T.C.
İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

WEB TABANLI OLTALAMA SALDIRILARININ MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE TESPİTİ

MUSTAFA KAYTAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Haziran - 2016

Tezin Başlığı : Web Tabanlı Oltalama Saldırılarının Makine Öğrenmesi Yöntemleri İle Tespiti

Tezi Hazırlayan : Mustafa KAYTAN

Sınav Tarihi : 03.06.2016

Yukarıda adı geçen tez jürimizce değerlendirilerek Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans Tezi olarak kabul edilmiştir.

Sınav Jüri Üyeleri

Tez Danışmanı: **Doç. Dr. Davut HANBAY**
İnönü Üniversitesi …….

Prof. Dr. Ali KARCI
İnönü Üniversitesi …….

Doç. Dr. Resul DAŞ
Fırat Üniversitesi …….

Prof. Dr. Alaattin ESEN
Enstitü Müdürü

ONUR SÖZÜ

Yüksek Lisans Tezi olarak sunduğum "Web Tabanlı Oltalama Saldırılarının Makine Öğrenmesi Yöntemleri İle Tespiti" başlıklı bu çalışmanın bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım bütün kaynakların, hem metin içinde hem de kaynakçada yöntemine uygun biçimde gösterilenlerden oluştuğunu belirtir, bunu onurumla doğrularım.

Mustafa KAYTAN

ÖZET

Yüksek Lisans Tezi

WEB TABANLI OLTALAMA SALDIRILARININ MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE TESPİTİ

Mustafa KAYTAN

İnönü Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

86 + xi sayfa

2016

Danışman: Doç. Dr. Davut HANBAY

Bu tez çalışmasında öncelikle bilgi güvenliğine yönelik tehditler açıklanmış; bu tehditlere karşı savunma yöntemleri ve öneriler sunulmuştur. Oltalama web sitelerinin tespit edilmesine yönelik olarak iki uygulama gerçekleştirilmiştir. Birinci uygulamada Yapay Sinir Ağı modeli ile oltalama web sitelerinin tespit edilmesine yönelik sınıflandırma uygulaması gerçekleştirilmiştir. Bu uygulama ile oluşturulan ağlara 5-li çapraz geçerlilik testi uygulanmıştır. Ortalama sınıflandırma doğruluğu %90,61, en yüksek sınıflandırma doğruluğu ise %92,45 olarak ölçülmüştür. İkinci uygulamada ise Aşırı Öğrenme Makinesi modeli ile oltalama web sitelerinin tespit edilmesine yönelik sınıflandırma uygulaması gerçekleştirilmiştir. Bu uygulamada 10-lu çapraz geçerlilik testi uygulanmıştır. Ortalama sınıflandırma doğruluğu %95,05, en yüksek sınıflandırma doğruluğu ise %95,93 olarak ölçülmüştür.

ANAHTAR KELİMELER: Makine Öğrenmesi, Yapay Sinir Ağı, Aşırı Öğrenme Makinesi, sınıflandırma, oltalama, bilgi güvenliği.

ABSTRACT

M.Sc.Thesis

WEB-BASED PHISHING ATTACKS DETECTION WITH MACHINE LEARNING METHODS

Mustafa KAYTAN

İnönü University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

86 + xi pages

2016

Supervisor: Assoc. Prof. Dr. Davut HANBAY

In this thesis, firstly the threats on information security are described; methods of defense against these threats, and recommendations are presented. Two applications in order to identify the phishing website were performed. In the first application, classification application has been performed for the detection of phishing website by Artificial Neural Network model. 5-fold cross-validation test has been applied to the created networks with the first application. The average classification accuracy was achieved as 90.61%, and the highest classification accuracy was achieved as 92.45%. In the second application, classification application has been performed for the detection of phishing website by Extreme Learning Machine model. In the second application, 10-fold cross-validation test has been applied. The average classification accuracy was achieved as 95.05%, and the highest classification accuracy was achieved as 95.93%.

KEYWORDS: Machine Learning, Artificial Neural Network, Extreme Learning Machine, classification, phishing, information security.

TEŞEKKÜR

Bu çalışmanın her aşamasında yardımlarını ve ilgilerini esirgemeyen, her konuda kendisine danışabildiğim, öneri ve desteğini esirgemeyen, çalışmalarımda beni yönlendiren saygıdeğer danışman hocam Sayın Doç. Dr. Davut HANBAY'a;

Ayrıca her konuda bana destek olan, hayatım boyunca hep yanımda olan, her türlü fedakârlıkta bulunan aileme

teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

KISALTMALAR

ACK	Acknowledgement
ANN	Artificial Neural Network
AÖM	Aşırı Öğrenme Makinesi
ARP	Address Resolution Protocol
BGYS	Bilgi Güvenliği Yönetim Sistemi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CD	Compact Disc
CSRF	Cross-Site Request Forgery
ÇKA	Çok Katmanlı Algılayıcı
DDoS	Distributed Denial of Service
DLP	Data Leakage Prevention
DNS	Domain Name System
DOM	Document Object Model
DoS	Denial of Service
DT	Decision Tree
DVD	Digital Versatile Disc
DVM	Destek Vektör Makinesi
ELM	Extreme Learning Machine
FTP	File Transfer Protocol
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KA	Karar Ağacı
KDD	Knowledge Discovery and Data mining
MAC	Media Access Control
MARK	Multiple Adaptive Reduced Kernel

MITM	Man In The Middle
MKBoost	Multiple Kernel Boost
ML	Machine Learning
MLP	Multi Layer Perceptron
MOVICAB	MObile VIsualisation Connectionist Agent-Based
MsSQL	Microsoft Structured Query Language
MySQL	My Structured Query Language
NAC	Network Access Control
NAT	Network Address Translation
NB	Naive Bayes
NSL	Network Security Laboratory
NUAIS	Non-Uniform Adaptive Image Segmentation
OPF	Optimum-Path Forest
OS	Operating System
OS-ELM	Online Sequential Extreme Learning Machine
OSSIM	Open Source Security Information Management
RDP	Remote Desktop Protocol
RMSE	Root Mean Squared Error
RT	Real Time
SES	Saldırı Engelleme Sistemi
SFH	Server Form Handler
SIEM	Security Information and Event Management
SLFN	Single-hidden Layer Feedforward Neural Network
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Socket Layer
STS	Saldırı Tespit Sistemi
SVM	Support Vector Machine
SYN	Synchronize
TCP	Transmission Control Protocol
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UCI	University of California, Irvine
UDP	User Datagram Protocol
URL	Uniform Resource Locator

USB	Universal Serial Bus
VPN	Virtual Private Network
YSA	Yapay Sinir Ağı

1. GİRİŞ

Siber güvenlik her geçen gün daha da önem kazanmaktadır. Bireylerden başlayarak devletlere kadar hemen herkesi ilgilendiren bir konu haline gelmektedir. Kurumlar arasında siber güvenliğe verilen önem büyük farklılıklar göstermektedir. Siber tehdidin hedefleri; bireyler, kurumlar veya devletler olabilmektedir [1].

Kurumsal bilgi güvenliği; bilgi varlıklarının tespit edilmesi, zafiyetlerinin belirlenmesi, istenmeyen tehditlerden ve tehlikelerden korunmak amacıyla gerekli güvenlik analizlerinin yapılması ve gerekli önlemlerin alınması olarak tanımlanabilir [2].

Geçmişte klasik savaş araçlarıyla yapılan savaşlar, günümüzde siber teknolojilerle gerçekleştirilmektedir. Bir ülkenin güvenliği ile siber güvenlik kavramlarının anlamları birbirine yaklaşmaktadır. Bir kuruma yapılabilecek siber bir saldırı düşük maliyetli olabilir ama buna karşı alınacak olan siber bir savunma ise yüksek maliyetli olarak karşımıza çıkmaktadır. Siber güvenlik, yaşadığımız asırda ülkemizin en yeni ve en önemli sorunudur. Siber savaş, bilişim uzmanları tarafından bilgi ve iletişim teknolojileri kullanılarak bir kuruma ya da bir devlete yapılan saldırı ve bu kurum ya da devletin bu teknolojileri kullanarak yaptığı savunma olarak tanımlanabilir [1].

Siber saldırılar daha önce tanımlanmış koşullar altında veya belirli bir tarihte başlatılabilir. Tespit edilen saldırı araçlarının adli bilişim uzmanları tarafından bile tamamen bir ağdan kaldırılması kolay olmayabilir. Tüm karşı saldırı seçeneklerinin ortadan kaldırıldığından emin olmak siber saldırı teknolojisiyle imkânsız gibi görünmektedir [3].

Günümüzde bilgi iletişim araçları kullanılarak bilgi çok yoğun bir şekilde iletilmektedir. Bu amaçla çeşitli problem tiplerine çeşitli çözüm yöntemleri geliştirilmiştir. Makine Öğrenmesi (Machine Learning (ML)) yöntemleri, bilgi güvenliğine yönelik uygulama geliştirmede de kullanılabilmektedir. Optimizasyon, sınıflandırma, tahmin ve karar destek sistemi ile bilgi güvenliğinden sorumlu kişiye büyük faydalar sağlanabilmektedir. Günümüzde akıllı uygulamalar geliştirmek gittikçe popüler bir konu olmaya başlamıştır. Akıllı olmayan bir uygulama, kullanıcıyı gerekli olmayan, tekrar gerektiren bir iş yapmak durumunda bırakabileceğinden verim kaybına sebep olabilmektedir.

Son yıllarda akıllı yöntemlerdeki gelişmeler, akıllı yöntemleri karmaşık

sistemlerin modellenmesinde kullanmayı mümkün hale getirmiştir [4].

Bilgi ve iletişim araçlarının oluşturduğu ağlara farklı amaçlar için saldırılar olmaktadır. Bu saldırıların tespit edilip gerekli önlemlerin alınması gerekmektedir. Bilgisayar teknolojisinin gelişimi ile beraber yapay zekâ alanındaki çalışmaların da hız kazandığı görülmektedir. Yapay zekâ yöntemleriyle bilgi güvenliğine yönelik yapılan çalışmaların her geçen gün daha da arttığı görülmektedir. Akıllı sistemler, bilgi güvenliğinden sorumlu olan uzman bir kişiye karar verme sürecinde büyük yararlar sağlamaktadır [5].

Makine öğrenmesi yöntemleri, çeşitli alanlarda sınıflandırma amacı ile kullanılabilmektedir. Sınıflandırma, bir verinin belirli kurallara göre düzenlenmiş veri setindeki sınıflardan hangisine ait olduğunu tespit etme süreci olarak düşünülebilir. Birçok alanda kullanılan ve önemli bir yere sahip olan sınıflandırma, bilgi güvenliği için de ayrı bir yere sahiptir.

1.1 Çalışmanın Amacı

Bilgi ve iletişim sistemleri; konak, ağ veya melez yapılarda olabilmektedir. Bu yapılarda saldırı, savunma veya her iki amaca hizmet eden çeşitli araçlar kullanılabilmektedir. Bilgi güvenliğine yönelik saldırı yöntemleri ve araçları ile bilgi güvenliğini sağlamaya yönelik tedbirler ve araçların tamamı bu tez çalışmasında ele alınamayacak kadar çeşitlilik göstermektedir. Bu tez çalışmasında siber güvenliğe yönelik bazı tehditler ile bu tehditlere karşı alınabilecek bazı önlemler anlatılmıştır.

Bu yüksek lisans tez çalışmasının amacı, bilgi güvenliğini sağlamaya yönelik çeşitli öneriler sunmak ve çeşitli makine öğrenmesi tekniklerinin web tabanlı oltalama saldırılarında etkili bir şekilde kullanılabildiğini göstermektir. Bu amaca yönelik olarak;

1. Makine öğrenmesi yöntemlerinden Yapay Sinir Ağı (YSA) (Artificial Neural Network (ANN)) kullanılarak bilgi güvenliğine yönelik bir saldırı olan ve oltalama diye adlandırılan web sitelerinin belirlenmesine yönelik sınıflandırma yapmak için bir uygulama yapılmıştır.
2. Makine öğrenmesi tekniklerinden Aşırı Öğrenme Makinesi (AÖM) (Extreme Learning Machine (ELM)) yöntemi ile oltalama olarak tabir edilen web sitelerinin tespit edilmesine yönelik sınıflandırma yapmak için bir uygulama yapılmıştır.

3. Uygulamalarda kullanılan veri setindeki kurallardan iki tanesi için iki yeni kural önerilmiştir.
4. Bilgi güvenliğini sağlamaya yönelik olarak bazı öneriler sunulmuştur.

1.2 Çalışmanın Organizasyonu

Bu bölümde çalışmanın amacı, çalışmanın organizasyonu ve kaynak özetlerine yer verilmiştir. Takip eden diğer bölümler için çalışma organizasyonu aşağıda sıralanmıştır.

Bölüm 2'de, kuramsal temellere yer verilmiştir. Siber saldırı tehditleri ile siber savunma tedbirleri ele alınmıştır.

Bölüm 3'te, materyal ve yöntem açıklanmıştır. Bu tez çalışması için gerçekleştirilen uygulamalarda kullanılan veri seti ile ilgili bilgilere yer verilmiştir. Veri seti özellikleri, kuralları ve örnekleri anlatılmıştır. Bu tez çalışmasındaki uygulamalarda kullanılan akıllı yöntemlerden YSA ve AÖM hakkında gerekli bilgilere yer verilmiştir. Uygulamaların doğruluğunu ölçmek için kullanılan k-katlı çapraz geçerlilik testi ile ilgili gerekli bilgilere yer verilmiştir.

Bölüm 4'te, bu tez çalışması için genel bir sistem mimarisi sunulmuştur.

Bölüm 5'te, tez çalışmasında kullanılan veri seti için oluşturulan kuralların ikisi için yeni kurallar önerilmiş ve anlatılmıştır.

Bölüm 6'da, YSA ile web tabanlı oltalama saldırısının tespiti konusu anlatılmış ve uygulama sonucuna yer verilmiştir.

Bölüm 7'de, AÖM ile web tabanlı oltalama saldırısının tespiti konusu anlatılmış ve uygulama sonucuna yer verilmiştir.

Bölüm 8'de, sonuçlar ve öneriler sunulmuştur. Sonuçlar kısmında bu tez çalışması için gerçekleştirilen iki uygulama sonucuna yer verilmiştir. Tez çalışmasında kullanılan veri seti için önerilen kurallar belirtilmiştir. Öneriler kısmında kurumsal bilgi güvenliğine yönelik bazı öneriler sıralanmıştır.

Kaynaklar bölümünde ise bu tez çalışmasında faydalanılan kaynaklar sıralanmıştır. Toplam 95 kaynak kullanılmıştır.

Bu tez çalışmasından 2 uluslararası bildiri yapılmıştır. Bir uluslararası hakemli dergi yayını hazırlanmış ve değerlendirilmek üzere dergiye gönderilmiştir.

1.3 Kaynak Özetleri

Bilgi ve iletişim teknolojisinin gelişmesi ile beraber bilgi güvenliğine yönelik tehditler çeşitli türlerde görülebilmektedir. Bu tehditlerin kişiye veya kuruma vereceği zararların önlenmesi, bilgisayar sistemlerindeki verileri koruma adına önem arz etmektedir. Literatür incelemesi yapıldığında siber tehditlere karşı bu bölümde de görüleceği üzere çeşitli siber savunma yöntemleri üzerinde çalışmaların yapıldığı gözlemlenmektedir. Bu çalışmalarda makine öğrenmesi tekniklerinin de kullanılabildiği görülmektedir. Verimli bir oltalama web sayfası algılayıcı [6], oltalama tespiti için web sitesi logosunun kullanımı [7] örnek olarak verilebilir.

Singh vd [8] tarafından yapılan çalışmada saldırı tespiti için Online Sequential Extreme Learning Machine (OS-ELM) denilen bir teknik sunulmuştur. Önerilen tekniğin performansını değerlendirmek için Network Security Laboratory-Knowledge Discovery and Data mining (NSL-KDD) 2009 veri seti kullanılmıştır. İkili sınıf NSL-KDD veri seti için deneysel sonuçlarda 2,43 s'lik tespit süresinde %1,74 yanlış pozitif oranı ile %98,66 doğruluğa ulaşılmıştır. Çoklu sınıf NSL-KDD veri seti için önerilen Saldırı Tespit Sistemi (STS) (Intrusion Detection System (IDS)) deneysel sonuçlarında 2,65 s'lik tespit süresinde %1,74 yanlış pozitif oranı ile %97,67 doğruluğa ulaşılmıştır. Kyoto Üniversitesi veri seti için önerilen STS deneysel sonuçlarında %5,76 yanlış pozitif oranı ile %96,37 doğruluğa ulaşılmıştır.

Fossaceca vd [9] tarafından yapılan çalışmada saldırı sınıfları örnek verileri üzerinde bir yapı geliştirilmiştir. Çalışma için ML platformu olarak AÖM kullanılmıştır. Oluşturulan sistem, Multiple Adaptive Reduced Kernel Extreme Learning Machine (MARK-ELM) olarak adlandırılmıştır. Bu yaklaşım, çeşitli ML veri setleri üzerinde test edilmiştir. Bu veri setlerinden biri olarak saldırı tespiti için KDD (Knowledge Discovery and Data mining) Cup 99 veri seti kullanılmıştır. Yapılan çalışmaların sonucunda MARK-ELM yaklaşımının UCI (University of California, Irvine) Makine Öğrenmesi Deposu küçük veri setlerinin çoğu için iyi, daha büyük veri setleri içinse ölçeklenebilir olduğu ifade edilmiştir. UCI veri seti için ulaşılan performansın, Multiple Kernel Boost Destek Vektör Makinesi (MKBoost DVM) (MKBoost Support Vector Machine (SVM)) ile benzer olduğu söylenmiştir. Deneysel sonuçlarda MARK-ELM'nin saldırı tespit verileri üzerinde diğer yaklaşımlara göre üstün tespit oranlarına ulaştığı ve çok daha düşük yanlış alarm oranlarına ulaştığı söylenmiştir.

