Yerleştirme	Doğruluk: 98.89	Bilinen
Yang vd. 2019 [56]	Enron, Personal Image, Spam Archive	LSTM ve CNN	Doğruluk: 98.48 Hatırlama: 98.52 Hassasiyet: 98.52 F-ölçütü: 98.45	Yeni ve Melez
Jain vd. 2019 [57]	SMS Spam ve Twitter spam veri kümesi	DVM, Naïve Bayes, ANN, k-NN, RF, LSTM / LSTM	Doğruluk: 99.01 Hatırlama: 99.35 Hassasiyet: 98.74 F-ölçütü: 99.24	Yeni
Nagisetty ve Gupta. 2019 [58]	UNSW-NB15 ve NSL-KDD99	MLP, CNN, DNN, Otomatik Kodlayıcı / DNN ve MLP	Doğruluk(DNN): 99.24 F-ölçütü(MLP): 99.28 RMSE(DNN): 0.4	Bilinen
Roy vd. 2020 [59]	747 spam ve 4.827 normal SMS veri kümesi	NB, RF, GB, LR, LSTM, SGD / CNN	Doğruluk: 99.44 Hatırlama: 99.8 Hassasiyet: 99.6 F-ölçütü: 99.8 AUC: 97.7	Bilinen

Tablo 2 dikkatli bir şekilde incelendiğinde, Spam tespiti için derin öğrenme ile açık veri kümelerinde test yapılmasının yanı sıra, araştırmacılarının kendisinin bir araya getirdiği veri kümeleri de [50, 52, 55, 59] de kullanılmıştır.

Önerilen yöntemlerde genel olarak LSTM ve CNN algoritmaları [50, 52, 54, 56-59], performans metriği olarak da genellikle Doğruluk, Hatırlama, Hassasiyet ve F-ölçütü metrikleri [49, 51, 56, 57, 59] kullanılmakla birlikte AUC [51, 59], RMSE [58] ölçütlerinin de çeşitli çalışmalarda kullanıldığı görülmektedir. Sadece metin içeren veri kümeleri [49, 51, 54, 53, 57], olduğu gibi spam resim içeren veri kümeleri [50, 52, 56] ile de çalışılmıştır. Genel olarak metin içeren veri kümelerinde LSTM algoritması [54, 57] ile daha yüksek başarım elde edilirken resim içeren veri kümelerinde CNN algoritmasının başarımı [50, 52] daha yüksektir. Dengesiz veri kümesi kullanılan bir çalışmada CNN, LSTM'den daha iyi başarım sonucu vermektedir [59]. Ayrıca melez spam tespit yöntem yaklaşımlarının tespit algoritmalarının başarımını artırdığı görülmektedir [54, 56]. %99 civarı başarım oranı veren çalışmalarda [54-59] LSTM, CNN, Kelime Yerleştirme, DNN ve MLP teknikleri kullanılmıştır.

Metin içeren veri kümelerinde LSTM, görüntü içeren veri kümelerinde CNN algoritmasının için daha etkili olduğu, melez yaklaşımların yüksek başarımlara ulaşabildiği, bazı veri kümelerinde DNN ve MLP algoritmalarının daha iyi sonuçlar verdiği belirlenmiştir.

Klasik makine öğrenme algoritmaları ile derin öğrenme algoritmalarının başarımını karşılaştıran çalışmalar dikkate alındığında, derin öğrenme algoritmalarının daha yüksek başarım oranı ile spam tespit ettiği anlaşılmaktadır [51, 53, 57-59].

Derin öğrenme temelli sistemlerle, makine öğrenmesindeki çalışmalar öznitelik mühendisliğinden ziyade model ve mimari mühendisliğine evrilmiştir. Elimizde çok küçük veri kümesi varsa problem derin öğrenme ile çözümü çok uygun olmamaktadır. Derin öğrenme modelinde bulunan hiper parametrelerin kendini en iyi sonucu verecek şekilde çalışılan modele güncelleyebilecek yapılar oluşturulması düşünülebilir.

Sonuçlar

Literatürde zamanla geliştirilen spam algılama sistemlerinin açık problemleri tespit edilmiş bunlarla ilgili çözüm önerileri getirilmiştir.

İstenmeyen e-posta tespitinde zamanla başarılı yöntemlerin sayısı artmış ancak bunların çoğu, spam gönderenlerin sürekli olarak spam oluşturma şeklini değiştirmesiyle etkinliğini yitirmiştir. Bu durum sürekli gelişen spam tespit yöntemlerinin ortaya çıkmasını sağlamıştır. Önceleri yapay zekâ tabanlı olmayan yöntemler etkili iken günümüzde makine öğrenmesi ve derin öğrenme algoritmalarının artması ve iyileştirilmesi ile istenmeyen e-posta tespitinde yapay zekâ tabanlı sistemler daha çok kullanılır hale gelmiştir.

