Kurumsal Eposta Sınıflandırma ve Değerlendirme Sistemi

A. YILDIZ, E. B. CEYHAN, Ş. SAĞIROĞLU

***Özet*—Sunulan çalışmada epostaları, içeriklerine göre anlamlandıran ve sınıflandıran bir sistem geliştirilmiştir. Çalışma kapsamında geliştirilen sistem, kurumlarda eposta hizmetlerini kullanan bütün personellere bilgi güvenliği farkındalığına yardımcı olmak için geliştirilmiştir.**

Çalışmada temel bir SMTP istemcisi geliştirilmiş ve kurumsal eposta sunucusuna bağlanarak epostalar, geliştirilen uygulama içerisine alınmıştır. Alınan epostaları analiz etmek için epostaların özgün kaynak içerikleri alınmıştır ve bu kaynak bilgilerinden başlık bilgileri ve içerik bilgileri ayrıştırılmıştır. Ayrıştırılan başlık bilgileri ve içerik bilgileri anlamlandırılmak için uygulamada görsel öğelerle ve sayısal değerlerle desteklenmiştir. Epostaların başlık analizlerinin yanında içerik olarak da değerlendirilmesi için kelimeler temel bir sadeleştirme işleminden geçirilip değerlendirilmiş ve sınıflamaya tabi tutulmuştur. Sınıflandırılan içerikler yeni gelen epostalara örnek set oluşturması için veri tabanına sadeleştirilerek kaydedilmiş ve yeni gelen epostalara; ortak veya benzer kelime sayılarını sayarak içerik benzerliği ölçülüp sınıflandırma tahmini yapılmıştır. Bu sayede ortak bir bilinç oluşturup içerik olarak epostaların taşıdığı bilgiler sınıflandırılabilmektedir ve kurumlarda bilginin değerinin ölçülmesi kolaylaşmaktadır. Yeni gelen epostalar için bir tahmin sunulabilmekte ve kullanıcıların aldıkları epostanın taşıdığı bilgi seviyesini ölçmelerinde yardımcı olunabilmektedir.

Sistemin genel sınıflandırma başarısı %80, istenmeyen eposta sınıflandırma başarısı ise %83 olarak elde edilmiştir. Bu sistem yerel ağda çalışabilen bir masaüstü uygulama olabilme özelliği ile literatüre katkı sağlamaktadır.

***Anahtar Kelimeler*—Elektronik posta, bilgi güvenliği, bilgi güvenliği farkındalığı, sınıflandırma.**

***Abstract*—In this paper, you can see the study about email classification and evaluation system which works according to email contents and header information. This system is developed to assist information security awareness for all staff types of any organization.**

In the study, a basic SMTP application is developed for connecting enterprise email server and getting emails. To analyze received emails from server, content information and header information are extracted and examined. After examination of headers and content, result is provided with visuals and numeric values to facilitate understanding of information value of email content. In addition to evaluation by the email header analysis, email content is subjected to a fundamental simplification process and after this process, words are saved to database to be reference for new incoming emails. Similarity of emails is calculated with common or similar words count between database and new incoming mail. Thus, new incoming emails can be evaluated according to common consciousness that created with words has been saved to database. And the system can provide estimates for all staff of enterprise about value of email content like spam, important or classified etc. Through this system aimed to decrease human factor in information security for enterprise security.

Overall classification success ratio of the system was obtained as %80 and spam email classification success ratio was obtained as %83. This system contributes to literature with being a desktop application that could work in local networks feature.

***Index Terms*—Electronic mail, Information security, Information security awareness, classification.**

I. GİRİŞ

EPOSTA mesajları başlık bilgileri ve gövde (ana kısım) bilgileri olarak yapılandırılmıştır ve standartlaştırılmıştır. Gövde genel olarak düz metin şeklindedir ancak HTML (Hyper Text Markup Language) ve MIME (Multi-purpose Internet Mail Extensions) formatlarını da barındırabilir. Ayrıca eposta gövdelerine bir takım multimedya ekleri de eklenebilir. Başlık bölümünde ise epostanın yönlendirilmesini ve kimliğini oluşturmayı sağlayan birçok özel alan vardır. Başlık bilgilerindeki özel alanlar arasında; Kimden (From), Kime (To), Bilgi (CC), Gizli Bilgi (BCC), Konu (Subject), Tarih (Date), Dönüş Yolu (Return Path) gibi alanlar vardır. Epostalar iletişim protokolü olarak Simple Mail Transfer Protocol (SMTP) kullanırlar. Diğer taraftan epostaların adresler arasında iletilmesini sağlayan Mail Transfer Agent (MTA) sunucuları vardır. Bu sunucuların bilgileri de başlık bilgilerine eklenir [1].