Wang vd [10] tarafından yapılan çalışmada anomali tespiti üzerine bir çalışma yapılmıştır. AÖM tabanlı bir algoritma önerilmiştir. Bu algoritma, L1-Norm Minimization ELM olarak adlandırılmıştır. Değerlendirme aşamasında ham veriler bir ön işlemden geçirilmiştir. Bu veriler Birleşik Devletler ile Japonya arasındaki Pasifik ötesi omurga bağlantısından elde edilmiştir. Bu şekilde 248 özellik içeren bir veri seti oluşturulmuştur. Deneysel çalışmada L1-ELM'nin değerlendirme veri setleri üzerinde iyi genelleme performansı gösterdiği ifade edilmiştir.

Pereira vd [11] çalışmalarında Optimum-Path Forest (OPF) olarak adlandırdıkları yeni bir örüntü tanıma yöntemi geliştirmişlerdir. Yaptıkları çalışmayla şu konularda katkıda bulunmuşlardır: Saldırı tespiti için OPF'yi uygulamak, bazı genel veri setlerindeki fazlalıkları tespit etmek ve bunların üzerinde özellik seçimi gerçekleştirmek. Yapılan bazı testler sonucunda OPF'nin en hızlı sınıflandırıcı olduğu gösterilmiştir. OPF'nin bilgisayar ağlarında saldırı tespiti için uygun bir araç olduğu ifade edilmiştir. OPF algoritmasının yeni saldırıları öğrenmek için diğer tekniklerden daha hızlı olduğu söylenmiştir [5].

Herrero vd [12] çalışmalarında yeni bir Hibrit Akıllı Saldırı Tespit Sistemi geliştirmişlerdir. Bu sistemi Real Time - MObile VIsualisation Connectionist Agent-Based – Intrusion Detection System (RT-MOVICAB-IDS) ifadesi ile isimlendirmişlerdir. Bu sistemin en önemli amaçlarından biri gerçek-zamanlı saldırı tespitini kolaylaştırmak olarak ifade edilmiştir. Gerçek veri setleri kullanılarak sunulan deneysel sonuçlar bu yeni Hibrit STS'nin performansını doğrulamıştır [5].

Wang vd [13] yaptıkları çalışma ile davranışsal imzalara dayalı bir Destek Vektör Makinesi (DVM) (Support Vector Machine (SVM)) sınıflandırıcı eğitimi ile otomatik bir zararlı yazılım tespit sistemi geliştirmişlerdir. Sınıflandırmadaki doğruluk problemlerini çözebilmek için çapraz bir doğrulama düzeni kullanmışlardır. Bunun için DVM'ler ile ilişkili 60 gerçek zararlı yazılım kümesi kullanmışlardır. Deneysel sonuçlar ile test verilerinin boyutu arttığında sınıflandırma hatasının azaldığı gösterilmiştir. Zararlı yazılım örneklerinin farklı boyutları için zararlı yazılım tespiti tahmin doğruluğunun %98,7'ye ulaştığı görülmüştür. DVM sınıflandırıcının belirsiz mobil zararlı yazılım için genel tespit doğruluğunun % 85'ten fazla olduğu görülmüştür [5].

El-Emam vd [14] tarafından yapılan çalışma ile renkli görüntülere büyük miktarda gizli mesajı verimli bir şekilde gizlemek için zeki bir hesaplama yöntemi geliştirilmiştir. Bu yöntem için Non-Uniform Adaptive Image Segmentation

(NUAIS) kullanılarak yeni bir steganografi algoritması önerilmiştir. Saldırganlar tarafından yapılabilecek olan istatistiksel ve görsel saldırılara karşı direnci artırmak için dört güvenlik katmanı tanıtılmıştır. Yapılan deneysel sonuçlar daha önce yapılan steganografi algoritmaları ile karşılaştırılmıştır. Çalışmada, önerdikleri algoritmanın verimli olduğunu göstermişlerdir [5].

Singh vd [15] tarafından yapılan çalışmada Hadoop, Hive ve Mahout gibi açık kaynak araçlarından faydalanılmıştır. Çalışma ile bir STS uygulaması gerçekleştirme amaçlanmıştır. STS uygulaması, makine öğrenme yaklaşımı kullanılarak eşten eşe botnet saldırılarının tespit edilmesi için kullanılmıştır [5].

Mukherjee vd [16] tarafından yapılan çalışma ile azaltılmış giriş özelliklerini belirlemenin STS oluşturmadaki önemi araştırılmıştır. Bunun için standart olan 3 farklı özellik seçim yönteminin başarımları kullanılmıştır. Çalışmada azaltılmış giriş özellikleri için bir yöntem önerilmiştir. Bunun için verimli sınıflandırıcılardan Naive Bayes uygulanmıştır. Deneysel sonuçlarda azaltılmış özelliklerin STS inşası için daha iyi başarım sağladığı gözlenmiştir [5].

Wang vd [17] tarafından yapılan çalışmada anomali tespiti için bir plan çerçevesi sunulmuştur. Ağ tomografisi olarak adlandırılan bir sistem kullanılmıştır. Bu sistemin uçtan uca ölçümlerde iç bağlantı başarımını incelemek için yeni bir yöntem olduğu ifade edilmiştir. Önerilen sistemin etkinliği, yapılan kapsamlı deneyler ile doğrulanmıştır [5].

Chan vd [18] tarafından yapılan çalışmada bilinen saldırı örneklerini ayırmada bir bulanık ilişki kuralı modeli öngörüsü amaçlamış ve anomaliler geliştirilmiştir. Modelin tespit veya tahmin oranının %100'e yakın ve yanlış alarm oranının %1'den düşük olduğu ifade edilmiştir. Rasgele Orman kullanan modelin sınıflandırma doğruluğunun Root Mean Squared Error (RMSE) ile 0,02'ye yaklaştığı görülmüştür. Oluşturulan yeni bulanık ilişki kuralı yönteminin güvenlik koruma katmanı olarak yararlı olacağı ifade edilmiştir [5].

Suarez-Tangil vd [19] yaptıkları çalışmanın Security Information and Event Management (SIEM) ile ilişkisini sunmuşlardır. Bunun için bir ilişki motoru geliştirilmiştir. Geliştirilen motorun çok adımlı saldırıların farklı tipleri üzerinde otomatik olarak öğrendiği ve koşula dayalı ilişki kurallarını ürettiği ifade edilmiştir. Saldırı için kurulan ilgili koşula göre olayları sınıflandırmak için bir dizi YSA eğitilmiştir. Çalışmanın doğrulanması için yapılan deney Open Source Security Information Management (OSSIM) sistemi üzerinde gerçekleştirilmiştir [5].

Baykara vd [20] tarafından yapılan çalışmada günümüzde yaygın bir kullanım alanına sahip olan güvenlik araçları detaylı bir şekilde incelenmiştir. Bu araçların kullanım alanları ve fonksiyonları gibi birçok özellik göz önüne alınarak 22 dal altında sunulmuştur. Ayrıca kişileri, kurumları ve kuruluşları ilgilendiren bilgi sistemlerinin güvenliklerini sağlamak için bir dizi çözüm önerileri sunulmuştur. Bilgi sistemleri güvenliği ile ilgili çeşitli güvenlik önlemleri, güvenlik araçları ve güvenlik politikaları sunulmuştur. Kişisel ya da kurumsal açıdan ihtiyaç olan temel güvenlik stratejileri açıklanmıştır.

Kartal vd [21] tarafından yapılan çalışmada IPv6 (Internet Protocol version 6) protokolünün yapısı, güvenlik ilkeleri ve getirdiği yenilikler anlatılmıştır. IPv6 ile IPv4 (Internet Protocol version 4) protokollerinin benzer ve farklı yönlerine değinilmiştir. Günümüze kadar gerçekleşen güvenlik açıkları sunulmuştur. Karşılaşılabilecek olumsuz durumlar anlatılmıştır. Sonuç olarak genel öneriler sunulmuştur.

Ertam vd [22] tarafından yapılan çalışmada, ağ güvenliğini artırabilmek ve ağ adli bilişimi incelemelerini basitleştirmek amacıyla ağ cihazlarında yapılması gereken yapılandırma ayarları anlatılmıştır.

Şentürk vd [23] tarafından yapılan çalışmada siber güvenlik ile ilgili beş alandaki akademik çalışma incelenmiştir. Bu beş alanı siber güvenlik yatırım kararlarının verilmesi sürecinde uygulanabilecek yatırım stratejileri, siber güvenlik risklerinin belirlenmesi ve ölçülmesi, güvenlik saldırılarının maliyet ve etkisinin ölçülmesi, güvenlik teknolojilerinin etkinliğinin ölçülmesi ve güvenlik yatırımlarının en uygun seviyesinin belirlenmesi olarak belirlemişlerdir. İncelenen çalışmaların son on beş yıldaki çalışmaları kapsadığı söylenmiştir. Belirlenen beş alan ile ilgili olarak literatürdeki eksik noktalara değinilmiştir. Yapılan çalışma ile sonraki araştırmalara yol gösterilmesi hedeflenmiştir.

Can vd [24] tarafından yapılan çalışmada YSA temelli bir STS tasarlama hedeflenmiştir. Geliştirilen sistem, KDD (Knowledge Discovery and Data mining)'99 verileri ile test edilmiştir. Önerilen sistemin performansının oldukça yüksek olduğu tespit edilmiştir.

Yılmaz vd [25] tarafından yapılan çalışmada teknolojik gelişmeyle beraber küreselleşme ile ilgili güvenlik endişelerinin belirmesi konusu araştırılmıştır. Bilgi toplumu stratejisi konusu, ülkemizde uygulanan boyutu ile ele alınmıştır. Bilgi toplumuna geçiş aşamasında dünyanın ve ülkemizin durumu araştırılmıştır. Kritik

altyapı sistemlerini oluşturan bilgi teknolojileri incelenmiştir. Kritik altyapı sistemlerine yönelik olan siber tehditler araştırılmıştır. Ayrıca bu kritik altyapı sistemlerinin risk analizi incelenmiştir.

Ceyhan vd [26] tarafından yapılan çalışmada kablosuz algılayıcı ağlar ile ilgili olarak bir araştırma yapılmıştır. Kablosuz algılayıcı ağların yapısı, ana çalışma konuları, güvenlik hedefleri, maruz kaldıkları ağ saldırıları, güvenlik protokolleri, güvenli yönlendirme, güvenli hizmet modelleri incelenmiştir. Kablosuz algılayıcı ağlarda güvenliği sağlayabilmek amacıyla çeşitli çözümler öneren akademik çalışmalar incelenmiştir. İncelenen bu akademik çalışmalardaki kablosuz algılayıcı ağlar ile ilgili güvenlik açıklıkları belirtilmiştir. Kablosuz algılayıcı ağ güvenliğinin sağlanması için yapılması gerekenlerle ilgili çalışmalar özet şeklinde sunulmuştur. Yapılan çalışma sonucunda elde edilen bulgular açıklanmıştır.

Saied vd [27] tarafından yapılan çalışmada gerçek zamanlı ortamda bilinen ve bilinmeyen dağıtılmış hizmet engelleme (Distributed Denial of Service (DDoS)) saldırılarını tespit etme ve azaltma amaçlanmıştır. DDoS saldırılarını tespit etmek için DDoS saldırı trafiğini gerçek trafikten ayıran belirli karakteristik özelliklere (örüntülere) bağlı bir YSA algoritması seçilmiştir.

Grzonka vd [28] tarafından yapılan çalışmada, güvenlik odaklı grid zamanlayıcıların yeni bir modeli tanımlanmıştır. Bu model, bir YSA ile desteklenmiştir. YSA modülü tarafından zamanlama yürütmeleri izlenmiştir. Bu modül ayrıca güvenli görev-makine eşleştirmelerini öğrenmiştir. YSA modülü tarafından bu öğrenme için makine hataları gözlenmiştir. Sonra, metasezgisel (metaheuristic) grid zamanlayıcılar (yapılan çalışmada-genetik tabanlı zamanlayıcılar), YSA tarafından desteklenmiştir. Bu destekleme, alt-optimum zamanlamaların entegrasyonuyla geçekleşmiştir. Bu alt-optimum zamanlamalar, zamanlamaların genetik popülasyonuyla, sinir ağları tarafından üretilmiştir. Genel zamanlayıcıların başarımı üzerinde YSA desteğinin etkisi incelenmiştir. Bu incelemeler, grid ağlarının (küçük, orta, büyük ve çok büyük gridler), dört tipi için yapılan deneyleri kapsamıştır. İki riskli ve güvenli mod güvenlik zamanlayıcı senaryosu ile altı genetik tabanlı grid zamanlayıcı üzerinde çalışılmıştır. Üretilen deneysel sonuçlar, yapılan izleme desteğinin yüksek etkinliğini göstermiştir. Deneysel sonuçlar, başlıca zamanlama ölçütlerinin (tamamlanma zamanı ve akış zamanı) değerlerini azaltması kapsamında incelenmiştir. Sonuçlar, zamanlayıcıların çalışma zamanları ve grid kaynak hataları açısından gözlenmiştir.

Santhana Lakshmi vd [29] tarafından yapılan çalışmada tahmin görevi modellemesi ve danışmanlı ML algoritmaları yani Çok Katmanlı Algılayıcı (ÇKA) (Multi Layer Perceptron (MLP)) için ML yöntemi kullanılmıştır. Sonuçları incelemek için Karar Ağacı (KA) (Decision Tree (DT)) tümevarım ve Naive Bayes (NB) sınıflandırma kullanılmıştır. KA sınıflandırıcının, diğer öğrenme algoritmalarıyla karşılaştırıldığında, oltalama web sitesini daha doğru tahmin ettiği gözlenmiştir.

Olivo vd [30] tarafından yapılan çalışmada oltalama tespit motoru için güvenilirlik, iyi bir performans ve esneklik sağlayan ilgili özelliklerin minimum kümesini üreten bir yöntem önerilmiştir. Oltalama karşıtı düzenin tespit motorunu optimize etmek için önerilen yöntemin kullanılabilir olduğu yapılan çalışmada rapor edilen deneysel sonuçlar ile gösterilmiştir.

Islam vd [31] tarafından yapılan çalışmada oltalama eposta filtreleme için çok katmanlı sınıflandırma modeli olarak adlandırılan yeni bir yaklaşım önerilmiştir. Mesaj başlığının ve mesaj içeriğinin önemine dayalı oltalama epostanın özelliklerini çıkarmak ve öncelik sırasına göre özellikleri seçmek için yenilikçi bir yöntem önerilmiştir. Çok katmanlı bir sınıflandırma işleminde optimum zamanlamayı bulmak için sınıflandırıcı algoritmaları ertelemesinin etkisi incelenmiştir. Detaylı bir deneysel başarım ve önerilen algoritmanın analizi sunulmuştur. Deneylerin sonuçlarında, önerilen algoritmanın önemli ölçüde daha düşük karmaşıklık ile yanlış pozitif sorunlarını azalttığı görülmüştür.

Chen vd [32] tarafından yapılan çalışmada oltalama saldırılarının şiddeti, hedeflenen firmalar tarafından piyasa değerinde yaşanan risk seviyeleri ve potansiyel kayıpları açısından değerlendirilmiştir. Ortak veritabanı üzerinde yayımlanan 1030 oltalama uyarısı ile hedeflenen firmalarla ilgili finansal veriler melez bir yöntem kullanılarak analiz edilmiştir. Saldırının şiddeti, metinden ifade çıkarma ve danışmanlı sınıflandırma kullanılarak %89 doğruluğa kadar tahmin edilmiştir. Yapılan araştırma ile bazı önemli metinsel ve finansal değişkenler tanımlanmıştır. Saldırıların şiddeti ve potansiyel finansal kaybın etkisi araştırılmıştır.

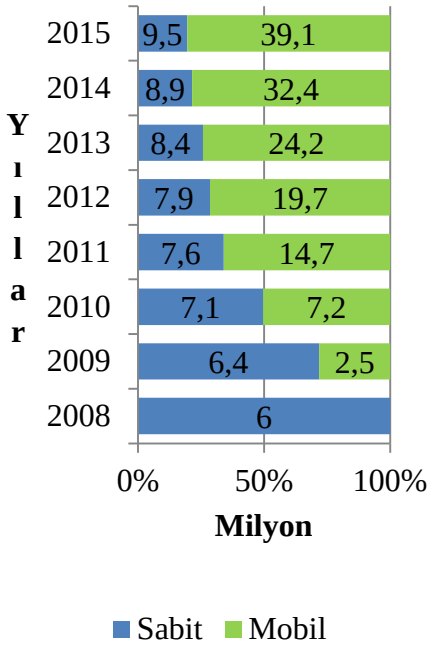
Li vd [33] tarafından yapılan çalışmada oltalama web sitesi tespiti için asgari kapsayan top destek vektör makinesi (minimum enclosing ball support vector machine (BVM)) tabanlı yeni bir yaklaşım önerilmiştir. Bu yaklaşım ile oltalama web sitesi tespiti için yüksek hız ve yüksek doğruluk sağlama amaçlanmıştır. Özellik vektörleri bütünlüğünü artırmak amacıyla çalışmalar yapılmıştır. Öncelikle Belge

Nesne Modeli (Document Object Model (DOM)) ağacına göre web sitesinin topoloji yapısının bir analizi yapılmıştır. Sonra web sitesinin 12 topolojik özelliğini çıkarmak için web crawler kullanılmıştır. Daha sonra, BVM sınıflandırıcı tarafından özellik vektörleri tespit edilmiştir. Önerilen yöntem, genel DVM ile karşılaştırılmıştır. Önerilen yöntemin nispeten yüksek tespit hassasiyetine sahip olduğu görülmüştür. Ayrıca önerilen yöntemin büyük ölçekli veriler üzerinde yakınsamanın yavaş hızının dezavantajını tamamladığı görülmüştür. Deneysel sonuçlarda önerilen yöntemin DVM'den daha iyi başarıma sahip olduğu görülmüştür. Önerilen sistemin doğruluğu ve geçerliliği değerlendirilmiştir.