Literatürde yapay zekâ tabanlı olan sistemler ile birlikte yapay zekâ tabanlı olmayan spam tespit sistemleri birlikte kullanılmaktadır. İşlemci gücünün ile birlikte grafik işlem birimlerinin kapasitelerinin artmasıyla makine öğrenmesi tekniklerinin yanında derin öğrenme yöntemleri de istenmeyen elektronik posta tespitinde daha fazla tercih edilmeye başlanmıştır.

Mevcut hesaplama ve veri miktarındaki artışları kolayca tolere edebilen derin öğrenmeye dayalı yöntemlerin gelecekte spam e-posta tespitinde daha da başarılı olacağı düşünülmektedir. Derin sinir ağlarının şuanda geliştirilmekte olan yeni öğrenme algoritmaları ve mimariler ile birlikte bu ilerlemeyi daha da hızlandıracağı kolayca tahmin edilebilmektedir.

Derin öğrenme uygulamalarında veri kümesinin büyüklüğü ve çeşitliliği öğrenme için en önemli etmendir. Veri kümemiz ne kadar büyük olursa öğrenme o oranda iyi olacaktır Büyük veri olan sistemlerde derin öğrenme yöntemlerinin kullanılması önerilmektedir.

Birçok kullanıcı cihazdaki tüm e-postalarına erişmeyi tercih etmekte olup kullanıcı davranışı göz önünde bulundurularak kullanıcıya özel olarak tasarlanmış bir spam filtresi düşünülmesi de gerekmektedir.

Bu alanda çalışmak isteyen araştırmacılar için mevcut problemlerden en önemlisi, Türkçe e-postaları içeren veri kümelerinin az veri içermesi ve yetersiz sayıda olmasıdır. Türkçe spam içeren veri kümelerinin oluşturulması birçok araştırmacıya çalışmalarında kolaylık sağlayacaktır.

Akıllı telefonların piyasaya girmesiyle ortaya çıkan mesajlaşma uygulamaları her ne kadar fazla olsa da e-postaların kullanımına uzunca bir süre daha devam edileceği aşikârdır. E-postaların kolay, ucuz, internete bağlı her cihazdan erişilebilir olması reklam amaçlı veya kötü niyetli internet kullanıcıları için kaynak olmaya devam edecektir. İstenmeyen e-postaların ayrıştırılması için makine öğrenmesi ve derin öğrenme temelli yeni yöntemler geliştirilmelidir.

Kaynaklar

[1] Campaignmonitor. 2019. The Shocking Truth about How Many Emails Are Sent. https://www.campaignmonitor.com/blog/email-marketing/2019/05/shocking-truth-about-how-many-emails-sent/ (Erişim Tarihi: 22.02.2020).

[2] Statista. 2020. Number of e-mail users worldwide from 2017 to 2023. https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/ (Erişim Tarihi: 22.02.2020).

[3] Bauer, E. 2018. 15 Outrageous Email Spam Statistics that Still Ring True in 2018. https://www.propellercrm.com/blog/email-spam-statistics. (Erişim Tarihi: 22.02.2020).

[4] Statista. 2019. Global e-mail spam rate from 2012 to 2018.

https://www.statista.com/statistics/270899/global-e-mail-spam-rate/ (Erişim Tarihi: 28.02.2020).

[5] Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., & Alazab, M. 2019. A Comprehensive Survey for Intelligent Spam Email Detection. IEEE Access, Access, IEEE, 7, 168261–168295. https://doi.org/10.1109/ACCESS.2019.2954791

[6] Ruef, M., & Young, E. 2019. Securing Email of your own Domain - SPF, DKIM and DMARC. https://doi.org/10.6084/m9.figshare.10145189

[7] Geerthik, S., & Anish, T. P. 2013. Filtering spam: Current trends and techniques. International Journal of Mechatronics, Electrical and Computer Technology Austrian E-Journals of Universal Scientific Organization, 3, 208-223.

[8] Gansterer, W., Ilger, M., Lechner, P., Neumayer, R., & Strauß, J. 2005. Anti-spam methods-state of the art. Institute of Distributed and Multimedia Systems, University of Vienna, 28, 29.

[9] Bajaj, K. S., Egbufor, F., & Pieprzyk, J. 2011. Critical analysis of spam prevention techniques. In 2011 Third International Workshop on Security and Communication Networks (IWSCN) (pp. 83-87). IEEE.

[10] Chiba, D., Akiyama, M., Yagi, T., Hato, K., Mori, T., & Goto, S. 2018. DomainChroma: Building actionable threat intelligence from malicious domain names. Computers & Security, 77, 138-161.

[11] Ramachandran, A., Feamster, N., & Vempala, S. 2007. Filtering spam with behavioral blacklisting. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 342-351).