Kimden başlığında epostayı gönderen kişinin eposta adres bilgisi bulunur. Kime başlığında epostayı alacak kişinin eposta bilgisi bulunur. Bilgi başlığı, epostayı alan kişiden ayrıca bir kopya da buradaki adrese göndermek için bulunan başlık alanıdır, buraya birden fazla eposta adresi yazılabilir ve hepsine bir kopya gönderilir. Gizli Bilgi başlığı da Bilgi başlığı ile aynı şekilde çalışır ancak alıcı kişi Gizli Bilgi kısmındaki alıcıyı/alıcıları göremez. Konu başlığı epostanın konusunu belirten başlık alanıdır. Tarih başlığı epostanın gönderilme/alınma tarihini gösteren alandır. Tarih başlığındaki tarih bilgisi kullanılan eposta uygulaması aracılığıyla epostanın kaynağına eklenir. Dönüş Yolu başlık alanı, epostaların gönderimleri sonrasında iletildi mesajının alınması veya iletimin başarısız olması durumunda başarısız bildiriminin

kime yapılacağını belirten başlık alanıdır.

Eposta kullanımı internetin ortaya çıkmasından bugüne kadar hızla artmaktadır. Resmi ve kişisel yazışmalarda, birçok internet sitesi aboneliğinde ya da birçok paylaşımda eposta yazışmaları kullanılmaktadır. Günümüzde; bir günde ortalama 200 milyardan fazla eposta gönderilmektedir [3].

Kurumsal yazışmalarda da birçok yazışma, kayıtlı olarak veya kayıtsız olarak epostalar aracılığıyla yapılmaktadır. Yapılan bu yazışmalarda birçok sınıflandırılmış ya da sınıflandırılmamış bilgi paylaşılmaktadır. Kurumlarda eposta ile paylaşılan bu bilgilerin gizli olmasından veya kritik öneme sahip olmasından dolayı genelde güvenlik zafiyeti ortaya çıkmaktadır. Bu duruma da dolaylı olarak kullanıcı sebep olmaktadır. Kurumlarda birçok alanda eğitimli veya eğitimsiz çalışan bulunmaktadır. Bu çalışanlar ne kadar eğitilse de veya uyarılsa da zaman zaman insan faktöründen dolayı gözden kaçan durumlar olabilmektedir. Bu gözden kaçan durumları en aza indirmek için akıllı yazılımlar devreye girmektedir. Eposta sınıflandırma ile ilgili yazılımlar genel olarak veri madenciliği teknikleriyle veya gönderen adresin uzantılarına göre sınıflandırma yapabilmektedir. Benzer olarak gelişmiş eposta sağlayıcıları epostaların içeriklerini de analiz edip gelişmiş bilgisayarlarla klasörleme şeklinde sınıflandırma yapabilmektedir [4].

Kurumlarda eposta sınıflandırması sadece varlık yönetimini kolaylaştırıyor gibi görünse de epostalar aracılığıyla halen büyük sayılarda kullanıcılar ve kurumlar, iletilen zararlı virüslerden ve istenmeyen epostalardan zarar görmektedir. Bu zarar, donanımsal seviyede olabildiği gibi birçok ilgisiz epostayla ilgilenip zaman kaybından dolayı ortaya çıkan bir zarar da olabilmektedir [5].

Çalışmanın ikinci bölümünde literatürdeki ilgili çalışmalardan bahsedilmiş, üçüncü bölümde geliştirilen sistem hakkında bilgiler paylaşılmış, dördüncü bölümde geliştirilen sistemin işleyişi detaylandırılmış,

II. İLGİLİ ÇALIŞMALAR

Yapılan literatür taramasında, çalışmaların genel olarak eposta klasörleme konulu olduğu görülmüştür. Bu çalışmalarda genelde istenmeyen posta tespiti ve klasörleme üzerine yoğunlaşılmıştır. Geliştirilen algoritmalarla epostanın spam olup olmadığı ya da spor, haber ve sinema gibi konularla ilgili olup olmadığını anlamaya yönelik çalışmalar yapılmıştır. Bu yaklaşımlar da gönderen adresin uzantısından veya tanınan epostaların sınıflandırılmasından yola çıkılarak yapılmıştır. Ayrıca sınıflandırma ve kümeleme için geliştirilmiş algoritmalar da bulunmaktadır [4]. Benzer şekilde daha gelişmiş olarak istenmeyen epostalardan Botnet tespiti yapmayı amaçlayan çalışmalar da literatürde mevcuttur. Bu çalışmalarda toplu olarak gönderilen istenmeyen epostaların göndericileri üzerinde analiz yapılıp Botnet tespiti yapmak amaçlanmıştır [9].

A. Eposta Sınıflandırma Konulu Akademik Çalışmalar

Araştırmacılar eposta sınıflandırma çalışmalarında genel olarak kullanım kolaylığı ve istenmeyen eposta tespiti üzerine yoğunlaşmıştır. Ama bu hizmeti gelişmiş eposta hizmet sağlayıcıları da varsayılan olarak verebilmektedir. Eposta hizmet sağlayıcıları ve gelişmiş eposta yönetim araçları (Outlook v.b.) da benzer şekilde klasörleme için destek vermektedir.