Gowtham vd [34] tarafından yapılan çalışmada meşru ve oltalama web sayfalarının özellikleri derinlemesine araştırılmıştır. Yapılan analizlere dayalı olarak benzer türdeki web sayfalarından 15 özelliği çıkarmak için sezgiseller önerilmiştir. Önerilen sezgisel sonuçlar, oltalama siteleri tespit etmek için eğitilmiş bir makine öğrenmesi algoritmasına bir giriş olarak beslenmiştir. Oluşturulan sistemde, web sayfalarına sezgiseller uygulanmadan önce, iki ön tarama modülü kullanılmıştır. Ön onaylı site tanımlayıcı olan ilk modül ile kullanıcı tarafından korunan özel beyaz bir listeye karşı web sayfaları denetlenmiştir. Giriş formu bulucu olan ikinci modül ile de giriş formları bulunmadığı zaman web sayfaları meşru olarak sınıflandırılmıştır. Kullanılan modüller yardımıyla sistemdeki gereksiz hesaplama azaltılmıştır. Ayrıca kullanılan modüller ile yanlış negatif üzerinde ödün verilmeden yanlış pozitif oranı azaltılmıştır. Web sayfaları tüm modüller kullanılarak, %99,8 hassasiyetle ve %0,4 yanlış pozitif oranıyla sınıflandırılabilmiştir. Deneysel sonuçlar ile önerilen yöntemin kullanıcıları çevrimiçi kimlik saldırılarından korumak için verimli olduğu gösterilmiştir.

2. KURAMSAL TEMELLER

Tüm dünyada olduğu gibi ülkemizde de internetin kullanımı gittikçe artmaktadır. Şekil **2.1**'de [35] 2008 yılı ile 2015 yılı dördüncü çeyrek sonu arasındaki Türkiye'deki çevirmeli (dial up) internet hariç ve sabit, mobil, kablo, fiber vb. genişbant internet dahil olmak üzere genişbant internet abone sayısı gösterilmektedir. İnternetin kullanımının artması ile beraber bilişim sistemlerine yönelik saldırı ve saldırı türleri de artmakta ve bu saldırılara karşı da çeşitli savunma yöntemleri geliştirilmektedir.

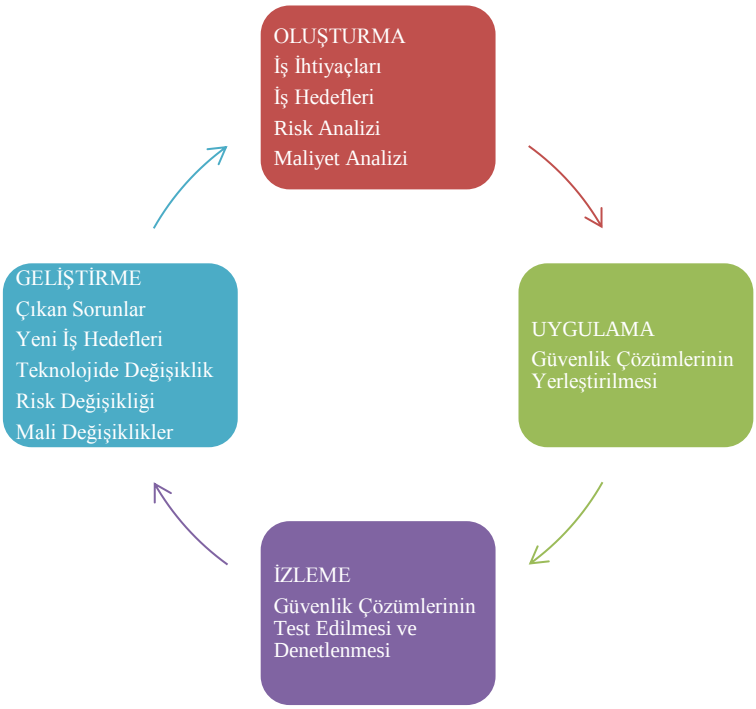


Şekil 2.1 Genişbant internet abone sayısı [35]

Bilgi güvenliğinin hedeflediği temel unsurlar gizlilik, bütünlük ve erişilebilirliktir. Bunların dışında kimlik sınaması, inkâr edilememe, güvenilirlik, kayıt tutma ve yetkilendirme unsurları da vardır. Bilgi güvenliğinin hedeflediği temel unsurlar Şekil **2.2**'de gösterilmektedir.

Şekil 2.2 Bilgi güvenliği temel unsurları.

Güvenlik politikaları, organizasyon ile ilgili dinamik kurallar şeklinde ifade edilebilir. Genel olarak bir organizasyonda bazı aşamaların işlemesi beklenmektedir. Yazılım yaşam döngüsü ile güvenlik politikası yaşam döngüsü birbirine benzetile bilinir. Şekil **2.3**'ten [36] de görüldüğü gibi güvenlik politikaları; oluşturma, uygulama, izleme ve geliştirme adımlarından oluşmaktadır. Güvenlik politikalarının oluşabilecek yeni risklere ve farklı ihtiyaçlara göre güncellenmesi gerekmektedir.



Şekil 2.3 Güvenlik politikası dört aşamalı yaşam döngüsü [36]

Bilgi sistemlerine yapılabilecek saldırılar farkı dallarda sınıflandırılabilir. Şekil **2.4**'te araç, kasıt, yol, hedef ve saldırgan olmak üzere beş farklı sınıflandırma ve bunlara bağlı olan alt sınıflandırmalara yer verilmiştir [37].

Şekil 2.4 Bilgi sistemlerine yönelik saldırıların sınıflandırılması [37]

2.1 Siber Saldırı Tehditleri

İnternet, çok sayıda ve sürekli genişlemekte olan, farklı yazılımları ve donanımları kullanan bilgi ve iletişim araçlarının yer aldığı bir ortam olarak düşünülebilir. Bilgisayar kullanımının artması toplumsal alanda büyük değişimlere

sebep olmuş ve hayatımızı çok kolaylaştırmıştır. İnternet'in geniş kitlelere ulaşması ile yeryüzünde coğrafi olarak bulunduğumuz yerden kaynaklanan bazı kısıtlamalar ortadan kalkmıştır. İnsanların her türlü bilgiye ulaşabildikleri yeni bir dünya oluşmuştur. Bu dünya kimi zaman sanal dünya, kimi zaman da siber uzay gibi terimlerle anılmaktadır. Siber uzayın merkezinin ve sınırlarının olmaması, ağ şeklindeki yapısından dolayı herhangi bir idarenin veya devletin elinde olmayışından hukuki ve uluslararası ilişkiler bakımından da o bireye veya o devlete verilecek bir ceza kararını almayı zorlaştırabilir. Bundan dolayı ulusal ve uluslararası alanda bu konunun teknik, sosyal, hukuki alanlarında daha iyi düzenlemeler yapılmalıdır. Söz konusu siber uzay olunca bu bir devletin fiziki sınırlarını aşıp başka bir devletin sınırları içerisine girmektedir [1].

Siber ortam, kara, deniz, hava ve uzay ortamlarından sonra gelen beşinci savaş alanı olarak düşünülebilir. Günümüzde neredeyse tüm bilgiler bilgi ve iletişim araçlarına depolanmakta ve çalıştırılmaktadır. Bilişim teknolojisindeki gelişmeler siber uzaydaki olanakları arttırıp kötü amaçlı kullanılmak istendiğinde insanları, kurumları ve devletleri tehdit eden bir konuma gelebilmektedir. Kurumlar bu beşinci ortam için savunma amaçlı hazırlıklar yapmalıdır. Siber savaş terimi şimdiye kadar net bir şekilde tanımlanamadığından dolayı siber savaşın gerçek bir savaş olup olmadığı ve dolayısıyla böyle bir sanal saldırı sonucunda saldırıyı yapan devlete karşı klasik anlamda bildiğimiz bir savaşın açılıp açılamayacağı tartışılabilir [1].

Bir saldırgan tarafından saldırı amacıyla çeşitli araçlar kullanılabilmektedir. Bu araçlar arasında, oltalama web sitesi, paket koklayıcı, casus yazılım, truva, solucan, hizmet engelleme ve virüs sayılabilir. Bu araçların dışında kullanıcılar da bir siber saldırı aracı olarak kullanılabilmektedir.

Bir kullanıcı ilgi çekici bir bağlantıya tıkladığında makinesini bir saldırganın denetimine vermiş olabilir. Saldırganın denetimini ele geçirdiği bu makine ciddi bir suçta kullanılabilir. Kullanıcı da bu suça aracılık etme ve ortak olma gibi bir duruma düşebilmektedir [38].

Türkiye'nin, siber saldırılar ve suçlar bakımından hedefteki ilk 10 ülke arasında olduğu ifade edilmiştir. Türkiye'nin, siber saldırı yapan ülkeler arasında ise ilk sıralarda olduğu söylenmiştir. Kamu kurumları başta olmak üzere kurumsal ve bireysel bazda siber güvenlik bakımından yeterli olabilecek bilgi, bilinç ve farkındalık aşamasına henüz erişilememiştir. 2013 ve 2014 yıllarında 30 kamu

kurumu, 27 üniversite, 2 telekomünikasyon şirketi, 13 sigorta şirketi ve 9 bankanın saldırganlar tarafından saldırıya uğradığı ifade edilmiştir [39].

Teknoloji sürekli bir şekilde gelişim göstermektedir. Benzer şekilde bilişim sistemlerine yapılan saldırı türleri de sürekli gelişmektedir. Bilgi iletişim sistemlerinde alınan güvenlik önlemleri gelişen teknolojiye karşı yetersiz kalabilmektedir. Bu bölümde siber saldırı tehditlerine yer verilmiştir.

2.1.1 Oltalama

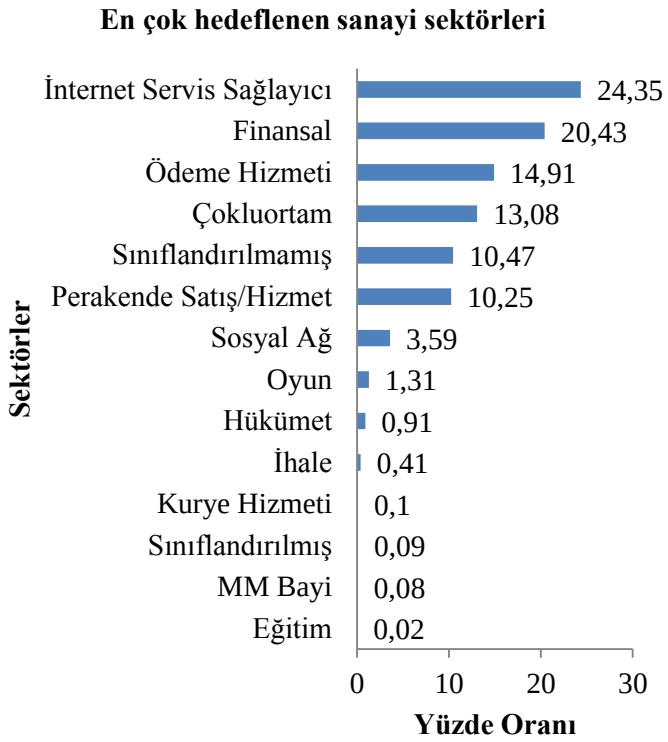
Oltalama (phishing) saldırısı üst sırada yer alan tehditlerden biri olduğundan [40] bu çalışmada ele alınmıştır. Tablo **2.1**'de [40] 2014 ve 2015 yıllarına ait tehditlere genel bakış ve bu tehditlerin karşılaştırılması gösterilmektedir.

Tablo 2.1 2014 ve 2015 yıllarına ait tehditlere genel bakış ve bu tehditlerin karşılaştırılması [40]

Sıralama	Üst Tehditler 2014	Eğilim 2014	Üst Tehditler 2015	Eğilim 2015	Sıralamada Değişim
1	Kötü niyetli kod: Solucanlar/Truvalar	▲	Kötü amaçlı yazılım	▲	■
2	Web tabanlı saldırılar	▲	Web tabanlı saldırılar	▲	■
3	Web uygulaması/ Enjeksiyon saldırıları	▲	Web uygulama saldırıları	▲	■
4	Botnetler	▼	Botnetler	▼	■
5	Hizmet reddi	▲	Hizmet reddi	▲	■
6	Spam	▼	Fiziksel hasar/ hırsızlık/ zarar	■	▲
7	Oltalama	▲	İçeriden tehdit (kötü niyetli, yanlışlıkla)	▲	▲
8	Exploit kitler	▼	Oltalama	■	▼
9	Veri ihlalleri	▲	Spam	▼	▼
10	Fiziksel hasar/ hırsızlık/ zarar	▲	Exploit kitler	▲	▼
11	İçeriden tahdit	■	Veri ihlalleri	■	▼
12	Bilgi sızması	▲	Kimlik hırsızlığı	■	▲
13	Kimlik hırsızlığı/ Dolandırıcılık	▲	Bilgi sızması	▲	▼
14	Siber casusluk	▲	Fidye yazılımı	▲	▲
15	Fidye yazılımı/ Dolandırıcılık yazılımı/ Korkutma yazılımı	▼	Siber casusluk	▲	▼
Gösterge: ▲Artma, ▼Azalma, ■Sabit					

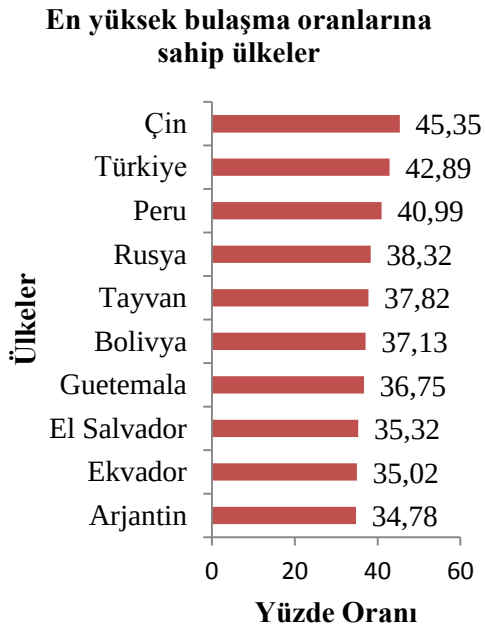
Şekil 2.5'te [41] 2015 yılı 3. çeyreğine ait oltalama saldırılarına en çok maruz kalan sanayi sektörleri yer almaktadır. Şekilden de görüleceği gibi oltalama

saldırılarının hedeflediği sektörlerin başında %24,35 ile İnternet Servis Sağlayıcı sektörü yer alırken 2. sırada %20,43 ile finansal sektör yer almaktadır.



Şekil 2.5 2015 yılı 3. çeyreğine ait oltalama saldırılarına en çok maruz kalan endüstri sektörleri [41]

Şekil 2.6'da [41] 2015 yılı 3. çeyreğine ait oltalama saldırılarında en yüksek bulaşma oranına sahip ülkeler yer almaktadır. Şekilden de görüleceği gibi oltalama saldırılarının bulaşma oranı en yüksek olan ülke %45,35 ile Çin olurken, Türkiye ise %42,89 ile 2. sırada yer almaktadır.



Şekil 2.6 2015 yılı 3. çeyreğine ait oltalama saldırılarında en yüksek bulaşma oranına sahip ülkeler [41]

2.1.2 Paket koklama

Paket koklama (packet sniffing) saldırısı ağa yapılan saldırılar içerisinde en kolay olan saldırı türlerinden biri olarak değerlendirilebilir. Ağ üzerindeki paketlerin yakalanması, izlenmesi ve incelenmesi işlemi koklama olarak adlandırılır. Bu işlem için ağ cihazları ve bilgisayarlar ile kablolu veya kablosuz bağlantı kurularak paket izleme programı kullanılır. Koklama işlemi iyi veya kötü niyetli kullanılabilir. Ağ üzerindeki saldırıların tespit edilebilmesi, paketlerin verimli bir şekilde alınması ve gönderilmesi amacı ile kullanılabilir. Bunun aksine ağ üzerindeki paketler ele geçirilip şifrelenmemiş veriler üzerinde inceleme de yapılabilir. Bu şekilde kişisel bilgilere ulaşılabilir.