[12] Lin, P. C., Lin, P. H., Chiou, P. R., & Liu, C. T. 2013. Detecting spamming activities by network monitoring with Bloom filters. In 2013 15th International Conference on Advanced Communications Technology (ICACT) (pp. 163-168). IEEE.

[13] Khanna, S., Chaudhry, H., & Bindra, G. S. 2012. Inbound & Outbound Email Traffic Analysis and Its SPAM Impact. In 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (pp. 181-186). IEEE.

[14] Laorden, C., Santos, I., Sanz, B., Alvarez, G., & Bringas, P. G. 2012. Word sense disambiguation for spam filtering. Electronic Commerce Research and Applications, 11(3), 290-298.

[15] Hu, Y., Guo, C., Ngai, E. W. T., Liu, M., & Chen, S. 2010. A scalable intelligent non-content-based spam-filtering framework. Expert Systems with Applications, 37(12), 8557-8565.

[16] Statista. 2019, Aralık. https://www.statista.com/statistics/263086/countries-of-origin-of-spam/. (Erişim Tarihi: 29.02.2020).

[17] Bradbury, D. 2014. Can we make email secure?. Network Security, 2014(3), 13-16.

[18] Greenstadt, R., & Kaminsky, M. 2002. Evolving Spam Filters Using Genetic Algorithms. Technical Report 3836. Massachusetts Institute of Technology.

[19] Saleh, A. J., Karim, A., Shanmugam, B., Azam, S., Kannoorpatti, K., Jonkman, M., & Boer, F. D. 2019. An intelligent spam detection model based on artificial immune system. Information, 10(6), 209.

[20] Shrivastava, J. N., & Bindu, M. H. 2013. E-mail classification using genetic algorithm with heuristic fitness function. *International Journal of Computer Trends and Technology (IJCTT)*, *4*(8), 2956-2961.

[21] Choudhary, M., & Dhaka, V. S. 2013. Automatic E-mails classification using genetic algorithm. In *Special Conference Issue: National Conference on Cloud Computing and Big Data* (pp. 42-49).

[22] Zhao, W., & Zhang, Z. 2005. An email classification model based on rough set theory. In *Proceedings of the 2005 International Conference on Active Media Technology, 2005.(AMT 2005).* (pp. 403-408). IEEE.

[23] Altunyaprak, C. 2006. Bayes yöntemi kullanarak istenmeyen elektronik postaların filtrelenmesi. Yüksek Lisans Tezi, Muğla Üniversitesi Fen Bilimleri Enstitüsü

[24] Norte Sosa, J. 2010. Spam Classification Using Machine Learning Techniques-Sinespam (Master's thesis, Universitat Politècnica de Catalunya).

[25] Yumak, B. 2011. Elektronik postaların ayrıştırılmasında Naïve bayesian ve Bulanık Mantık yöntemlerinin karşılaştırılması. Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, 97, Ankara.

[26] Awad, W. A., & ELseuofi, S. M. 2011. Machine learning methods for spam e-mail classification. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), 173-184.

[27] Idris, I., & Abdulhamid, S. M. 2014. An improved AIS based e-mail classification technique for spam detection. *arXiv preprint arXiv:1402.1242*.

[28] Bhagyashri, G., Pratap, H., & Patil, D. Y. 2013. Auto E-mails classification using bayesian filter. International Journal of Advanced technology & Engineering Research, 3(4).

[29] Ateş, N. 2014. Destek vektör makineleri ve Gauss karışım modeli ile istenmeyen e-postaların tespiti. Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, 57, Samsun.

[30] Ergin, S., Sora Gunal, E., Yigit, H., & Aydin, R. 2012. Turkish anti-spam filtering using binary and probabilistic models. Global Journal on Technology, 1.

[31] Sharma, A. K., Prajapat, S. K., & Aslam, M. 2014. A comparative study between naïve Bayes and neural network (MLP) classifier for spam email detection. *Int. J. Comput. Appl.*

[32] Karthika, R., & Visalakshi, P. 2015. A hybrid ACO based feature selection method for email spam classification. WSEAS Trans. Comput., 14, 171-177.

[33] Renuka, D. K., Visalakshi, P., & Sankar, T. 2015. Improving E-mail spam classification using ant colony optimization algorithm. Int. J. Comput. Appl, 22-26.

[34] Tuteja, S. K. and Bogiri, N. 2016. Email Spam filtering using BPNN classification algorithm. 2016 International Conference on Automatic Control and

Dynamic Optimization Techniques (ICACDOT), IEEE, 915-919.

[35] Palanisamy, C., Kumaresan, T., & Varalakshmi, S. E. (2016). Combined techniques for detecting email spam using negative selection and particle swarm optimization. Int. J. Adv. Res. Trends Eng. Technol., 3.