Yapılan çalışmalarda metin kümeleme üzerine VSM, KNN, Ripper, Maksimum Entropy, Winnow ve ANN gibi gelişmiş algoritmalar kullanılmıştır. Bu algoritmalar sayesinde metin içerikleri kategorilendirilmiş ve klasörlenmiştir. Çalışmalarda, gönderilen epostaların önemsiz eposta olup olmadığı sınıflandırmasına ek olarak ilgilenilen, ilgi dışı veya önemli önemsiz gibi sınıflandırmalar da yapılmaktadır [4]. Benzer şekilde içerik sınıflandırmasında yapay sinir ağları algoritmalarını kullanan çalışmalar da mevcuttur. Bu çalışmalarda web içerikleri çok katmanlı yapay sinir ağı modeli kullanılarak sınıflandırılmış ve bilgi güvenliği açıklıklarının giderilmesine katkıda bulunmuştur [19].

B. Eposta Sınıflandırma Konulu Ticari Ürünler

Kurumsal çözümler için ticari profesyonel çözümler bulunmaktadır. Bunlar eposta sınıflandırması yapabilen veya çok daha gelişmiş şekilde değerli bilgi takibi yapabilen Data Loss/Leak Prevention (Veri kaybı önleme) uygulamalarıdır. Ancak bu uygulamalar da açık kaynaklı olmadıkları için kurumlarda yine bir güven problemi oluşturmaktadır.

Eposta sınıflandırma alanında ticari uygulamalar arasında Boldon James firmasının "E-mail Classifier" uygulaması örnek olarak verilebilir. Boldon James E-mail Classifier uygulamasının yetenekleri şöyledir [17]:

- Bilgi güvenliği politikalarını uygular,
- Güvenlik politikaları hakkında kullanıcı bilincini yükseltir,
- Veri kaybı önleme (DLP) önlemleri geliştirir,
- Yapılandırılmamış bilgi kontrolleri,
- İç ve dış veri sızıntısını önler,
- Microsoft, Windows Hak Yönetimi politikaları, artı-posta şifreleme ve imzalama,
- Otomatik olarak en hassas içeriği koruma,
- Kullanıcı davranışı ve uyum pozisyon görünürlüğünü sağlama,
- Düşük dağıtım ve yönetim maliyetleri sağlama.

Bu konudaki bir diğer otorite de DLP (Data Loss/Leak Prevention) uygulamalarıdır. Bu uygulamalar bilgi güvenliği için çok daha gelişmiş olarak ağ katmanında veya son kullanıcı katmanında değerli bilgilerin sızdırılmasını veya paylaşılmasını engelleyici çok yetenekli uygulamalardır.

Eposta sınıflandırma alanında ticari uygulamalar arasında Boldon James firmasının "E-mail Classifier" uygulaması örnek olarak verilebilir. DLP uygulamalarına profesyonel cevap veren uygulamalar arasında GTB Technologies firmasının "GTB's Complete Data Protection Platform" ürünü örnek olarak verilebilir. Bu uygulama DLP konusunda birçok yerde karşılaşılan bir üründür. Bu ürün; bütün portlarda ve protokollerde, dosya paylaşımlarında, veritabanlarında, veri havuzlarında, Outlook kullanımında, büyük verilerde, mobil

cihazlarda, dizüstü ve masaüstü bilgisayarlarda ve bazı bulut çözümlerinde DLP hizmetini sağlayabilmektedir [18].

III. GELİŞTİRİLEN SİSTEM

Geliştirilen eposta sınıflandırma ve değerlendirme sistemi, kurumsal eposta sunucularında alınan önlemlerin ve genel güvenlik duvarı politikalarının yetersiz kaldığı durumlarda veya bu politikaların kapsamının dışında bir istisna oluştuğu durumlarda, bilgi varlıklarının korunması için epostada paylaşılan bilginin içeriğindeki kelimelere göre; gizli veya önemli bilgi olup olmadığı şeklinde, değerini ölçüp kullanıcıya bir tahmin sunarak kullanıcının paylaştığı bilginin değerinin farkına varmasını sağlamaktadır. Sistem bu yönüyle veri kaybı önleme sistemlerine benzerlik göstermektedir. Örneğin kullanıcının dışarıya ileteceği bir epostayı içeriğindeki kelimelerin gizli epostalar sınıfına benziyorsa kullanıcı uyarılıp sehven yapılacak hataların önüne geçilebilir.