Bazı paket koklama araçları [42]:

TCPdump,

Ethereal,

Net2pcap,

Snoop,

Angst,

Ngrep,
Ettercap,
Dsniff,
Cain and Abel,
AIM Sniffer,
TCPtrace,
TCPtrack,
Nstreams,
Argus,
Karpski,
IPgrab,
Nast,
Aldebaran,
ScoopLM,
Gulp,
Libpcap,
Nfsen,
Nfdump.

2.1.3 MAC aldatmacası

Bütün makinelerdeki ağ bağdaştırıcılarında var olan, benzersiz, 48 bit'ten oluşan fiziksel adres numarası MAC (Media Access Control) olarak adlandırılır. Ağ kartının orijinal MAC adresi yerine farklı MAC adresi gösterme yöntemi ise MAC aldatmacası (MAC spoofing) olarak adlandırılır. MAC aldatmacası işlemi farklı amaçlar için gerçekleştirilebilmektedir. Bir makinenin diğer bir makineyi taklit etmesi veya ağda gizlenmesi gibi değişik amaçlar için kullanılabilmektedir.

2.1.4 IP aldatmacası

Bir ağ üzerinde veri iletimi yapılırken hedef makineye, kaynak makinenin IP (Internet Protocol) adresinin farklı gösterilmesi işlemi IP aldatmacası (IP spoofing) olarak adlandırılır. Saldırgan, DoS (Denial of Service) saldırısında gerçek IP adresini gizleyerek kendisinin tespit edilmesini güçleştirebilmektedir.

2.1.5 DNS zehirlenmesi

ARP zehirlenmesi (ARP poisoning) ile DNS (Domain Name System) zehirlenmesi (DNS poisoning) birbirine benzer yapıdaki saldırı türleridir. IP numaraları ile etki alanı adlarının eşleştirildiği tablolar DNS sunucularında yer alır. Bir saldırgan tarafından bu tablolarda değişiklik yapılabilir. Saldırgan tarafından bir etki alanı adına ayrılmış olan IP adresi değiştirilebilir. Bu şekilde bir kullanıcı IP adresi değiştirilmiş olan etki alanı adı ile sunucuya bağlanmak yerine saldırganın sunucusuna yönlendirilmiş olur.

2.1.6 ARP zehirlenmesi

ARP (Address Resolution Protocol) zehirlenmesi (ARP poisoning), ağ izlemede kullanılan bir yöntemdir. Switch kullanan yerel bir ağda ortadaki adam olarak bilinen Man In The Middle (MITM) saldırısında kullanılabilir. Hub cihazının kaynak makineden hedef makineye gönderdiği veriler tüm makineler tarafından görülebilmektedir. Fakat bu veriler sadece hedef makine tarafından işleme alınmaktadır. Switch cihazının kaynak makineden hedef makineye gönderdiği veriler tüm makineler tarafından görülememektedir. Bu veriler sadece hedef makine tarafından görülebilmekte ve işleme alınmaktadır. Bu işlem switch tarafından ARP tablosu kullanılarak gerçekleştirilir. ARP tablosunda MAC adresi ile IP adresi eşleştirmeleri yer almaktadır. ARP kullanılarak MAC ve IP dönüştürme işlemleri gerçekleştirilir. Saldırgan tarafından bu saldırı türünde ARP tablosu kullanılarak MAC ve IP eşleştirmelerinde değişiklik yapılır. Saldırgan tarafından kendi makinesinin MAC adresi ile belirlediği makinenin IP adresi eşleştirilir. Bu şekilde belirlenen makineye gitmesi gereken veriler saldırganın kendi makinesine gönderilir.

2.1.7 HTTP taşması

İnternet protokollerinden uygulama katmanında yer alan HTTP (Hyper Text Transfer Protocol), web sayfalarını sunmak amacı ile kullanılır. Saldırgan tarafından hedef makineye sürekli web sayfası isteği gönderilerek makinenin meşgul edilmesi sağlanır. Web sayfası isteklerine cevap verilebilmesi için gönderilen ve alınan veri miktarı önemlidir. HTTP ile iletilen bu veri miktarı yalnızca UDP (User Datagram

Protocol) ya da yalnızca TCP ile iletilen veri miktarına oranla daha fazladır. Bu veri miktarının fazla olmasından dolayı bu saldırı türü hedef makinenin kaynaklarını daha fazla sömürür. SYN taşması saldırısı bu saldırı türüne göre daha etkilidir. HTTP taşması saldırısı ile IP aldatmacası saldırısı birlikte gerçekleştirilemez. Çünkü HTTP, TCP'yi kullanmaktadır. TCP'yi kullanmak için de bağlantı kurulumu sağlanmalıdır.

2.1.8 SYN taşması

SYN (Synchronize) taşması (SYN flood), DoS saldırı türlerinden biridir. İki makine arasında TCP (Transmission Control Protocol) ile bir bağlantı gerçekleştirilir. TCP paketleri SYN ve ACK (Acknowledgement) bayraklarına sahiptir. Bu paketler makineler tarafından karşılıklı bir biçimde birbirlerine gönderilir. TCP'de bu aşamaya el sıkışma denilmektedir. Bu aşamada saldırgan paket iletimini sömürerek SYN taşması saldırısı gerçekleştirebilir. Saldırgan tarafından hedef makineye SYN bayraklı TCP paketi devamlı gönderilir. Hedef makine gelen her SYN bayraklı TCP paketine ACK bayraklı TCP paketi ile cevap vermeye çalışır. Belirli bir süre sonucunda hedef makine gelen isteklere cevap veremez. DoS saldırı türleri içerisinde en basit saldırı türlerinden biri olarak bilinmektedir.

2.1.9 ACK/FIN/PUSH taşması

Hedef makineye veri iletilirken TCP paketlerinin başlığında bulunan ACK (Acknowledgement), FIN veya PUSH bayrakları ayarlanır. Saldırgan tarafından bu paketler hedef makineye devamlı gönderilir. Saldırgan tarafından bu şekilde hedef makinenin kapasitesi zorlanmaya çalışılır. SYN taşması saldırısı ile başarılı olamayan saldırgan tarafından bu saldırı yöntemi kullanılabilir. SYN taşma saldırısı bu saldırı türünden daha etkilidir. Bu saldırı türünün engellenmesi kolaydır.

2.1.10 UDP taşması

Saldırgan tarafından hedef makineye devamlı UDP (User Datagram Protocol) paketleri gönderilir. UDP protokolünde oturum kurulumu bulunmamaktadır. Bundan dolayı saldırgan tarafından hedef makineye istenildiği kadar paket iletilebilir.

Saldırgan bu aşamada IP aldatma saldırısı da gerçekleştirebilir. Hedef makine kendisine gelen UDP paketinin ardından gelebilecek diğer paketler için bağlantıyı bir süre daha açık tutar. Saldırgan bu şekilde hedef makinede sürekli bir kaynak tüketimini gerçekleştirir. Belirli bir süre sonucunda hedef makinenin kapasitesinin üzerine çıkılır. Bu aşamadan sonra hedef makine gelen isteklere yanıt veremez bir duruma gelir.

2.1.11 DNS taşması

UDP (User Datagram Protocol) üzerinde çalışan bir DNS makinesi, saldırganların hedefi olabilir. Saldırgan bu saldırı türünde UDP üzerinden IP aldatmaca yöntemini kullanarak DNS istek paketlerini hedef makineye gönderebilir. Bu DNS istek paketleri belli bir sıra gözetilmeksizin ve devamlı bir şekilde hedef DNS makinesine gönderilir. Bu şekilde DNS makinesi saldırgan tarafından meşgul edilmiş olur.

2.1.12 İşletim sistemi tarama

Hedef makinedeki işletim sisteminin belirlenmesi işlemine işletim sistemi tarama (Operating System (OS) fingerprinting) denilmektedir. Bu işlemde hedef makinenin gönderdiği veriler üzerinde aktif ve pasif olarak inceleme yapılır. Bir saldırgan tarafından hedef makineye gönderilen veri paketlerine karşılık gelen veri paketleri üzerinde inceleme yapılabilir. Yapılan bu işlem aktif mod olarak adlandırılır. Bir saldırgan tarafından hedef makineye bağlanmadan yalnızca ağdaki veri paketleri üzerinde inceleme yapılabilir. Yapılan bu işlem pasif mod olarak adlandırılır. Saldırganın pasif mod ile işletim sistemi tarama saldırısı için kullandığı araç bir çeşit koklama aracı gibi işlev görebilir.

Bazı işletim sistemi tarama araçları [43]:
SinFP3,
Nessus.

Bazı fingerprinting araçları [42]:
Nmap,

P0f,
Xprobe,
CronOS,
Queso,
Amap,
Disco,
Sprint.

2.1.13 IP tarama

Ağdaki aktif makineleri bulma işlemi IP tarama (IP scanning) olarak adlandırılmaktadır. Ping scan yöntemi ile IP tarama yapılabilir. Bu yöntem ile saptanan IP adresine saldırgan tarafından ICMP (Internet Control Message Protocol) echo request paketi gönderilir. Saptanan IP adresi kullanılıyorsa ICMP echo reply paketi alınır. Güvenlik duvarı kullanan bazı makineler ping paketlerinin iletilmesini engelleyebilirler. Saldırgan bu durumda port tarama yöntemlerini kullanarak saldırı girişiminde bulunabilir.

Bazı ağ tarama araçları [42]:
Nmap,
Amap,
Vmap,
Unicornscan,
TTLscan,
IKE-scan,
Paketto.

2.1.14 Kod istismarı

Saldırganlar tarafından kod istismarı (code exploit) ile donanım veya yazılım sistemlerinde oluşan güvenlik açıklarından, aksamalarından veya hatalarından yararlanılabilir. Kod istismarı; bir komut dizini, bir veri yığını veya bir yazılım parçası ile gerçekleştirilebilir.

2.1.15 Virüs

Virüs (virus), kendini sistemdeki programlardan veya dosyalardan biri olarak değiştirebilen bilgisayar kodu olarak belirtilebilir. Bir kullanıcı tarafından ilgili program veya dosya çalıştırıldıktan sonra fark edilebilir. Bir kullanıcı tarafından gerekli denetimler yapılmadan USB (Universal Serial Bus)'nin otomatik olarak çalıştırılması veya bir kullanıcıdan gelen e-postanın açılması gibi farklı şekillerde etkili olabilmektedirler [44].

2.1.16 Solucan

Solucan (worm); ana makineye saldıran, ağ ile yayılabilen, kötü niyetli kod bulunduran bir program olarak ifade edilebilir. Solucanın kendi kendine yayılabilme özelliği, solucan ile virüs arasındaki farklardan biridir. Solucanlar, önyükleme bölümlerine ya da ana makine dosyalarına bağlı değildir. Solucanlar, uygulamalardaki güvenlik açıklarını veya e-posta listelerini kullanarak yayılabilirler. Bu özelliklerinden ötürü virüslerden daha fazla yaşayabilirler. İnternetin geniş çaplı kullanımından ötürü, kısa bir süre içerisinde dünya geneline yayılabilmektedirler. Hızlı ve bağımsız bir şekilde çoğalabilme yeteneklerinden dolayı, diğer kötü niyetli yazılımlardan daha tehlikelidirler. Bir sistemde etkinleştirildikleri zaman farklı türdeki bazı sıkıntılara yol açabilirler. Solucanlar tarafından programlar etkisiz duruma getirilebilir, sistem başarımı düşürülebilir ve dosyalar silinebilir. Solucan, diğer sızıntı tipleri için "taşıma yöntemi" görevi üstlenir [45].

2.1.17 Truva

Truva (trojan), yararlı gibi görünen, ancak diğer taraftan kötü amaçlı çalışarak önemli ve gizli bilgileri dışarıya ileten casus program olarak tanımlanabilir. Truva çalıştırılarak sistemde bir arka kapı açılabilir ve bu sayede saldırgana ait ve dışarıda olan makineyle iletişim kurulabilir. Bu şekilde bir saldırgan tarafından, kişisel belgeler, kredi kartı bilgileri, e-posta adresleri ve şifreler gibi yetkisiz bilgilere erişilebilmekte ve bu yetkisiz bilgiler kendi makinesine yönlendirilebilmektedir. Truvaların, virüslerin aksine kendilerini kopyalama özellikleri görülmemektedir. Truvanın aktif olabilmesi için öncelikli olarak çalıştırılması gerekmektedir [46].

Bazı truva araçları [42]:

NukeNabber,

AIMspy,

NetSpy.

2.1.18 Kök dizin

Kök dizin (rootkit), sistem yöneticisinin herhangi bir izni olmadan ve yasal olmayan bir şekilde bilgisayar sisteminin denetimini ele geçirmek amacıyla tasarlanmış bir program olarak tanımlanabilir. Donanım üzerinde çalışmakta olan işletim sisteminin denetimini sağlamayı hedeflemektedirler. Bu yüzden kök dizin tarafından donanımsal olarak bir erişime ihtiyaç duyulmamaktadır. İşletim sisteminin güvenlik ayarlarını değiştirerek veya ele geçirerek varlıklarını gizleyebilirler. Bir kök dizini, truva atı şeklinde de olabileceğinden, bir kullanıcıyı kendisinin güvenli olduğuna inandırabilir. Kök dizinin kullandığı teknikler arasında bilgisayardaki dosyaları gizleme, işletim sistemi sistem bilgilerini gizleme, izleme uygulamalarındaki çalışan işlemleri gizleme sayılabilir [47].

2.1.19 Hizmet engelleme

Hizmet engelleme (Denial of Service (DoS)) saldırısı ile saldırganlar tarafından bir ağ veya sistem iletişim kurulamaz duruma düşürülebilmektedir. Saldırganlar bu saldırıyı birden fazla yerden sistematik bir şekilde de gerçekleştirebilmektedirler. Bu şekildeki bir saldırı türü de dağıtılmış hizmet engelleme (Distributed DoS (DDoS)) saldırısı olarak adlandırılmaktadır.

Saldırganlar tarafından DoS veya DDoS saldırıları ile kaynakların tüketilip iletişimin engellenmesi amaçlanmaktadır. Bu saldırı türleri ile ilgili olarak yapılan çalışmaların büyük çoğunluğunun farklı tipteki ağ ve ağ katmanlarında DoS veya DDoS tespitine yönelik olduğu görülmektedir. Bu saldırı türleri ile ilgili olarak yapılan çalışmaların bir kısmının ise saldırı kaynağını doğru bir şekilde tespit etme ile ilgili olduğu görülmektedir. Yapılan çalışmalar içerisinde anomali tespiti temelli sistemler üzerine odaklananların çoğunlukta olduğu görülmektedir. Araştırmacılar tarafından farklı disiplinlerdeki yöntemler kullanılarak DoS veya DDoS saldırıları

tespit edilmeye çalışılmaktadır. Bu disiplinler arasında otomata teorisi, bilgi teorisi, doğa-esinli hesaplama, olasılık, veri madenciliği ve ML sayılabilir [48].

Bazı DDoS saldırı araçları [49]:
X Orbit Ion Canon (XOIC),
DDoS sIMulator (DDoSIM),
DDoS Attacks Via Other Sites Execution Tool (DAVOSET),
PyLoris.

Bazı DoS/DDoS saldırı araçları [42]:
Jolt,
Burbonic,
Targa,
Blast20,
Crazy Pinger,
UDPFlood,
FSMax,
Nemsey,
Panther,
Land & LaTierra,
Slowloris,
BlackEnergy,
HOIC,
Trinoo,
Shaft,
Knight,
Kaiten,
RefRef,
LOIC,
Hgod,
TFN,
TFN2K,
Stacheldrath,
Mstream,

Trinity.

2.1.20 CSRF

Siteler arası istek sahteciliği (Cross-Site Request Forgery (CSRF)) saldırısı ile bir kullanıcının e-posta hesabından e-posta gönderme, e-posta hesabının ayarlarını değiştirme, banka hesabından para gönderme işlemleri yapılabilmektedir. Bu saldırı, sitelerdeki bir güvenlik açığından faydalanmaktadır. Bu güvenlik açığı, uygulamayı geliştiren kişi tarafından, uygulamanın geliştirilme sürecinde, istemci makineden gelen isteklerin kullanıcıdan geldiğinin düşünülmesinden kaynaklanmaktadır. Kullanıcı tarafından, kendi oturum bilgisiyle web sayfasındaki işlemler yapılabilmektedir. Saldırganlar tarafından kullanıcının oturumunda araya girme veya oturum bilgisini kesme gibi saldırılar yapılabilmektedir [50].

2.1.21 Diğer bazı saldırı araçları

Bazı bilgi toplama araçları [42]:
ASS,
NMap,
p0f,
MingSweeper,
THC Amap,
Angry IP Scanner.

Bazı paket enjeksiyon araçları [42]:
Packeth,
Packit,
Packet Excalibur,
Nemesis,
Tcpinject,
Libnet,
SendIP,
IPsorcery,
Pacgen,

ARP-SK,
ARPspoof,
Libpal,
Aicmpsend.

Bazı kullanıcı saldırısı araçları [42]:
Yaga,
SQL attack,
Netcat,
ntfsdos.

Bazı ağ izleme araçları [42]:
Tnv,
Network Traffic Monitor,
Rumint,
EtherApe,
NetGrok,
NetViewer,
VizNet.

2.2 Siber Savunma Tedbirleri

Siber güvenlikte reaktif yaklaşım veya geleneksel yaklaşım anlayışı bir saldırı olduktan sonra gerekli önlemlerin alınması temeline dayanır. Proaktif yaklaşım veya çağdaş yaklaşım anlayışı ise bir saldırı olmadan gerekli önlemlerin alınması temeline dayanır. Kişi, kurum veya kuruluş olsun bilgi güvenliğinin sağlanması için proaktif önlemlerin alınması ve bu önlemler için de çeşitli araçların ve tekniklerin kullanılması gerekmektedir.