[36] Zavvar, M., Rezaei, M., & Garavand, S. 2016. Email spam detection using combination of particle swarm optimization and artificial neural network and support vector machine. International Journal of Modern Education and Computer Science, 8(7), 68.

[37] Foqaha, M. A. M. 2016. Email spam classification using hybrid approach of RBF neural network and particle swarm optimization. International Journal of Network Security & Its Applications, 8(4), 17-28.

[38] Sharma, A., & Suryawanshi, A. 2016. A novel method for detecting spam email using KNN classification with spearman correlation as distance measure. International Journal of Computer Applications, 136(6), 28-35.

[39] Alkaht, I. J., & Al-Khatib, B. 2016. Filtering SPAM Using Several Stages Neural Networks. Int. Rev. Comp. Softw., 11, 2.

[40] Rajamohana, S. P., Umamaheswari, K., & Abirami, B. 2017. Adaptive binary flower pollination algorithm for feature selection in review spam detection. In 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT) (pp. 1-4). IEEE.

[41] Ott Myle, Choi Yejin, Cardie Claire, T. Hancock Jeffrey, "Finding deceptive opinion spam by any stretch of imagination", ACM Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies, vol. 1, pp. 309-319, 2011.

[42] Akinyelu, A. A., & Adewumi, A. O. 2014. Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics, 2014.

[43] Yıldız, A. 2017. Kurumsal e-posta sınıflandırma sistemi. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 82, Ankara.

[44] Şahin, E. 2018. Makine öğrenme yöntemleri ve kelime kümesi tekniği ile istenmeyen e-posta / e-posta sınıflaması. Yüksek Lisans Tezi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, 60, Ankara.

[45] Kale, B. 2018. Veri madenciliği sınıflandırma algoritmaları ile e-posta önemliliğinin belirlenmesi. Yüksek Lisans Tezi, Çukuruova Üniversitesi Fen Bilimleri Enstitüsü, 120, Adana.

[46] Nazlı, N. 2018. Analysis of machine learning – based spam filtering techniques. Yüksek Lisans Tezi, Çankaya University The Graduate School of Natural and Applied Sciences, 79, Ankara.

[47] Al-Azzawi, F. 2018. Wrapper feature selection approach for spam e-mail filtering. Master Thesis, Erciyes University Graduate school of natural and applied science, Kayseri.

[48] Salihi, A. K. A. 2019. Spam detection by using word-vector learning algorithm in online social networks. Master Thesis, Fırat University Graduate school of natural and applied sciences institute, 46, Elazığ.

[49] Tyagi, A. 2016. Content Based Spam Classification-A Deep Learning Approach (Master's thesis, Graduate Studies).

[50] Shang, E.-X. and Zhang, H.-G. 2016. Image spam classification based on convolutional neural network. 2016 International Conference on Machine Learning and Cybernetics (ICMLC), IEEE, 398-403.

[51] Roy, S. S., Sinha, A., Roy, R., Barna, C. and Samui, P. 2016. Spam Email Detection Using Deep Support Vector Machine, Support Vector Machine and Artificial Neural Network. International Workshop Soft Computing Applications, Springer, 162-174.

[52] Seth, S. and Biswas, S. 2017. Multimodal Spam Classification Using Deep Learning Techniques. 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), IEEE, 346-349.

[53] Yawen, W., Fan, Y. and Yanxi, W. 2018. Research of Email Classification based on Deep Neural Network. 2018 Second International Conference of Sensor Network and Computer Engineering (ICSNCE 2018), Atlantis Press.

[54] Ra, V., HBa, B. G., Ma, A. K., KPa, S., Poornachandran, P. and Verma, A. 2018. DeepAnti-PhishNet: Applying deep neural networks for phishing email detection. Proc. 1st AntiPhishing Shared Pilot 4th ACM Int. Workshop Secur. Privacy Anal.(IWSPA), Tempe, AZ, USA, 1-11.

[55] Bagui, S., Nandi, D., Bagui, S. and White, R. J. 2019. Classifying Phishing Email Using Machine Learning and Deep Learning. 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, 1-2.

[56] Yang, H., Liu, Q., Zhou, S. and Luo, Y. 2019. A Spam Filtering Method Based on Multi-Modal Fusion. *Applied Sciences*, 9:6, 1152.

[57] Jain, G., Sharma, M. and Agarwal, B. 2019. Optimizing semantic LSTM for spam detection. *International Journal of Information Technology*, 11:2, 239-250.

[58] Nagisetty, A. and Gupta, G. P. 2019. Framework for Detection of Malicious Activities in IoT Networks using Keras Deep Learning Library. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), IEEE, 633-637.

[59] Roy, P. K., Singh, J. P. and Banerjee, S. 2020. Deep learning to filter SMS Spam. *Future Generation Computer Systems*, 102, 524-5