Uygulamada sınıflandırma işlemi, kullanıcının epostaları okuyup değerlendirdiği sınıflandırma seçimleri hatırlanarak geçmişte yaptığı davranışlardan yeni gelen epostaları değerlendirmesi şeklinde gerçekleştirilmiştir. Bu sayede epostalara kullanıcının belirlediği uyarıcı etiketler verilmiş ve kullanıcıyla etkileşime geçilmiştir. Etiketler epostanın taşıdığı bilginin değerinin anlaşılmasına yardımcı olacak şekilde tasarlanmıştır ve kullanıma göre yeni etiketler belirlenebilmektedir. Geri bildirim şeklinde doğrulamayla eposta içerikleri sınıflandırılmış ve sınıflandırılan içeriklerle yeni gelen epostaların benzerliğine ve geçmişteki okunup sınıflandırılan epostalara göre veri tabanı oluşturulmuştur.

Saldırı içeren bir epostanın tespiti durumunda sistem, ortak havuzdan tahmin yaptığı için diğer kullanıcılara bir tahmin sunmakta ve kullanıcıyı uyarmaktadır. Bu uyarı da olası saldırıların önlenmesine veya en kötü durumda bir kullanıcı saldırıya uğrayınca bir sonrakilerin uyarılmasını sağlamaktadır. Aynı şekilde eposta içeriğinde paylaşılan bilginin değeri de sınıflandırma etiketlerine ortak veya benzer kelimeler sayılarak ölçülmekte ve sınıflandırması için var olan etiketlerden tahmini etiketler sunulmaktadır.

Literatürdeki yaklaşımlar ve uygulamalar bütün epostaları internette paylaşmayı gerektirdiği için kurumsal politikalarla çelişebilir. Kurumlarda gizlilik ve bilgi güvenliği gereği birçok eposta ve doküman dışarıya kapalıdır. Bu durumda kurumların kendi iç yazışmaları için kendilerinin geliştirdiği ve dışarıya kapalı bir uygulama gereksinimi ortaya çıkmıştır. Sunulan bu çalışmada geliştirilen eposta sınıflandırma ve değerlendirme sistemi ile kurumların epostalarını dışarıya açmadan kendi veritabanlarında saklayacakları bilgilerle, kendi belirledikleri kelime gruplarıyla sınıflandırma yapabilen ve bu kelime gruplarına göre bilgi değerini ölçebilen bir uygulamaya sahip olacaklardır.

A. Geliştirilen Sistemin Amacı

Sunulan çalışmada epostaları içeriklerine göre anlamlandıran ve sınıflandıran bir sistem geliştirilmiştir. Çalışma kapsamında geliştirilen sistemde temel amaç, kurumsal eposta hizmetlerinde alınan ve gönderilen epostaların değerlendirilmesi ve anlamlandırılmasıyla kullanıcılara önermelerde bulunarak paylaşılan bilginin önemi ve bilgi güvenliği seviyesinin anlaşılmasında kolaylık sağlamaktır. Bu sayede kullanıcıların bilgi güvenliği seviyesi ve farkındalığının arttırılması sağlanmıştır. Yapılan çalışma kapsamında Windows Form teknolojisi kullanılarak Microsoft Visual C# yazılım diliyle bir uygulama geliştirilmiştir. Bu uygulama ile elektronik posta sunucusundan epostalar alınarak sınıflandırılmakta ve uygulama tarafından daha önceki sınıflandırma sonuçlarına bakılarak tahmini bir sınıflandırma yapılabilmektedir.

B. Sistemin Çalışması

Geliştirilen sistem genel olarak makine öğrenmesi alt yapısı yaklaşımıyla kurgulanmıştır. Sunucudan alınan epostalar uygulama tarafından önce ön işlemden geçirilip yalınlaştırılmış ve veri tabanına kaydedilecek formatta düzenlenmiştir. Ekler, bağlaçlar ve rakamlar gibi anlam ağırlığı olmayan kelimeler çıkarıldıktan sonra kullanıcıdan epostanın sınıf niteliği hakkında bilgi alınıp, kalan kelimeler veritabanına kaydedilmiştir. Yeni gelen epostaların analizi için de veritabanında oluşturulan kelime havuzuna benzetim yapılarak en çok hangi sınıftaki kelimelere benziyorsa o epostanın sınıf bilgisi tahmini sınıf olarak sunulmuştur. Bu sayede örneğin daha önce gizli olarak sınıflandırılmış bir epostanın benzeri bir eposta alınırsa, kullanıcı epostanın değeri hakkında uyarılmakta ve o epostayla iletişim kurmadan önce bilinçlendirilmesi sağlanmaktadır.