Bu bölümde siber savunma tedbirlerine yönelik olarak bazı araçlara ve yöntemlere değinilmiştir. Siber güvenliği sağlanma konusu çok geniş bir konu olduğu için belli başlı bazı konular ele alınmıştır.

2.2.1 Saldırı Tespit Sistemi

Saldırı Tespit Sistemi (STS) (Intrusion Detection System (IDS)) üzerinde önceden tanımlanmış saldırı imzaları vardır. STS'ler, saldırı imzasına uyan bir saldırıyı raporlayabilme özelliğine sahiptirler. STS'ler tarafından sistem yöneticisi saldırı anında uyarılabilir. STS'lerin ağdaki veri alış verişine engel olma gibi yetenekleri yoktur.

STS, bilgi sistemlerini korumada "alarm" özelliği taşır. Ağ üzerinden yapılabilecek saldırılara karşı kullanılır. Bir donanım veya yazılım bileşeni olabilir. STS ile bir sisteme yapılabilecek izinsiz erişim ve kötü amaçlı kullanım tespit edilebilir. Bu sayede bir saldırganın bir sisteme sızma girişimi önlenebilir. STS ile bir saldırganın profili, bir sistemde bulunan güvenlik açıkları ve saldırı türü gibi bilgiler elde edilebilir [51].

Bazı Saldırı Tespit Sistemleri [42]:

Automated Data Analysis and Mining (ADAM),

Minnesota Intrusion Detection System (MINDS),

Dependable Network Intrusion Detection System (DNIDS),

HIDE,

Network Self-Organizing Maps (NSOM),

Flow-based Statistical Aggregation Scheme for Network Anomaly Detection (FSAS),

Network at Guard (N@G),

Fuzzy Intrusion Recognition Engine (FIRE),

NFIDS,

D-WARD,

Large-scale Automated DDoS detection System (LADS),

ANTID,

DCD,

CERN Investigation of Network Behavior and Anomaly Detection (CINBDS),

NetSTAT,

Bro,

Snort,

PAYL,
ALERT-ID,
MAD-IDS,
ML-DIDS.

2.2.2 Saldırı Engelleme Sistemi

Saldırı Engelleme Sistemi (SES) (Intrusion Prevention System (IPS)), bir ağ üzerindeki farklı ağ bölümlerinde korumak istenen bölüme kurulabilir. Saldırı trafiğini engelleyebilme özellikleri vardır. Üzerlerinde önceden belirlenmiş saldırı imzaları bulunur. Ağ trafiği üzerinde bu saldırı imzaları ile eşleşen zararlı ağ trafiğini arayabilirler. Bu zararlı ağ trafiğini yakaladıklarında TCP iletişimi sonlandırma, paket düşürme gibi işlemleri yapabilirler. DoS ve DDoS saldırılarına karşı ağı koruyabilirler.

Bir sisteme yapılan saldırının yalnızca güvenlik duvarıyla tespit edilmesi ya da engellenmesi mümkün görülmemektedir. Bunun sebebi olarak güvenlik duvarının, üzerinden geçen paketleri incelememesi gösterilmektedir. Güvenlik duvarı yalnızca üzerindeki tablodaki kurallara bakıp bir paketin geçişine izin verebilir. Bundan dolayı gelen paketi inceleyebilen, gerekirse önceki paket ile bu paketi karşılaştırabilen, şüpheli bir durumda paket geçişine izin vermeyip sistemi koruyan farklı bir güvenlik uygulamasına ihtiyaç duyulmuştur. Ağ literatüründe bu işleri yapabilen uygulama IPS olarak adlandırılmaktadır [52].

2.2.3 Güvenlik duvarı

Temel ağ güvenliği sistemlerinden olan güvenlik duvarı (firewall) statik izleme yeteneğine sahiptir. Ağdaki veri akışı, tanımlı kurallara göre yapılıp erişim denetimi sağlanır. Tanımlı olan bu kurallar ile kurallar tablosu oluşturulur. Kurallar tablosu istenmeyen veri akışını engelleyebilir. Ağda farklı bölümler arasında erişim kuralları uygulanabilir. Güvenlik duvarları dış dünya ile iletişim kurarak bir kullanıcının şifreli iletişimde bulunabilmesini sağlarlar. Bu sayede veri gizliliği korumasına katkı sağlanmış olur.

2.2.4 Web uygulama güvenlik duvarı

IPS'in görevleri ile web uygulama güvenlik duvarı (web application firewall)'nın görevleri birbirine benzer yapılar olarak görülebilir. Web uygulama güvenlik duvarı üzerinde önceden belirlenmiş trafik imzalarının yer aldığı görülmektedir. Bu güvenlik duvarı türünün üretilmesinin sebebi web hizmetlerinin geniş çaplı bir kullanım alanına sahip olmasıdır. Bu güvenlik duvarları bir yazılımın geliştirilme aşamalarında gerekli tedbirlerin alınmadığı durumlar için ilave güvenlik tedbirleri alınmasında faydalı olabilmektedir. Bu güvenlik duvarları web sunucularına ve hizmetlerine yapılabilecek saldırıları engelleyebilirler.

2.2.5 Veritabanı güvenlik duvarı

Veritabanlarına yapılabilecek kötü niyetli müdahalelerin önlenebilmesi, gelen sorguların incelenebilmesi veri güvenliği açısından önem taşımaktadır. Bu amaçlar için veritabanı güvenlik duvarı (database firewall) kullanılabilir. Bu türdeki güvenlik duvarlarının kullanıcının genel davranış eğilimlerini öğrenebilme yetenekleri vardır. Bu davranış eğilimleri dışına çıkıldığında uyarı mesajı verebilen sistemlerdir. Web güvenlik duvarı ile veritabanı güvenlik duvarı beraber kullanılabilir. Bu şekilde kurulan bir sistem ile kullanıcıların webdeki faaliyetleri izlenebilir.

2.2.6 Ağ erişim denetimi

Ağ erişim denetimi (Network Access Control (NAC)) sistemleri ile bir organizasyonun iç ağına bir dış ağın eklenmesi engellenebilir. Bu engellemenin amacı güvenlik durumu eksik ya da bilinmeyen bir dış ağın iç ağı tehdit etmesinin önüne geçilmesidir.

2.2.7 Yük dengeleyici

Bilgi ve iletişim araçları üzerindeki ağ trafiğinin işlem hacmi çok yüksek düzeylere çıkabilmektedir. Yük dengeleyici tarafından ağdaki sunuculardan bazılarına gelen yoğun talepler, yoğunluğu daha az olan sunucular üzerinde paylaştırılarak denge sağlanmaya çalışılır. Örnek olarak yük dengeleyici tarafından

bir web sunucuya SSL (Secure Socket Layer) sonlandırma görevi verilebilir. Bu şekilde diğer sunucuların şifreleme işlemi yapmasına gerek kalmaz. Sonuç olarak başarım elde edilmiş olunur.

2.2.8 URL filtreleme

URL (Uniform Resource Locator) filtreleme (URL filtering), ağ üzerindeki istemci makinelerin internet erişim ayarlarının yapılması amacı ile kullanılır. Bazı web sitelerine erişimi kısıtlama veya erişime izin verme gibi işlemeler için kullanılırlar. URL filtreleme yazılımları vekil sunucu ile beraber çalışabilirler. Bu şekilde ağdaki trafik denetlenebilir ve zararlı olan yazılımlar üzerinde inceleme yapılabilir.

2.2.9 Vekil sunucu

Vekil sunucu (proxy server) yalnız kullanılabileceği gibi URL filtresi ile de kullanılabilir. Bu sunucular internetten aynı dosyanın birden fazla indirilmemesi için kullanılırlar. Bu sunucular tarafından internetten indirilen dosyalar saklandıklarından dolayı bant genişliği verimli bir şekilde kullanılmış olur.

2.2.10 Zafiyet tarama

Zafiyet tarama (vulnerability scanning) yazılımları, bir sistemdeki zayıflıkların tespitinde kullanılırlar. Bu türdeki yazılımlar bir organizasyondaki güvenlik politikalarına uymayan durumları tespit edebilirler. Sistemdeki eksik yamalar, çalışan uygulamalardaki ve işletim sistemindeki açıklıklar zafiyet tarama ile tespit edilebilir.

Bazı zafiyet tarama araçları [53]:
AVDS,
Patchlink scan,
Nessus,
NeXpose,
QualysGuard,

SAINT,
McAfee VM.

2.2.11 Risk analizi yönetim sistemi

Risk analizi yönetim sistemi (risk analysis management system) bir ağ modeli oluşturabilen bir yapı olarak düşünülebilir. Bu yapıyı oluşturabilmek için yönlendirici, switch ve güvenlik duvarı gibi aygıtların yapılandırma ayarları donanım bağlamında tespit edilebilir. Ayrıca bu yapıyı oluşturabilmek için sistem üzerinde kurulu olan zafiyet tarama yazılımı ile sistem açıkları yazılım bağlamında tespit edilebilir. Risk analizleri bu ağ modeli ile yapılır. Riskler öncelik durumuna göre sıralanır. Bu şekilde en yüksek riske sahip sistemler, kaynakların hangi durumlarda öncelikle kullanılması gerektiği ve bu kaynakların nerelerde kullanılması gerektiği gibi konular üzerinde gerekli bilgilere ulaşılmış olur.

2.2.12 Güvenlik bilgileri ve olay yönetimi

Güvenlik bilgileri ve olay yönetimi (Security Information and Event Management (SIEM)) sistemlerinin kayıt tutma ve ilişki kurma özellikleri vardır. Ağdaki farklı sistemlerin ve aygıtların çoğu tarafından kendileri ile ilgili olay kayıtları tutulabilmektedir. Bu kayıtlar çok farklı şekillerde tutulabilmektedir. Bu nedenle bu kayıtların ilişkilendirilmeleri çok zor olabilmektedir. SIEM sistemleri tarafından bu kayıtlar toplanıp ilişkilendirilebilmektedir. Normal olarak tespit edilemeyen güvenlik ile ilgili olaylar mantıksal kurallar ile tespit edilebilir.

2.2.13 Veri Kaçağı Önleme

Veri Kaçağı Önleme (Data Leakage Prevention (DLP)) sistemleri, önemli verilerin ağ içinden ağ dışına çıkartılmasını engelleyebilirler. Bu tür sistemlerin ağ ve istemci modelleri bulunabilmektedir. Bu sistemin bulunduğu bir istemcide veri kaçağının engellenebilmesi için cihazı denetleyen bileşenler bulunabilmektedir.

Bazı DLP araçları [54], [55]:
Triton (Websense),

Fidelis XPS (General Dynamics Fidelis Cybersecurity Solutions),
McAfee Data Loss Prevention (McAfee),
Check Point DLP (Check Point Software Technologies),
Varonis IDU Classification Framework (Varonis Systems),
AirWatch (VMware).

3. MATERYAL VE YÖNTEM

3.1 Veri Seti

Oltalama web siteleri veri seti ağırlıklı olarak PhishTank arşivi, MillerSmiles arşivi ve Google arama operatörlerinden toplanmıştır. Yapılan çalışmada karşılaşılan zorluklardan biri, güvenilir eğitim veri setlerinin bulunmaması olarak ifade edilmiştir. Bu zorluğun bu alanda çalışma yapmak isteyen herhangi bir araştırmacının karşılaştığı bir zorluk olduğu söylenmiştir. Son zamanlarda oltalama web siteleri tahmini ile ilgili birçok çalışma yapılmıştır. Buna rağmen şimdiye kadar güvenilir bir eğitim veri seti yayımlanmamıştır. Bunun olası nedeni olarak oltalama web sayfalarını tanımlayan belirleyici özellikler üzerinde bir görüş birliği sağlanamaması gösterile bilinir. Bu nedenle mümkün olan tüm özellikleri kapsayan bir veri seti oluşturmak oldukça zor görülmüştür. Veri setinde önemli özellikler üzerinde durulmuştur. Veri setinin oltalama web sitelerini tahmin etmede etkili olduğu kanıtlanmıştır. Veri setine ek olarak bazı yeni özellikler önerilmiştir [56].

Veri setinin ve kuralların oluşturulması ile ilgili olarak yapılan bazı çalışmalar [57], [58], [59] ile katkıda bulunulmuştur.

Bu tez çalışması için "oltalama web siteleri özellikleri" ve "eğitim veri seti" ile ilgili olmak üzere iki dosyadan faydalanılmıştır. Oltalama web sitesi özellikleri dosyasında, daha önce yapılan çalışmalara [57], [58], [59] ilave olarak bazı özellikler eklenmiş, bazı düzeltmeler yapılmıştır [60].

Tablo **3.1**'de [61] veri setine ait öznitelikler, sınıf ve değerler görülmektedir. Giriş veri seti toplam olarak 30 öznitelikten oluşmaktadır. Giriş veri seti öznitelikleri, oluşturulan kurallara göre 1, 0 veya -1 değerlerini alabilmektedir. Bu şekilde oluşturulan giriş veri setine ait öznitelikler 2 veya 3 farklı değer alabilmektedir. Çıkış veri setindeki sınıf 1 veya -1 değerlerini alabilmektedir. Bu şekilde elde edilen çıkış veri setine ait sonuçlar 2 farklı değer alabilmektedir.

Tablo 3.1 Veri setindeki öznitelikler, sınıf ve değerleri [61]

		Değerler		
Öznitelikler	IP_adresi	-1	1	
	URL_uzunluğu	1	0	-1
	kısaltma_servisi	1	-1	
	@_simgesi	1	-1	
	//_simgesi	-1	1	
	önek_sonek	-1	1	
	alt_etki_alanı	-1	0	1
	SSL_sertifikası	-1	1	0
	etki_alanı_kayıt_süresi	-1	1	
	favicon	1	-1	
	port	1	-1	
	HTTPS_simgesi	-1	1	
	URL_isteği	1	-1	
	URL_anchor	-1	0	1
	etiketlerdeki_bağlantılar	1	-1	0
	SFH	-1	1	0
	eposta_bilgi_gönderme	-1	1	
	anormal_URL	-1	1	
	yönlendirme	0	1	
	onMouseOver	1	-1	
	sağ_tıklama	1	-1	
	açılır_pencere	1	-1	
	iframe	1	-1	
	etki_alanı_yaşı	-1	1	
	DNS_kayıt	-1	1	
	web_trafiği	-1	0	1
	PageRank	-1	1	
	Google_index	1	-1	
	işaret_eden_bağlantılar	1	0	-1
	istatistiksel_rapor	-1	1	
Sınıf	sonuç	-1	1	

Veri setinde 11055 adet örnek bulunmaktadır. Tablo **3.2**'de [61] bu çalışmada kullanılan veri setindeki ilk 10 örnek gösterilmektedir. Tablodaki her bir satır veri setindeki bir örnek için gösterilmektedir. Bir satırda yer alan değerlerden ilk 30 değer ile giriş verileri yani öznitelikler temsil edilmektedir. Bir satırda yer alan değerlerden son değer ile de çıkış verileri yani sınıflandırma sonucu temsil edilmektedir.

Tablo 3.2 Veri setindeki ilk 10 örnek [61]

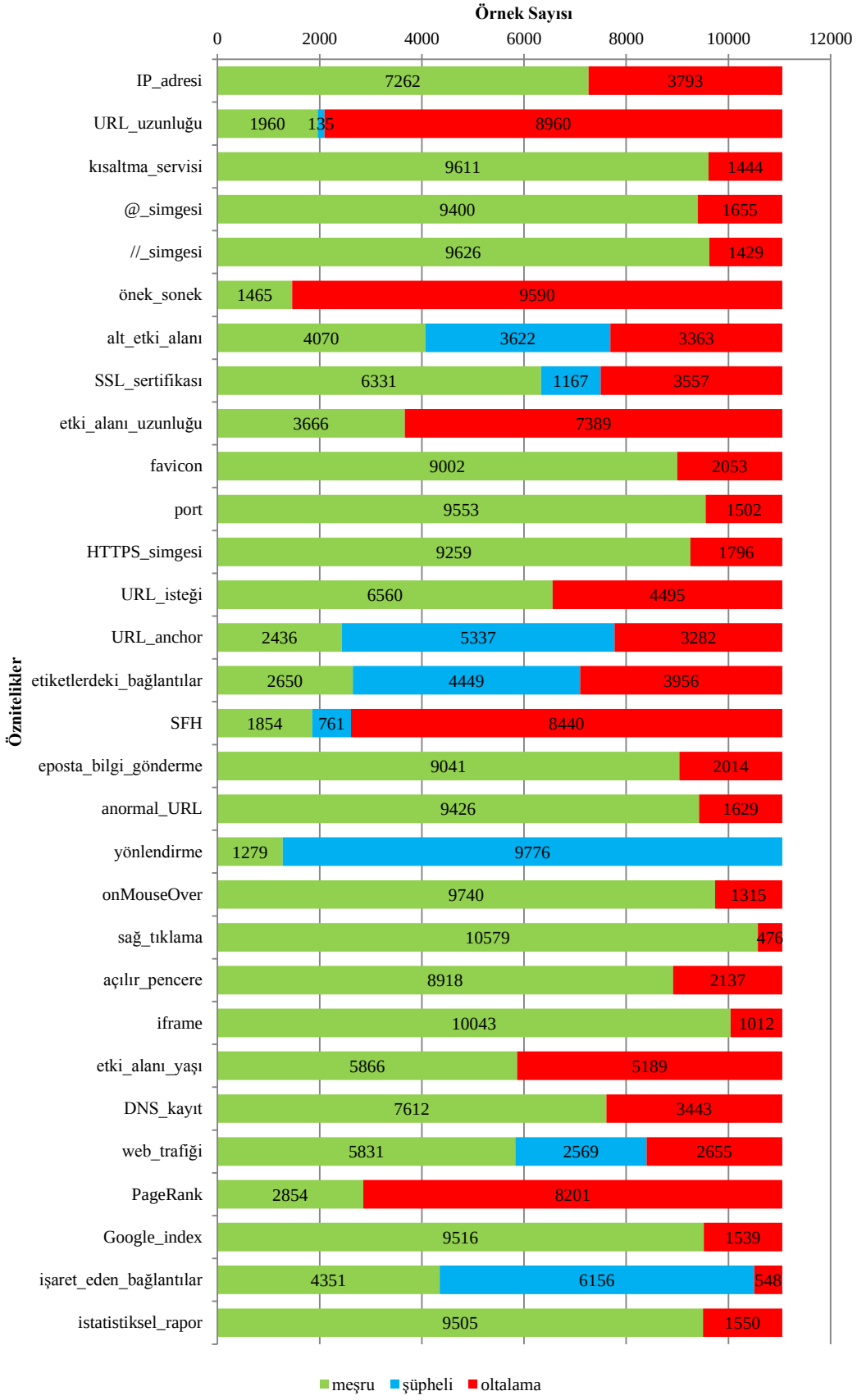
IP_adresi	URL_uzunluğu	kısaltma_servisi	@_simgesi	//_simgesi	önek_sonek	alt_etki_alanı	SSL_sertifikası	etki_alanı_uzunluğu	favicon	port	HTTPS_simgesi	URL_isteği	URL_anchor	etiketlerdeki_bağlantılar	SFH	eposta_bilgi_gönderme	anormal_URL	yönlendirme	onMouseOver	sağ_tıklama	açılır_pencere	iframe	etki_alanı_yaşı	DNS_kayıt	web_trafiği	PageRank	Google_index	işaret_eden_bağlantılar	istatistiksel_rapor	sonuç
-1	1	1	1	-1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	-1	-1	0	1	1	1	1	-1	-1	-1	-1	1	1	-1	-1
1	1	1	1	1	-1	0	1	-1	1	1	-1	1	0	-1	-1	1	1	0	1	1	1	1	-1	-1	0	-1	1	1	1	-1
1	0	1	1	1	-1	-1	-1	-1	1	1	-1	1	0	-1	-1	-1	-1	0	1	1	1	1	1	-1	1	-1	1	0	-1	-1
1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	0	-1	1	1	0	1	1	1	1	-1	-1	1	-1	1	-1	1	-1
1	0	-1	1	1	-1	1	1	-1	1	1	1	1	0	0	-1	1	1	0	-1	1	-1	1	-1	-1	0	-1	1	1	1	1
-1	0	-1	1	-1	-1	1	1	-1	1	1	-1	1	0	0	-1	-1	-1	0	1	1	1	1	1	1	1	-1	1	-1	-1	1
1	0	-1	1	1	-1	-1	-1	1	1	1	1	-1	-1	0	-1	-1	-1	0	1	1	1	1	1	-1	-1	-1	1	0	-1	-1
1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	-1	-1	1	1	0	1	1	1	1	-1	-1	0	-1	1	0	1	-1
1	0	-1	1	1	-1	1	1	-1	1	1	-1	1	0	1	-1	1	1	0	1	1	1	1	1	-1	1	1	1	0	1	1
1	1	-1	1	1	-1	-1	1	-1	1	1	1	1	0	1	-1	1	1	0	1	1	1	1	1	-1	0	-1	1	0	1	-1

Veri setinde giriş özellikleri için oluşturulan kurallarda bir web sitesi meşru, şüpheli veya oltalama olarak ele alınmıştır. Veri setinde çıkış için ise meşru veya oltalama şeklinde bir sınıflandırma yapılmıştır. Bu tez çalışmasında meşru için 1, şüpheli için 0 ve oltalama için -1 değerleri kullanılmıştır. Tablo 3.3'te bu çalışmada veri setindeki değerlere uygulanan yöntem görülmektedir.

Tablo 3.3 Veri setindeki değerlere uygulanan yöntem

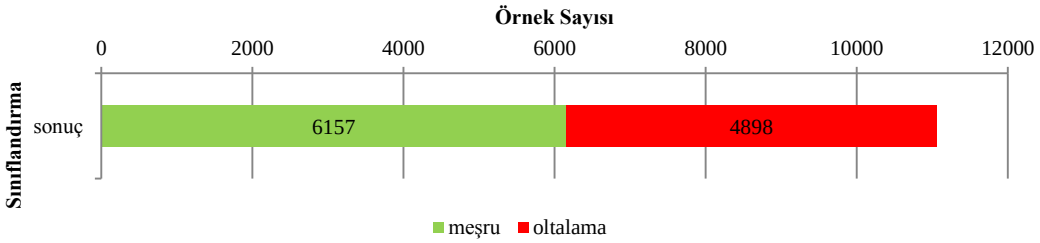
	Meşru	Şüpheli	Oltalama
Giriş veri seti değerleri	1	0	-1
Çıkış veri seti değerleri	1	mevcut değil	-1

Bu tez çalışmasında özniteliklerin her biri için meşru, şüpheli ve oltalama örnek sayıları tespit edilmiştir. Özniteliklerin bazılarının iki, bazılarının ise üç değer aldığı görülmektedir. Bunun nedeni öznitelikler için oluşturulan kurallardan kaynaklanmaktadır. Veri setinde toplam olarak 11055 adet örnek yer almaktadır. Veri seti 30 adet öznitelikten oluşmaktadır. Giriş veri seti öznitelikleri için meşru, şüpheli ve oltalama örnek sayıları Şekil 3.1'de gösterilmektedir.



Şekil 3.1 Giriş veri seti öznitelikleri için meşru, şüpheli ve oltalama sayıları

Bu tez çalışmasında sınıflandırma sonucu için meşru ve oltalama örnek sayıları tespit edilmiştir. Sınıflandırma sonucunun iki değer aldığı görülmektedir. Sınıflandırma sonucu sadece meşru veya oltalama için yapılmıştır. Sınıflandırma sonucu şüpheli olarak bir sınıflandırmaya tabi tutulmamıştır. Çıkış veri seti sınıflandırma sonucu için meşru ve oltalama sayıları Şekil 3.2'de gösterilmektedir.



Şekil 3.2 Çıkış veri seti sınıflandırma sonucu için meşru ve oltalama sayıları

3.2 Veri Seti Özellikleri, Kuralları ve Örnekleri

Oltalama web sitesi tahmini ile ilgili yapılan çalışmalarda karşılaşılan sorunlardan birinin güvenilir eğitim veri setlerinin bulunmaması olarak ifade edilmiştir. Bu sorunlardan kaynaklanan güçlüğe rağmen son zamanlarda veri madenciliği tekniklerini kullanan oltalama web sitesi tahmini ile ilgili birçok makale yayınlanmıştır. Güvenilir bir eğitim veri seti şimdiye kadar yayınlanmamıştır. Bunun olası sebebi sonucu olarak oltalama web sitelerini tanımlayan belirli özellikler üzerinde literatürde bir görüş birliğine varılmamıştır. Bundan dolayı olası tüm özellikleri kapsayan bir veri seti oluşturmak kolay görülmemiştir [62].

Yapılan çalışma [62] ile önemli özelliklerin açıklanması, ispatlanması ve oltalama web sitelerinin tahmin edilmesi amaçlanmıştır. Ek olarak bazı yeni özellikler önerilmiştir. Deneysel olarak bazı tanınmış özellikler için yeni kurallar atanmıştır. Diğer bazı özellikler için güncellemeler yapılmıştır.

3.2.1 IP adresi kullanma

Özellik 1

URL'de etki alanı adına alternatif olarak bir IP adresi kullanılabilir. Bu şekilde kullanıcıların kişisel bilgileri elde edilebilir. Bazen IP adresi 16 sayı tabanı koduna dönüştürülebilmektedir [62].

Örnek:

http://126.99.3.124/page.html

http://0x59.0xCD.0xCB.0x63/3/visa.br/main.html

Kural:

etki alanında IP adresi var → oltalama

aksi takdirde → meşru

3.2.2 Uzun URL kullanma

Özellik 2

Oltalama saldırısı yapanlar tarafından uzun URL kullanılabilmektedir. Bunun nedeni adres çubuğundaki şüpheli kısmın gizlenmesinin arzu edilmesidir. Çalışmayı doğrulamak için veri setindeki URL'lerin uzunlukları hesaplanmıştır. Bu şekilde ortalama URL uzunluğu bulunmuştur. URL uzunluğu 54'e eşit veya 54'ten büyük karakter sayısına sahipse URL oltalama olarak sınıflandırılmıştır. Veri seti incelendiğinde 1220 adet URL'nin uzunluklarının 54'e eşit veya 54'ten büyük olduğu görülmüştür. Bu da toplam veri seti boyutunun %48,8'ini oluşturmuştur. Bu kural, frekansa dayalı bir yöntem kullanılarak güncellenmiştir. Bu şekilde doğruluğu arttırılmıştır [62]. Oltalama URL uzunluklarını meşru olanlardan ayıran güvenilir bir uzunluk değerinin olmadığı ifade edilmiştir [57]. Yapılan bir çalışmada [63] meşru URL'lerin uzunluğu 75 karakter ya da 75 karakterden az olarak önerilmesine rağmen bunun sebebi açıklanmamıştır [57].

Örnek:

http://example.com/40/a/x42f3f320f41403a327c56c884b674567b5990097656f/?cmd=_root&z;update=22115e77a6c89a9ef2f8d3f9ee3267/46&adk/ghf112115e86a6;c85a9ab2f8d3f9aa5291f9@site.html

Kural:

URL uzunluğu < 54 → meşru

URL uzunluğu ≥ 54 ve ≤ 75 → şüpheli

aksi takdirde → oltalama

3.2.3 TinyURL kullanma

Özellik 3

URL kısaltma, “World Wide Web” üzerinde bir yöntem olarak kullanılabilmektedir. URL uzunluğu kısaltılabilmekte ve bu şekilde bile bir web sayfası açılabilmektedir. Uzun URL etki alanı adına bağlı olan kısa URL etki alanı adı HTTP yönlendirmesi ile gerçekleştirilebilmektedir [62].

Örnek:

URL:
https://en.wikipedia.org/wiki/First-generation_programming_language
(67 karakterden oluşmaktadır)
TinyURL:
http://tinyurl.com/jgpnoqo
(26 karakterden oluşmaktadır)

Kural:

TinyURL kullanılır → oltalama
aksi takdirde → meşru

3.2.4 URL’deki bir bölümü kullanma

Özellik 4

URL'de “@” simgesinden önceki kısmın tarayıcı tarafından görmezden gelindiği söylenmiştir. URL’de “@” simgesinden sonraki kısmın ise genellikle gerçek adres olduğu söylenmiştir [62].

Örnek:

http://signin.example.com@10.18.34.5/

Kural:

URL'de @ simgesi var → oltalama
aksi takdirde → meşru

3.2.5 Farklı web sitesine yönlendirme

Özellik 5

URL'de "//" simgesi kullanımı ile kullanıcı başka bir web sitesine yönlendirilebilmektedir. Çalışmada "//" simgesinin konumu üzerinde durulmuştur. URL; "HTTP" ile başlıyorsa "//" simgesinin altıncı konumda, "HTTPS" ile başlıyorsa "//" simgesinin yedinci konumda olması gerektiği söylenmiştir [62].

Örnek:

http://www.example.com ("//" simgesi altıncı konumda)

https://www.example.com ("//" simgesi yedinci konumda)

Kural:

URL'de "//" işaretinin en son görüldüğü konum > 7 → oltalama

aksi takdirde → meşru

3.2.6 Etki alanına "-" simgesi ile ayrılmış önek veya sonek ekleme

Özellik 6

Meşru olan URL'lerde tire simgesinin nadiren kullanılır. Oltalama saldırısı yapanlar tarafından etki alanı adına "-" ile ayrılmış önekler veya sonekler eklenebilir. Bu şekilde kullanıcıların meşru bir web sayfasını kullandıkları sanmaları sağlanmış olur [62].

Örnek:

http://signin-example.com

Kural:

etki alanı adında "-" simgesi var → oltalama

aksi takdirde → meşru

3.2.7 Alt etki alanı ve çoklu alt etki alanları

Özellik 7

Bu özellik kuralını oluşturmak için öncelikle gerçekte kendisi bir alt etki alanı olan URL'deki "www." görmezden gelinmiştir. Sonra eğer varsa URL'deki ülke kodu görmezden gelinmiştir. Sonunda URL'deki kalan noktalar sayılmıştır. Noktaların sayısı 1'e eşitse URL alt etki alanına sahip olmadığından web sitesi "meşru" olarak sınıflandırılmıştır. Noktaların sayısı 2'ye eşitse URL bir alt etki alanına sahip olduğundan web sitesi "şüpheli" olarak sınıflandırılmıştır. Noktaların sayısı 2'den büyükse URL çoklu alt etki alanlarına sahip olduğundan web sitesi "oltalama" olarak sınıflandırılmıştır [62].

Örnek:

www.example.com.tr

("www." ve ".tr" ifadelerindeki noktalar hariç olmak üzere nokta sayısı=1'dir.)

Kural:

etki alanındaki noktalar = 1 → meşru

etki alanındaki noktalar = 2 → şüpheli

aksi takdirde → oltalama

3.2.8 HTTPS kullanma

Özellik 8

Bir web sitesinin meşruluğu için HTTPS (HTTP Secure) varlığına önem verilmiştir. Ancak bu yeterli görülmemiştir. Yazarlar [57], [59]; HTTPS kullanma, güvenilir güvenlik sertifikası sağlayıcısı ve sertifika yaşını kapsayan sertifika denetimini önermişlerdir. Veri setleri test edildiğinde bir sertifikanın yaşının en az 2 yıl olduğu görülmüştür [62].

Örnek:

Bazı güvenilir güvenlik sertifikası sağlayıcıları [64]:

Comodo,

Symantec,

GoDaddy,
GlobalSign,
DigiCert.

Kural:
HTTPS kullanma, güvenli sertifika, sertifika yaşı ≥ 1 yıl → meşru
HTTPS kullanma, güvenli olmayan sertifika → şüpheli
aksi takdirde → oltalama

3.2.9 Etki alanı kayıt süresi

Özellik 9
Oltalama bir web sitesinin kısa ömürlü olduğu söylenmiştir. Güvenilir olan etki alanları için düzenli olarak birkaç yıl için ödeme yapıldığı ifade edilmiştir. Veri setinde en uzun ömürlü sahte etki alanlarının sadece bir yıl için kullanıldığı görülmüştür [62].

Örnek:
www.example.com
Expires On : April 22, 2018
Registered On : April 22, 2009
Updated On : April 22, 2016

Kural:
etki alanları kayıt süresinin dolması ≤ 1 yıl → oltalama
aksi takdirde → meşru

3.2.10 Favicon kullanımı

Özellik 10
Favicon, belirli bir web sayfasına özgü olan, bir grafik imaj veya bir ikon olarak tanımlanmıştır. Favicon, grafiksel tarayıcılar ve haber okuyucuları gibi birçok kullanıcı arayüzünde gösterilebilmektedir. Favicon, web sitesi kimliğinin görsel bir hatırlatıcısı gibi adres çubuğunda yer alabilmektedir. Favicon içeren bir web sayfası,

adres çubuğunda gösterilen etki alanından farklı olan bir etki alanından yüklenirse, bu web sayfası “oltalama” olarak sınıflandırılmıştır [62].

Örnek:

<link
rel=“icon”
type=“image/icon”
sizes=“16x16”
href=“http://www.example.com/favicon.ico”>

Kural:

harici etki alanından yüklenmiş favicon → oltalama
aksi takdirde → meşru

3.2.11 Standart olmayan portları kullanma

Özellik 11

Bu özellik ile bir sunucudaki hizmetlerin açık veya kapalı durumları incelenmiştir. Saldırıları engellemek için yalnızca ihtiyaç duyulan portların açık olmasının gerekli olduğu söylenmiştir. Farklı güvenlik duvarlarının, Vekil (Proxy) ve Ağ Adres Çözümleme (Network Address Translation (NAT)) sunucularının varsayılan olarak portlarının tümünü veya çoğunu kapatabildiği ve sadece seçili olanları açabildiği söylenmiştir. Tüm portlar açıksa oltalama saldırısını yapan kişilerin neredeyse istedikleri tüm hizmetleri çalıştırabildiği söylenmiştir. Sonuç olarak bu şekilde kullanıcı bilgilerinin tehdit edilebildiği söylenmiştir [62].

Örnek:

Tablo 3.4’te [62] genel kullanılan bazı portlar ile ilgili olarak port numarası, hizmet adı, açıklama ve tercih durumu ile ilgili bilgiler görülmektedir.