C. Sistemin Etiketleme Yapısı

Çalışma kapsamında epostalar için belirli sınıflar tasarlanmış ve bu sınıflara renkler tahsis edilmiştir. Kullanıcılar bu sınıfları kendilerine göre özelleştirebilirler. Bilgi güvenliği uzmanlarının veya yetkili kullanıcıların daha önceden belirlediği sınıflandırılmış içerikler bu etiketleri taşımaktadır ve yeni gelen epostalar da bu içeriklerin etiketleriyle tahminlenecektir. Bu çalışma kapsamında etiketlerin renk yapıları,

- ISTENMEYEN POSTA: Siyah
- ÖNEMLİ: Turuncu
- TASNİF DIŞI: Yeşil
- GİZLİ: Sarı
- HİZMETE ÖZEL: Mavi
- VİRÜS: Kırmızı

olarak belirlenmiştir.

D. Sistemin Değerlendirme Yapısı

Geliştirilen sistemde epostanın kaynak verisi incelenip tehditlerin algılanması sağlanmaktadır. Kaynak verisiyle mesaj kimliği, epostanın ulaşmasına kadar oluşan gecikme süresi, epostanın üzerinden geçtiği sunucu bilgileri ile ayrıntıları ve kaynağı HTML veya RAW formatında görüntüleme özellikleri sunulmuştur.

Değerlendirme yapısında mesaj kaynağının el ile

incelenmesi için de ayrıştırılıp kullanıcıya sunulması sağlanmıştır. Bu sayede kullanıcının değerlendirdiği epostaların içerikleri ön işlemden sonra kaydedilmiş ve tahminleme analizi için referans olarak kullanılmıştır.

Değerlendirilip analiz edilecek olan yeni gelen eposta, önceden veritabanına kaydedilmiş sınıflandırılmış kelimelerle aynı ön işlemden geçirilmiş ve uzaklık hesaplayan algoritmalarla benzetim yapılmıştır. Uzaklık belirleyen algoritmalar için uygulamada tasarlanan algoritmaya ek olarak, aynı kökten gelen veya birbirine benzeyen kelimelerle benzetimi hassaslaştırmak ve doğruluk oranını arttırmak [6] için Levenshtein Distance uzaklık hesaplayıcı algoritma da kullanılmıştır.

Uygulama kapsamında tasarlanan algoritmada, ön işlemden geçirilen eposta gövdesindeki kelime listesiyle veri tabanındaki kelime listeleri karşılaştırılır. Karşılaştırma sonucunda gelen eposta hangi eposta sınıfındaki kelimelere daha çok benziyorsa, o epostanın sınıf verisi tahmini sınıf olarak sunulur. Bu algoritmaya ek olarak Levenshtein Distance algoritmasıyla da opsiyonel olarak destek verilmiştir. Kullanıcının ilgili formdaki Levenshtein algoritmasını da kullanması için gereken kontrolü seçmesiyle benzetim detaylandırılır ve harf benzerlikleri sayılır, en fazla %20 farklı kelimeler aynı sayılır ve benzetim güçlendirilmiş olur.

IV. Geliştirilen Sistemin İşleyişi

Sistem için bir SMTP istemcisi geliştirilmiş ve bu istemciye bağlanan eposta adresinden epostaların alınması sağlanmıştır. Alınan epostalar gelen kutusu benzeri bir veri yapısında listelenmiştir ve detayların verildiği paneller eklenmiştir.

Bu alt yapı için .NET yapılarından Windows Form uygulamaları seçilmiş ve proje oluşturulmuştur. Oluşturulan bu projede .NET SMTPClient sınıfı kullanılmış, e-posta bağlantısı gerekli protokol çerçevesinde gerçekleştirilmiştir. Alınan epostalar bir gelen kutusu yapısına göre listelenmektedir. Listelemede seçilen e-posta için standart gelen kutusu gösterimlerinin yanında bir de bayrak yapısı ve değerlendirme sonucunu belirten etiketler gösterilmiştir.

Geliştirilen uygulamada POP3 bağlantısı yapan açık kaynaklı kütüphane kullanılmıştır ve standart bağlantı protokolleri bu kütüphane ile sağlanmıştır. Uygulamanın giriş ekranında kullanıcının eposta adresi ve parolası alınıp güvenli bir şekilde epostaların alınması sağlanmıştır. Alınan epostalar sistemin gelen kutusunda kullanıcıya sunulmaktadır.