Tablo 3.4 Genel kullanılan portlar [62]

Port Numarası	Hizmet Adı	Açıklama	Tercih Durumu
21	FTP	(File Transfer Protocol) Bir makineden diğerine dosya aktarır	Kapalı
22	SSH	(Secure Shell) Güvenli dosya aktarma sağlar	Kapalı
23	Telnet	Çift yönlü, etkileşimli, metin tabanlı bir iletişim sağlar	Kapalı
80	HTTP	(Hyper Text Transfer Protocol)	Açık
443	HTTPS	(HTTP Secure) Güvenli HTTP	Açık
445	SMB	(Server Message Block) Paylaşılan dosyalara, yazıcılara, seri portlara erişim sağlar	Kapalı
1433	MsSQL	(Microsoft Structured Query Language) Diğer yazılım uygulamalarıyla istenen verileri saklar ve alır	Kapalı
1521	Oracle	Webden Oracle veritabanına erişir	Kapalı
3306	MySQL	Webden MySQL veritabanına erişir	Kapalı
3389	RDP	(Remote Desktop Protocol) Uzaktan erişim ve uzaktan işbirliği sağlar	Kapalı

Kural:

port numarası öncelikli durumun dışında → oltalama

aksi takdirde → meşru

3.2.12 HTTPS belirteci kullanma

Özellik 12

Oltalama saldırganlarının bir URL'nin etki alanı kısmına "HTTPS" belirtecini ekleyebildikleri söylenmiştir. Bu işlemin, kullanıcıları yanıltmak amacı ile yapıldığı söylenmiştir [62].

Örnek:

http://https-example.com/

Kural:

URL'nin etki alanında HTTPS belirteci var → oltalama

aksi takdirde → meşru

3.2.13 URL isteği

Özellik 13

Resim, video ve ses gibi harici nesneleri içeren web sayfaları incelenmiştir. Meşru olan bir web sayfasında web sayfası adresi ve web sayfasında gömülü olan nesnelerin çoğunun aynı etki alanını paylaşabildiği söylenmiştir [62]. Veri seti incelendiğinde meşru web sitelerinin en kötü durumda %22'sinin, buna karşın oltalama web sitelerinin ise en iyi durumda %61'inin nesneleri farklı etki alanlarından aldığı görülmüştür [59].

Örnek:

<img src="http://home.example.com/images/6/common/logo.gif">

Kural:

URL isteği %'si < %22 → meşru

URL isteği %'si ≥ %22 ve < %61→ şüpheli

aksi takdirde → oltalama

3.2.14 Anchor'un URL'si

Özellik 14

Anchor, <a> etiketi ile belirtilen bir eleman olarak tanımlanmıştır. Bu özellik "URL İsteği" özelliği gibi ele alınmıştır. Ancak bu özellik için bazı işlemler yapılmıştır. <a> etiketlerinin ve web sitesinin farklı etki alanı adlarına sahip olabildiği söylenmiştir. Anchor elemanının herhangi bir web sayfasına bağlantısının olmayabildiği söylenmiştir [62]. Veri seti incelendiğinde meşru web sitelerinin en kötü durumda %31'inin, buna karşın oltalama web sitelerinin ise en iyi durumda %67'sinin anchor etiketinin farklı etki alanlarına bağlı olduğu görülmüştür [59].

Örnek:

Kural:

anchor URL'sinin %'si < %31 → meşru

anchor URL'sinin %'si ≥ %31 ve ≤ %67 → şüpheli

aksi takdirde → oltalama

3.2.15 Etiketlerdeki bağlantılar

Özellik 15

Bu özellik bir web sayfasının kaynak kodları bakımından incelenmiştir. Bir web sayfasında bu etiketlerin aynı etki alanına bağlı olmasının beklendiği söylenmiştir. Meşru web siteleri için yaygın olarak kullanılan etiketlerin kullanım amaçlarının farklı olduğu söylenmiştir. <meta> etiketinin HTML (Hyper Text Markup Language) belgesiyle ilgili metadata önerisi almak için kullanıldığı söylenmiştir. <script> etiketinin istemci tarafı script oluşturmak için kullanıldığı söylenmiştir. <link> etiketinin diğer web kaynaklarını almak için kullanıldığı söylenmiştir [62].

Örnek:

Tablo 3.5'te; <meta>, <script> ve <link> etiketlerinin bazı örnek kullanımları gösterilmektedir.

Tablo 3.5 Bazı etiketlerin örnek kullanımları

<meta> etiketi
<meta http-equiv="refresh" content="2"; url=http://www.example.com">
<script> etiketi
<script type="text/javascript" src=" http://www.example.com/javascript.js"><script>
<link> etiketi
<link rel="stylesheet" type="text/css" href="http://www.example.com/template.css">

Kural:

<meta>, <script> ve <link> 'teki bağlantıların %'si < %17 → meşru

<meta>, <script> ve <link> 'teki bağlantıların %'si ≥ %17 ve ≤ %81 → şüpheli

aksi takdirde → oltalama

3.2.16 Server Form Handler

Özellik 16

Gönderilen bir bilgiye karşılık bir eylemin alınması gerektiği söylenmiştir. Bunun için boş bir string veya about:blank içeren Server Form Handler (SFH) "oltalama" olarak sınıflandırılmıştır. Gönderilen bir bilginin nadiren dış etki alanları tarafından kullanıldığı söylenmiştir. Bunun için SFH ile web sayfası etki alanı adları birbirinden farklı ise "şüpheli" olarak sınıflandırılmıştır [62].

Örnek:

"http://www.example.com" için:

<form action="/search/index.php" method="post" target=" top">

Kural:

SFH "about: blank" veya boş → oltalama

SFH farklı bir etki alanını belirtir → şüpheli

aksi takdirde → meşru

3.2.17 Epostaya bilgi gönderme

Özellik 17

Bir kullanıcının kişisel bilgilerini bir sunucuya göndermesi için web formu kullanıldığı söylenmiştir. Sunucunun kendisine gelen bu bilgileri işlediği ifade edilmiştir. Oltalama saldırısını yapan kişinin, kullanıcının bu bilgilerini kendi epostasına yönlendirebildiği söylenmiştir. Bu amaçla saldırganın bazı yöntemleri kullanabildiği söylenmiştir. Sunucu taraflı bir dil ile "mail()" fonksiyonunun kullanılabildiği söylenmiştir. İstemci taraflı bir dil ile de "mailto:" kullanılabildiği ifade edilmiştir [62].

Örnek:

```
mail("anyone@example.com","our subject","our message")
<a
href="mailto:abc@example.com?Subject=our%20subject&body=our%20message">
Send</a>
```

Kural:

kullanıcı bilgilerini göndermek için "mail()" veya "mailto:" kullanılır → oltalama

aksi takdirde → meşru

3.2.18 Anormal URL

Özellik 18

Bu özelliğin WHOIS veri tabanından ayıklanabildiği söylenmiştir. Meşru bir web sitesinin kimliğinin genellikle kendi URL'sinin bir parçası olduğu söylenmiştir [62].

Örnek:

Wikipedia URL: https://en.wikipedia.org/wiki/Main_Page

Kural:

konak adı URL'de yok → oltalama

aksi takdirde → meşru

3.2.19 Web sitesi yönlendirme

Özellik 19

Bu özellik için bir web sitesinin kaç kez yönlendirildiği araştırılmıştır. Veri setinde meşru web sitelerinin en fazla bir kez yönlendirildiği görülmüştür. Veri setinde oltalama web sitelerinin ise en az dört kez yönlendirildiği görülmüştür [62].

Örnek:

http://www.example1.com/signin.php?redirect=http://www.example2.com/main.php

Kural:

yönlendirme sayfası sayısı ≤ 1 → meşru

yönlendirme sayfası sayısı ≥ 2 ve < 4 → şüpheli

aksi takdirde → oltalama

3.2.20 Durum çubuğu özelleştirme

Özellik 20

Oltalama saldırısı yapan kişiler tarafından kullanıcılara durum çubuğunda sahte bir URL gösterilebilmektedir. Bunu yapmak için JavaScript kullanılabildiği söylenmiştir. Bu özellik için web sayfası kaynak kodu incelenmiştir. Özellikle "onMouseOver" olayı üzerinde durulmuştur. Bu olayın durum çubuğunda herhangi bir değişiklik yapıp yapmadığına bakılmıştır [62].

Örnek:

<a href = "http://www.example1.com/"
onMouseOver = "window.status = ""
onMouseOut = "window.status = 'http://www.example2.com'">
Please click here

Kural:

onMouseOver durum çubuğunu değiştirir → oltalama
aksi takdirde → meşru

3.2.21 Sağ tıklamayı devre dışı bırakma

Özellik 21

Oltalama saldırısı yapan kişiler tarafından sağ tıklama fonksiyonunun devre dışı bırakılabildiği söylenmiştir. Bunun için JavaScript kullanılabildiği ifade edilmiştir. Bu şekilde kullanıcılar tarafından bir web sayfasının kaynak kodunun görüntülenemediği ve kaydedilemediği söylenmiştir. Bu özellik, bağlantıyı gizlemek için "onMouseOver" kullanma gibi düşünülmüştür. Web sayfası kaynak kodundaki "event.button==2" olayı araştırılmıştır. Ayrıca sağ tıklamanın devre dışı olup olmadığı denetlenmiştir [62].

Örnek:

<script language="javascript">
document.onmousedown=drc;

```
function drc(event)
{
 if(event.button==2)
  {
   alert("disable right click");
   return true;
  }
}
</script>
```

Kural:

sağ tıklama devre dışı → oltalama

aksi takdirde → meşru

3.2.22 Açılır pencere kullanma

Özellik 22

Meşru bir web sitesinde açılır bir pencerenin kullanıcıların kişisel bilgilerini göndermelerini istemesi olağan bir durum olarak görülmemiştir. Bu özelliğin bazı meşru web sitelerinde belirli amaçlar için kullanılabildiği söylenmiştir. Bu amaçlara örnek olarak sahtecilik faaliyetleri hakkında kullanıcıları uyarma, kullanıcıları karşılama duyurusunun yayınlanması verilmiştir. Bu amaçların hiçbirinde açılır pencerelerde kişisel bilgilerin sorulmadığı ifade edilmiştir [62].

Örnek:

```
<script>
toplist=window.open("http://www.example.com");
self.focus();
</script>
```

Kural:

açılır pencere metin alanlarını kapsar → oltalama

aksi takdirde → meşru

3.2.23 Iframe yönlendirme

Özellik 23

Bir HTML etiketi olan iframe etiketi incelenmiştir. Fazladan bir web sayfası göstermek için o an açık olan web sayfasında iframe etiketinin kullanıldığı söylenmiştir. Oltalama saldırısı yapanlar tarafından iframe etiketinin kullanılabildiği söylenmiştir. Örnek olarak bu şekilde oluşturulan bir web sayfasının çerçeve kenarlıkları olmadan görünmez yapılabildiği verilmiştir. Bunun için de tarayıcıda görsel bir işlem yapan frameBorder özelliğinin kullanıldığı söylenmiştir [62].

Örnek:

<iframe
src=http://www.example.com
width=350
height=250
frameborder=0
scrolling=no>
</iframe>

Kural:

iframe kullanılır → oltalama
aksi takdirde → meşru

3.2.24 Etki alanı yaşı

Özellik 24

Bu özellik, WHOIS veri tabanından [65] ayıklanabilmiştir. Oltalama web sitelerinin çoğunun kısa bir süre için yaşadıkları söylenmiştir. Veri setinde meşru bir etki alanının yaşının en az 6 ay olduğu gözlenmiştir [62].

Örnek:

www.example.com
Expires On : April 22, 2017
Registered On : April 22, 2016

Kural:

etki alanı yaşı ≥ 6 ay → meşru

aksi takdirde → oltalama

3.2.25 DNS kaydı

Özellik 25

Oltalama bir web sitesinin kimliğinin WHOIS veri tabanında [65] tanınmadığı veya konak adı için kayıtların bulunmadığı söylenmiştir [66]. DNS (Domain Name System) kaydı yoksa veya bulunmamışsa web sitesi "oltalama" olarak sınıflandırılmıştır. Aksi takdirde "meşru" olarak sınıflandırılmıştır [62].

Örnek:

example.com etki alanı adı için bulunan isim sunucuları:

Name Servers:

NS4.DNS4.EXAMPLE.COM 129.201.60.191

NS5.DNS5.EXAMPLE.COM 53.27.132.48

Kural:

etki alanı için DNS kaydı yok → oltalama

aksi takdirde → meşru

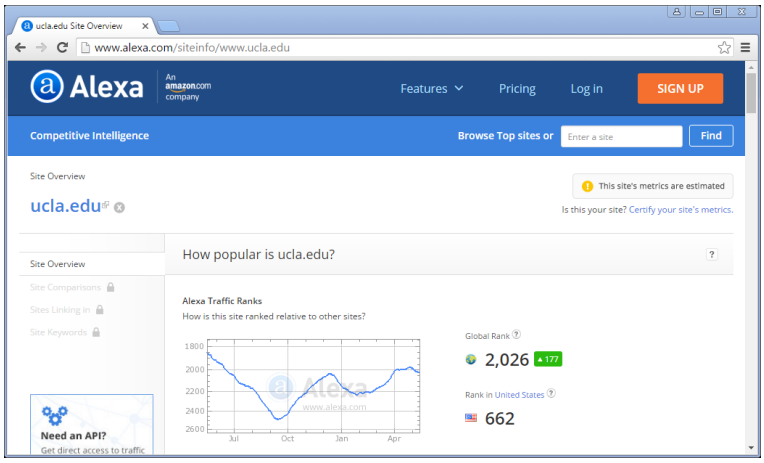
3.2.26 Web sitesi trafiği

Özellik 26

Bu özellik ile bir web sitesine olan ilgi ölçülmüştür. Bu ilgi, ziyaretçi sayıları ve ziyaret ettikleri sayfa sayıları ile tanımlanmıştır. Oltalama web siteleri kısa süreli yaşadıklarından Alexa veri tabanı [67] tarafından tanınmayabilmektedirler. Alexa, kullandığı farklı metriklerle trafiği iyi olan meşru web sitelerini 100 bin bandından sunabilmektedir. Etki alanı trafiği yoksa veya Alexa veri tabanı tarafından tanınmamışsa web sitesi "oltalama" olarak sınıflandırılmıştır. Aksi takdirde web sitesi "şüpheli" olarak sınıflandırılmıştır [62].

Örnek:

Şekil 3.3'te http://www.ucla.edu/ web sitesi için Alexa Trafik Sıralama değerleri görülmektedir. Global ve Birleşik Devletler'deki sıralama değerleri sırasıyla 2026 ve 662 olarak ölçülmüştür.



Şekil 3.3 ucla.edu için Alexa Trafik Sıralaması

Kural:

web sitesi sıralaması < 100.000 → meşru

web sitesi sıralaması > 100.000 → şüpheli

aksi takdirde → oltalama

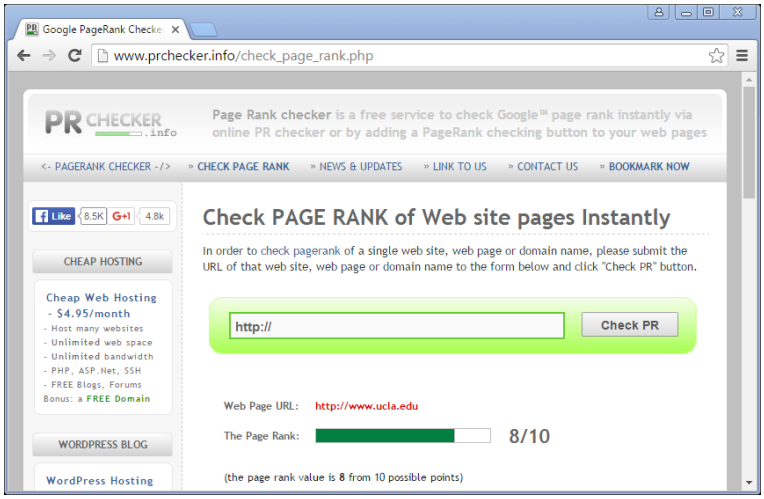
3.2.27 PageRank

Özellik 27

PageRank'ın 0'dan 1'e kadar olan bir değer olduğu söylenmiştir. PageRank'ın amacı İnternet'te bir web sayfasının önemini ölçmek olarak ifade edilmiştir. PageRank değerinin daha büyük olmasının daha önemli web sayfası anlamına geldiği söylenmiştir. Veri setinde oltalama web sayfalarının yaklaşık %95'inin PageRank'ının olmadığı görülmüştür. Geriye kalan oltalama web sayfalarının %5'lik kısmının PageRank'ının 0,2'ye ulaşabildiği görülmüştür [62]. PageRank değeri ölçümü için kullanılan bazı web tarayıcı eklentileri ve bazı web sitelerinin PageRank değerine 1 ile 10 arasında bir değer verdiği görülmektedir.

Örnek:

Şekil 3.4'te http://www.prchecker.info/ web sitesinde yapılan sorgulama sonucunda http://www.ucla.edu web sitesinin PageRank değeri 8 olarak ölçülmüştür.