A. *Uygulamanın Çalışma Prensipleri*

Uygulamanın giriş ekranında gerekli protokoller sağlandıktan sonra giriş yapılıp, gelen ekranda alınan epostalar listelenmektedir. Listelenen epostalara ait gönderen kişi ve gönderme tarihleri gibi temel bilgileri sunulmaktadır. Detayları görüntülenmek istenen eposta için bu listeye gidilip ilgili eposta tıklandığında sistem seçili eposta için analizleri yapıp detayları sağ tarafındaki panelde göstermektedir. Detayların gösterildiği panelde temel olarak kimden, kime, bilgi ve konu gibi başlıkların yanında mesaj ID, epostanın uğradığı sunucular ve gönderim esnasında yaşanan toplam gecikme gibi başlıklar da detaylı bir şekilde sunulmaktadır. Epostanın iletilirken uğradığı sunucuların ayrıntıları verilirken; sunucunun ismi, IP adresi, metodu ve tarih bilgileri verilmiştir. Mesaj ID alanında ise epostaların tekilliğini sağlayan kimlik bilgisi verilmiştir. Ayrıca buradaki kimlik bilgisi ile gönderen kişinin adresinin uzantıları benzemiyorsa muhtemel bir sahte eposta durumu olduğu anlaşılmaktadır. Bu durum mesaj ID alanında belirtilmektedir. Eposta içeriğinin hem HTML formatında gösterimi hem de işlenmemiş RAW formatında gösterimi sağlanabilmektedir. Bu seçimi yapmak için, mesaj kutusunun hemen solunda bulunan tercih kutularındaki seçimi değiştirmek yeterlidir.

Kategori alanındaki aşağı açılan liste ile seçili epostanın sınıflandırma etiketi belirlenip kaydedilebilmektedir. Belirlenen bu sınıflandırma etiketi kaydedilip o etiket ile ilgili veriseti oluşturulmuştur. Yeni gelen epostalar bu kayıtlardan elde edilen verisetine, bir denetimsiz dinamik öğrenme modeli ile tahminleme yapılıp etiket önerisiyle desteklenir. Örneğin gelen epostanın içeriği daha önce tasnif dışı olarak etiketlenen bir eposta içeriğine benziyorsa bu eposta da tasnif dışı olarak etiketlenmektedir.

B. *Uygulamada Kullanılan Değerlendirme Algoritmaları*

Çalışmada daha önceki bilgi değeri etiketlenen istenmeyen eposta veya zararlı epostaların tanınmasından dolayı ortak bir hafıza oluşturulmuş ve veritabanına kaydedilerek bir veri seti oluşturulmuştur. Veri setini oluşturacak içerik için anlamlı terimler seçilmiştir. Bu yapı için ön işleme algoritması geliştirilmiştir. Bu algoritma kapsamında noktalama işaretlerinin, eklerin, bağlaçların, rakamların ve gereksiz boşlukların çıkarılması şeklinde epostalar ön işleme tabi tutulmuştur. Ön işlemden sonra kaydedilen içeriklerle ortak bir hafıza oluşturmuştur.

Bu ortak hafıza eğitim setimiz olarak nitelendirilebilir. Ayrıca dinamik bir eğitim seti olduğu için ve geliştiği için denetimsiz bir öğrenme algoritması olarak nitelendirilebilir. Benzetim yapılırken daha önce etiketlendirilen epostaların içeriklerinin oluşturduğu veriseti yardımıyla tahminleme yapılmaktadır.

Benzetim için tasarlanan altyapı Google arama motorundaki "Bunu mu demek istediniz?" özelliğinde kullanılan algoritmalara benzerlik göstermektedir. Bu yapıda kullanıcılar yanlış yazdıkları kelimeler için sonuç bulamayınca düzeltip tekrar aramayı denemektedirler. Google da bu arama süreçlerini kaydedip kullanıcıların dillerinde hangi kelime için hangi yanlış yazımlar yapılabilir şeklinde bağıntılar biriktirmektedir. Bu bağıntıları kullanarak bu hizmeti sunmaktadır [19].

Benzetim yapısı için uygulamaya özel bir algoritma tasarlanmış ve Levenshtein algoritması ile desteklenmiştir. Uygulama için geliştirilen algoritmada ön işlemden geçen kelimeler veritabanındaki kelime havuzlarından hangisine daha çok benziyorsa o sınıfa ait olabileceği tahmini sunulmaktadır. Destekleyici algoritma olan Levenshtein algoritması ise dizi yapıları arasındaki benzerlik uzaklıklarını hesaplayan bir algoritmadır. Bu algoritma ile birbirine benzer ya da birbirinin

kökleri olan kelimeler bulunabilmektedir [7]-[8]. Uygulamada %20 benzerlik kabul edilebilir bir oran olarak alınmış ve aynı köklü veya benzer kelime olarak nitelendirilerek benzetim hassaslaştırılmıştır. Levenshtein mesafesi ölçülürken kelimelerin arasındaki uzaklık farkı %20 veya daha az ise kabul edilebilir olarak hesaplanmaktadır.

C. *Uygulama Sonuçları*

Uygulamada geliştirilen benzetim algoritması, Levenshtein destekli iken farklı, yalın haldeyken farklı sonuçlar üretebilmektedir. Bu farklı sonuçlar iki tahminin değerlerinin birbirine yakın olmasından kaynaklanmaktadır. Benzetim hassaslaştırılınca benzer köklü kelimelerle değerler daha detaylı incelenebildiği için tahminin doğruluğu arttırılmıştır. Yeterli eğitim veriseti oluşturulduktan sonra genel olarak uygulamadaki algoritmanın başarısı; daha önce tanımadığı önemsiz veya istenmeyen epostaları tanıyabildiği için başarılı olarak değerlendirilmiştir.

Sistem etiketleri tanımak için belirlenen sınıflara dahil edilen 10'ar eposta ile eğitildikten sonra tahmin başarısı hesaplanmıştır. Genel olarak 60 eposta içinden sistemin sunduğu tahmin sınıf ve okunup karar verilen sınıf arasında 48 eposta içeriği doğru sınıflandırılmıştır ve 12 eposta içeriği yanlış tahmin edilmiştir. Dolayısıyla sistemin genel sınıflandırma başarısı %80 olarak elde edilmiştir. Istenmeyen eposta etiketi için ise 30 eposta üzerinde sistemin başarısı ayrıca hesaplanmış ve Tablo 1'de sunulan karmaşıklık matrisi elde edilmiştir.

TABLO I. ISTENMEYEN EPOSTALAR İÇİN KARMAŞIKLIK MATRİSİ

		Tahmin	
		Pozitif	Negatif
Gerçek	Pozitif	8	3
	Negatif	2	17

Tablo 1'de sistemin analiz yapıp tahmin sunduğu 30 adet epostanın istenmeyen eposta etiketi için karmaşıklık matrisi sunulmaktadır. İstenmeyen eposta etiketi sınıflandırması sonucunda 30 epostadan 25'i doğru sınıflandırılmış, 5'i yanlış sınıflandırılmış, dolayısıyla %83 başarı sağlanmıştır.

V. SONUÇ

Sunulan çalışmada eposta içerikleri ve kaynak verileri incelenip anlamlandırma üzerine bir sistem geliştirilmiştir. Sistem eposta sunucusuna bağlanabilen ve eposta alabilen, sonrasında analizler yapıp %80 başarıyla tahminleme yapabilen bir istemci şeklinde tasarlanmıştır. Geliştirilen sistem ile kurumların eposta sunucularından epostalar alınmakta ve normal şartlarda epostaların işlenmemiş kaynağına bakıldığında anlaşılmayan ve analiz etmesi zor başlık bilgileri düzenlenerek kullanıcılara sunulmaktadır.

Geliştirilen sistem genel olarak; kurumsal eposta sunucusunda oturum açmak için giriş bilgilerini aldıktan sonra standart gelen kutusu benzeri bir yapı ile epostaları almaktadır. Sonrasında seçilen epostayı gösterirken başlık detaylarını anlaşılır biçimde göstermektedir. Bir masaüstü uygulaması olup yerel ağda çalışabilen bir uygulama olarak bu özellik literatürde ilktir. Başlık detaylarında kimden, bilgi ve konu başlığı gibi standart alanların yanında epostanın tekilliğini sağlayan mesaj ID, iletilme sürecinde oluşan toplam gecikme süresi ve epostanın iletilinceye kadar uğradığı sunucuların detayları listelenmiştir. Bu başlık detaylarının yanında epostalar kullanıcının belirlediği sınıflara göre de etiketlenebilmektedir. Bu etiketlerle bilgi güvenliği farkındalığı olan kullanıcıların sınıflandırma seçimleri hatırlanarak, bu sistemi kullanan diğer kullanıcıların da yeni gelen epostaları değerlendirmelerine yardımcı olmaları sağlanabilmektedir.

Sunulan çalışma ile kurumsal epostalarda paylaşılan bilgilerin güvenlik farkındalığını arttırmak ve epostalardaki bilgi değerini daha önceki okunup sınıflandırılan epostalara göre hesaplamak için bir sistem geliştirilmiştir. Bu sayede kullanıcıların sehven paylaştıkları bilgilerin değerleri hatırlatılacak ve bilgi güvenliğindeki insan faktörü azaltılabilecektir.

Literatürdeki eposta sınıflandırma çalışmalarında genel olarak kullanım kolaylığı ve istenmeyen eposta tespiti üzerine yoğunlaşılmıştır. Fakat bu hizmeti gelişmiş eposta hizmet sağlayıcıları da varsayılan olarak verebilmektedir. Kurumsal çözümler üreten firmalar güvenlik üzerine yoğunlaşmış profesyonel uygulamalar sunmaktadır. Bu uygulamaların da ciddi ücretler karşılığında kurulumları yapıldığı için tercih edilme oranları azalmaktadır. Aynı şekilde DLP çözümlerinin de bilgi değeri olan ve kritik işler yapan ya da üst bilgilerini korumak isteyen her kurumun kullanması gerekmektedir. Ancak bu uygulamalar da ciddi maliyetler gerektirdiği için her kurum bu imkanlara sahip olamamaktadır. Maliyet konusunda engeller olmasa bile kurumlar epostalarını dışardan bir uygulama üzerinden değerlendirmek istemeyebilmektedir.

Sunulan çalışmada geliştirilen sistem sayesinde kurumlar kendi kurallarını belirleyebilmekte ve dışarıya açık olmayan bir uygulamaya sahip olabilmektedir. Ayrıca bu sistem sayesinde kurumsal bilgi güvenliğinin sağlanmasındaki birincil ve yönetilmesi çok zor olan insan faktörünün etkilerini azaltmak için yardımcı bir uygulama sunulmaktadır. Aynı şekilde kurumsal veya kişisel bilgi güvenliği farkındalığı eksiği olan kullanıcılar da bu uygulama sayesinde eposta başlık yapıları analizi yetkinliğine sahip olabilmekte ve kişisel incelemelerde de farkındalıklarını arttırılabilmektedir. Geliştirilen sistem sayesinde, kurumlarda kullanılan eposta hizmetlerinde paylaşılan, tasnif edilmesi ve değerinin hesaplanması zor olan bilginin değerini hesaplamada, kurumlara epostalarını dışarıya açmalarına gerek kalmadan yardımcı olunabilmektedir.

KAYNAKLAR

[1] P. Resnick, "Internet Message Format", *RFC 2822*, 2001.
[2] M.T. Banday, F.A. Mir, J.A. Qadri, N.A. Shah, "Analyzing Internet e-mail date-spoofing", *Digital Investigation*, 7 (3-4), 145-153, 2011.

[3] Internet: "Dünya İstatistikleri, Bugün gönderilen Eposta Sayısı", http://www.worldometers.info Erişim Tarihi: 22.07.2015.
[4] I. Alsmadi, I. Alhami, "Clustering and classification of email contents", *Journal of King Saud University – Computer and Information Sciences*, 27 (1), 46–57, 2015.
[5] M. A. Al-Kadhi, "Assessment of the status of spam in the Kingdom of Saudi Arabia", *Journal of King Saud University – Computer and Information Sciences*, 23 (2), 45–58, 2011.
[6] Internet: "Levenshtein Uzaklığı Algoritması", http://en.wikipedia.org/wiki/Levenshtein_distance Erişim Tarihi: 22.07.2015.
[7] Internet: "OpenPOP .NET Kütüphanesi", http://sourceforge.net/projects/hpop Erişim Tarihi: 22.07.2015.
[8] Internet: "Levenshtein Algoritması Uygulaması", http://en.wikibooks.org/wiki/Algorithm_Implementation/Strings/Levenshtein_distance Erişim Tarihi: 22.07.2015.
[9] L. Zhuang, J. Dunagan, D.R. Simon, H.J. Wang, J.D. Tygar, "Characterizing Botnets from Email Spam Records", *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats LEET'08*, 2, 2008.
[10] H. Önal, "E-posta Başlıklarından Bilgi Toplama", *Bilgi Güvenliği Akademisi*, 2009.
[11] L. Daniel, L. Daniel, "E-mail Evidence", Digital Forensics for Legal Professionals, Bölüm 34, 239-244, 2012.
[12] D. Bradbury, "Can we make E-mail Secure?", Network Security, 2014 (3), 13-16, 2014.
[13] M. N. Marsono, M. W. El-Kharashi, F. Gebali, "A spam rejection scheme during SMTP sessions based on layer-3 e-mail classification", *Journal of Network and Computer Applications*, 32 (1), 236–257, 2009.
[14] G. González-Talaván, "A simple, configurable SMTP anti-spam filter: Greylists", *Computers & Security*, 25 (3), 229–236, 2006.
[15] W. Goralski, "SMTP and Email", *The Illustrated Network: How TCP/IP Works in a Modern Network*, Bölüm 21, 535–558, 2009.
[16] Boldon James, "Boldon James E-mail Classifier, Boldon James Product Datasheet, 1-2, 2015.
[17] GTB Technologies, "GTB's Complete Data Protection Platform","https://www.gtbtechnologies.com/en/products/the-gtb-data-loss-platform" About Product, Erişim Tarihi: 22.07.2015.
[18] Otomatik Tamamlama, https://support.google.com/websearch/answer/106230?hl=tr Erişim Tarihi: 22.07. 2015.
[19] E. N. Güven, H. Onur, Ş. Sağıroğlu, "Yapay Sinir Ağları ile Web İçeriklerini Sınıflandırma", Bilgi Dünyası, Cilt:9, No:1, s.158-178, Nisan 2008.

Şeref SAĞIROĞLU, Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü ve Bilgisayar Mühendisliği Bölüm Başkanıdır. İletişim için ss@gazi.edu.tr adresini kullanmaktadır.

Eyüp Burak CEYHAN, Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünde araştırma görevlisidir. İletişim için eyupburak@gmail.com adresini kullanmaktadır.

Abdurrahman YILDIZ, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği ABD'da Yüksek Lisans öğrenimine devam etmektedir. İletişim için abdurrahmanyildiz35@gmail.com adresini kullanmaktadır.