Şekil 3.4 http://www.ucla.edu için PageRank değeri

Kural:

sayfa sıralaması < 0,2 → oltalama

aksi takdirde → meşru

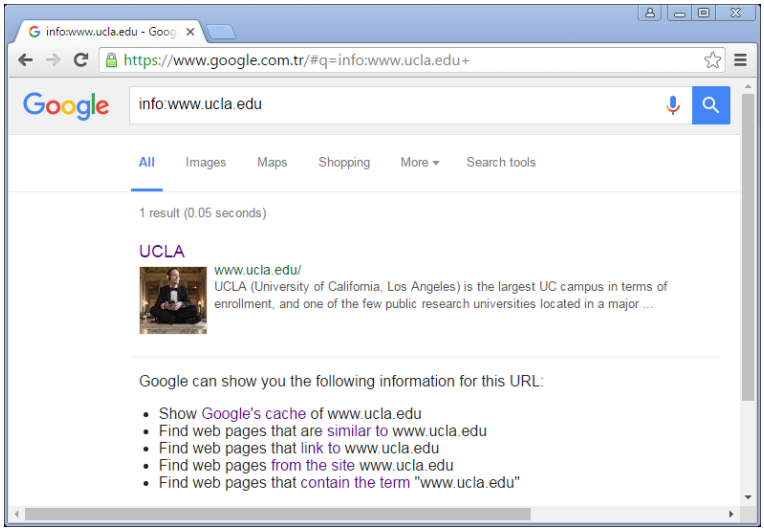
3.2.28 Google dizini

Özellik 28

Bu özellik ile bir web sitesinin Google dizininde olup olmadığı araştırılmıştır. Bir web sitesinin Google dizininde yer aldığında arama sonuçlarında görüldüğü söylenmiştir. Genellikle oltalama web sayfaları kısa bir süre için erişilebilir olduğundan birçok oltalama web sayfasının Google dizininde bulunamadığı söylenmiştir [62].

Örnek:

Şekil 3.5'te Google'da info:www.ucla.edu arama sonuç sayfası görülmektedir. Sayfada URL için beş farklı bilgi bağlantısı görülmektedir. Bu bağlantılara alternatif olarak sırasıyla cache: , related: , link: , site: operatörleri de kullanılabilir. Son sıradaki bağlantı ile "www.ucla.edu" ("" işaretleri dahil) ifadesi aratılmaktadır.



Şekil 3.5 Google'da URL'ye ait gösterilebilecek bilgiler

Kural:

Google tarafından dizine eklenen bir web sayfası → meşru

aksi takdirde → oltalama

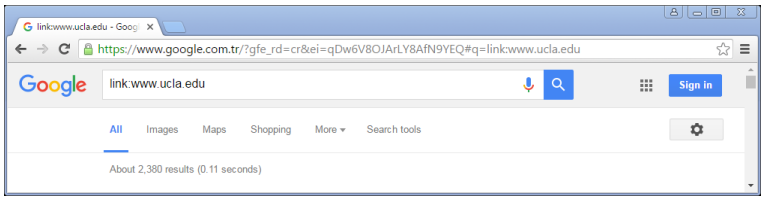
3.2.29 Sayfaya işaret eden bağlantıların sayısı

Özellik 29

Bazı bağlantılar aynı etki alanında olsa bile web sayfasına işaret eden bağlantıların sayısı meşruluk seviyesi açısından ele alınmıştır [68]. Veri setinde oltalama veri seti elemanlarının %98'inin kendine işaret eden bağlantısının bulunmadığı görülmüştür. Bunun nedeni olarak yaşam sürelerinin kısa olması gösterilmiştir. Meşru web sitelerinin kendilerini işaret eden en az 2 dış bağlantıya sahip olduğu görülmüştür [62].

Örnek:

Şekil 3.6'da Google'da "link:www.ucla.edu" arama sonuç sayfasında yaklaşık 2380 sonucun yer aldığı görülmektedir.



Şekil 3.6 Google'da link:www.ucla.edu arama sonucu

Kural:

web sayfasına işaret eden bağlantıların sayısı = 0 → oltalama

web sayfasına işaret eden bağlantıların sayısı > 0 ve ≤ 2 → şüpheli

aksi takdirde → meşru

3.2.30 İstatistiksel raporlar

Özellik 30

PhishTank [69] ve StopBadware [70] gibi bazı gruplar tarafından belirli süreler için oltalama web siteleri üzerinde birçok istatistiksel raporun hazırlandığı söylenmiştir. Bu sürelerin bazılarının aylık, bazılarının ise üç aylık olduğu söylenmiştir. Araştırmada PhisTank'ın ilk ondaki iki türü kullanılmıştır. Bu türler "İlk 10 Etki Alanı" ve "İlk 10 IP adresi" olup son üç yılda yayınlanan istatistiksel raporlara göre incelenmiştir. Son üç yıl aralığı Ocak 2010 ile Kasım 2012 arası olarak belirlenmiştir. StopBadware'den ise "İlk 50 IP adresi" kullanılmıştır [62].

Örnek:

2012 yılı Ekim ayı için PhishTank tarafından doğrulanan gönderimlerin 19301 adedinde bir etki alanı, 942 adedinde ise bir IP adresi kullanılmıştır. Tablo 3.6'da ise PhishTank'ın Ekim 2012'ye ait ilk 10 etki alanı ve ilk 10 IP kullanım istatistikleri görülmektedir [71].

Tablo 3.6 Ekim 2012'ye ait ilk 10 etki alanı ve ilk 10 IP istatistikleri [71]

	İlk 10 Etki Alanı (*)		**İlk 10 IP (*)**
1	addr.com (180)	1	118.194.237.51 (294)
2	digicozum.com (140)	2	69.90.211.44 (180)
3	google.com (129)	3	193.33.128.141 (176)
4	besdez.net (92)	4	72.55.153.110 (171)
5	altervista.org (87)	5	93.170.52.21 (160)
6	hickrecs.com (84)	6	209.217.251.146 (160)
7	eventcreation.dk (82)	7	93.170.52.31 (158)
8	toujoursports.com (70)	8	200.63.98.68 (145)
9	amezionuk.org (67)	9	77.223.131.106 (145)
10	bit.ly (64)	10	180.235.128.202 (135)
*** PhishTank tarafından doğrulanan gönderimlerin sayısı**			

Kural:

üst oltalama IP'leri veya üst etki alanlarına ait konak → oltalama

aksi takdirde → meşru

3.3 Akıllı Yöntemler

3.3.1 Yapay Sinir Ağı

YSA biyolojik sinir hücrelerinin (nöron) çalışma şeklini örnek alan güçlü bir sınıflandırma aracıdır. Nöron olarak adlandırılan sinir hücrelerinin bağlantılı işlem elemanlarının birlikte çalışması ile problem çözümü gerçekleştirilir. YSA, doğrusal olmayan bir modeldir ve farklı algoritmalar ile eğitile bilinir. Bundan dolayı problem çözmedeki başarısı yüksektir. Çok Katmanlı Algılayıcı (ÇKA), sınıflandırma, kümeleme, tahmin, eşleşme ve fonksiyon uydurma problemlerinde kullanılan doğrusal olmayan bir modeldir. ÇKA, bir giriş katmanı, en az bir gizli katman ve bir çıkış katmanı olmak üzere 3 katmandan oluşmaktadır. Dış dünyadan alınan bilgiler giriş katmanından ağa tanıtılıp gizli katmanlardan çıkış katmanına ulaşır. Çıkış katmanına ulaşan bu bilgiler çıkış katmanından dış dünyaya gönderilir [5].

YSA, farklı ağırlıklar ile birbirine bağlı olan birçok yapay sinir hücresinden oluşmaktadır. Doğrusal olan bir problemi çözebilmek için tek bir nöron kullanılır. Çok Katmanlı Algılayıcı (ÇKA) (Multi Layer Perceptron (MLP)) içinde Backpropagation ağları kullanılmaktadır. Backpropagation ağları sınıflandırmada kullanılan tekniklerden biridir. Delta öğrenme kuralı backpropagation ağlarında öğrenme fonksiyonu olarak kullanılmaktadır. MLP kullanılarak yapılan bir çalışmaya

örnek olarak parmak izi ile cinsiyet sınıflandırma [72] gösterilebilir**.**

Paralel işlem yapabilme gücüne sahip ve hızlı olan YSA, çözüm algoritması karışık veya güç olan problemleri çözebilmektedir. Bu işlemi, gözlemlere dayanarak ve gerçek zamanda gerçekleştirebilir. Bu sebeple bilinen metotlara göre daha avantajlıdır [73].

YSA, paralel işlem yeteneklerinden dolayı örüntü eşleştirme, lineer olmayan sistem modelleme, iletişim, elektrik ve elektronik endüstrisi, enerji üretimi, kimyasal endüstri, tıbbi uygulamalar, veri madenciliği ve kontrol için kullanılabilmektedir. Bundan ötürü ilişkisel modeller veya paralel dağıtılmış işlem modelleri olarak da bilinirler [74].

Bir YSA modeli tasarlanacağı zaman bazı noktalara dikkat edilmelidir. Öncelikle uygun bir sinir ağı modeli seçilmelidir. Sonra aktivasyon fonksiyonu ve aktivasyon değerleri tanımlanmalıdır. Her katman için katman sayısı ve birim sayısı seçilmelidir. Genel olarak istenen model katmanlardan oluşmaktadır. En genel modelde tüm birimler arasında tam bir bağlantının olduğu varsayılır. Bu bağlantılar iki yönlü veya tek yönlü olabilmektedir [75].

YSA'nın avantajları şu şekilde sıralanabilir [76]:

- Genel amaçlı bir bilgisayarla optik veya elektriksel olarak modellenebilirler.
- Hata toleransları vardır ve güçlüdürler.
- Özel donanım cihazları paralel çalışma kabiliyetlerinden yararlanmak için tasarlanmakta ve üretilmektedir.
- Uygulamalarda birçok öğrenme algoritması veya paradigması kullanılabilir.
- İlk tecrübe veya eğitim için girilen verilere göre öğrenme becerisi vardır.
- Öğrenme boyunca aldığı bilginin organizasyonunu ya da gösterilmesini kendisi yapabilir.

YSA'nın sahip olduğu özellikler şu şekilde sıralanabilir [77]:

- Matematiksel modeli, biyolojik bir nörondan ilham alınarak ifade edilmiştir.
- Birbiri ile bağlı çok sayıda işlem elemanından meydana gelir.

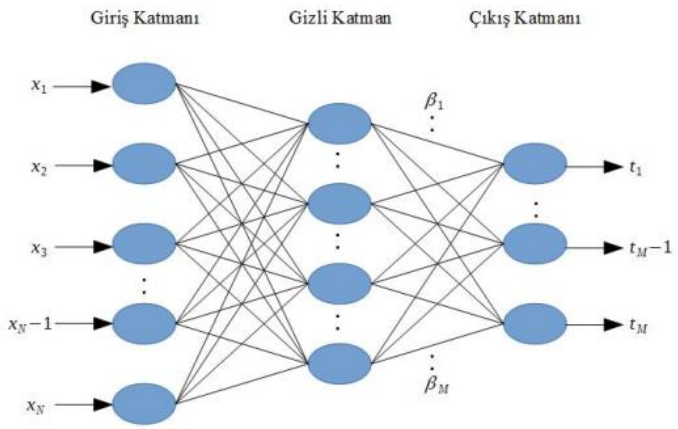
- Bilgiyi bağlantı ağırlıkları ile tutar.
- Bir işlem elemanı giriş uyarısına tepki verebilir. Bu tepki dinamik olabilir ve yerel bilgilere bağlıdır. (Giriş sinyali bağlantı ağırlıkları ve işlem elemanını etkileyen bağlantılar ile gelir.).
- Bağlantı ağırlıkları eğitim verileri ile ayarlanır. Bu sayede genelleme, hatırlama ve öğrenme kabiliyeti vardır.

3.3.2 Aşırı Öğrenme Makinesi

Huang vd [78] yaptıkları çalışma ile AÖM olarak adlandırdıkları öğrenme algoritmasını önermişlerdir. Bu algoritmayı tek gizli katmanlı ileri beslemeli sinir ağları (Single-hidden Layer Feedforward Neural Network (SLFN)) için sunmuşlardır. Bu ağlar gizli düğümleri rastgele seçerler, çıkış ağırlıklarını ise analitik olarak belirlerler. Bu algoritma teorik olarak iyi bir genelleme performansı sağlama eğilimindedir. Bunu da son derece hızlı bir öğrenme ile yapar. Deneysel sonuçlar bu algoritmanın iyi bir genelleme performansı sunduğunu göstermiştir. İleri beslemeli sinir ağları için bilinen algoritmalardan binlerce kez hızlı öğrenebildikleri ifade edilmiştir.

SLFN sinir ağı modeli için kullanılan AÖM [79], yapılan çalışmalarda öncelikle tek gizli katmanlı ileri beslemeli bir sinir ağı olarak önerilmiştir [78]. Daha sonra yapılan çalışmalarda ise sinir ağında tek gizli katman olmayan genelleştirilmiş ileri beslemeli bir sinir ağı olarak geliştirilmiştir [80]. AÖM tarafından oluşturulan sinir ağı giriş katmanındaki nöronların ağırlık değerleri ve gizli katmandaki nöronların eğim (eşik) değerleri rastgele üretilmekte, çıkış katmanındaki nöronların ağırlık değerleri ise analitik olarak ölçülmektedir [81]. Gizli katmanda hardlimit, gaussian ve sigmoid vb. aktivasyon fonksiyonları kullanılıp çıkış katmanında ise lineer fonksiyon kullanılır [82].

AÖM; doküman sınıflandırma [83], biyoenformatik [84], semantik kavramı algılama [85], güvenlik değerlendirmesi [86], yüz tanıma [87], görüntü süper çözünürlüğü [88] gibi geniş bir uygulama alanında başarılı bir şekilde uygulanmıştır.



Şekil 3.7 AÖM için ağ modeli

Şekil 3.7'deki gibi standart bir SLFN modeli için;

N,

$(x_i, t_i) \in R^{nxm}$ olmak üzere rastgele sayıdaki eğitim örneğine sahip bir veri setidir.

m sayıdaki sınıf ile birlikte $i = 1,2, \dots, N$ 'dir.

x_i,

giriştir ve

$x_i = [x_{i1}, x_{i2}, \dots, x_{in}]^T \in R^n$

ile ifade edilir.

t_i,

arzu edilen uygun çıkıştır ve

$t_i = [t_{i1}, t_{i2}, \dots, t_{im}]^T \in R^m$

ile ifade edilir.

Bu parametrelere sahip olan bir AÖM matematiksel olarak

$$\sum_{i=1}^{L} \beta_i g_i(x_j) = \sum_{i=1}^{L} \beta_i g(w_i . x_j + b_i) = o_j, \ j = 1,2, \dots, N \qquad (2,1)$$

gibi modellenir [78].

Bu modelde:

L,

gizli katman düğümlerinin sayısıdır.

$g(x)$,

aktivasyon fonksiyonudur.

w_i,

i'ninci gizli nöron ve giriş nöronlarına bağlı rastgele seçilen giriş ağırlık vektörü olup

$w_i = [w_{i1}, w_{i2}, \dots, w_{in}]^T$

ile gösterilir.

β_i,

i'ninci gizli nöron ve çıkış nöronlarına bağlı ağırlık vektörü olup

$\beta_i = [\beta_{i1}, \beta_{i2}, \dots, \beta_{im}]^T$

ile gösterilir.

b_i,

i'ninci gizli düğümün rastgele seçilen eşik (eğim) (threshold (bias)) değeridir.

o_j,

x_i girişine göre gerçek çıkıştır.

$w_i . x_j$,

w_i ile x_j'nin içsel çarpımını gösterir.

Çıkış düğümleri lineer olarak seçilir.

L tane gizli düğüme, $g(x)$ aktivasyon fonksiyonuna sahip standart bir SLFN, N sayıdaki örneği sıfır hataya yaklaştırabilir.

$\sum_{j=1}^{L} \|o_j - t_j\| = 0$, β_i, w_i ve b_i arasındaki ilişki matematiksel olarak

$$\sum_{i=1}^{L} \beta_i g(w_i . x_j + b_i) = t_j, \ j = 1,2, \dots, N \quad (2,2)$$

gibi ifade edilebilir.

Denklem (2,2)'deki N sayıdaki denklem

$$H\beta = T \quad (2,3)$$

gibi özlü bir şekilde modellenebilir.

H,

Huang vd [89] tarafından adlandırılmış olan gizli katman çıkış matrisidir.

$$H = \begin{bmatrix} g(w_1 . x_1 + b_1) & \cdots & g(w_L . x_1 + b_L) \\ \vdots & \ddots & \vdots \\ g(w_1 . x_N + b_1) & \cdots & g(w_L . x_N + b_L) \end{bmatrix}_{NxL} \quad (2,4)$$

$$\beta = \begin{bmatrix} \beta_1^T \\ \vdots \\ \beta_L^T \end{bmatrix}_{Lxm}$$

$$T = \begin{bmatrix} t_1^T \\ \vdots \\ t_N^T \end{bmatrix}_{Nxm}$$

Lineer denklem (2,3) çözülerek optimum çıkış ağırlık matrisi

$$\hat{\beta} = H^{\dagger}T \tag{2,5}$$

gibi elde edilir.

Denklem (2,5), β'nin tahmini değeri olarak kullanılır.

$H^{\dagger}$,

gizli katman çıkış matrisi olan H'ın Moore-Penrose genelleştirilmiş tersi [90] olarak gösterilir.

AÖM algoritması:

Adım 1: Rastgele gizli düğüm parametreleri üreterek rastgele gizli düğümler ata.

(w_i, b_i), $i = 1,2, \dots, L$

Adım 2: Gizli katman çıkış matrisini hesapla.

H

Adım 3: Çıkış ağırlık matrisini hesapla.

$\hat{\beta} = H^{\dagger}T$

3.4 k-katlı Çapraz Geçerlilik Testi

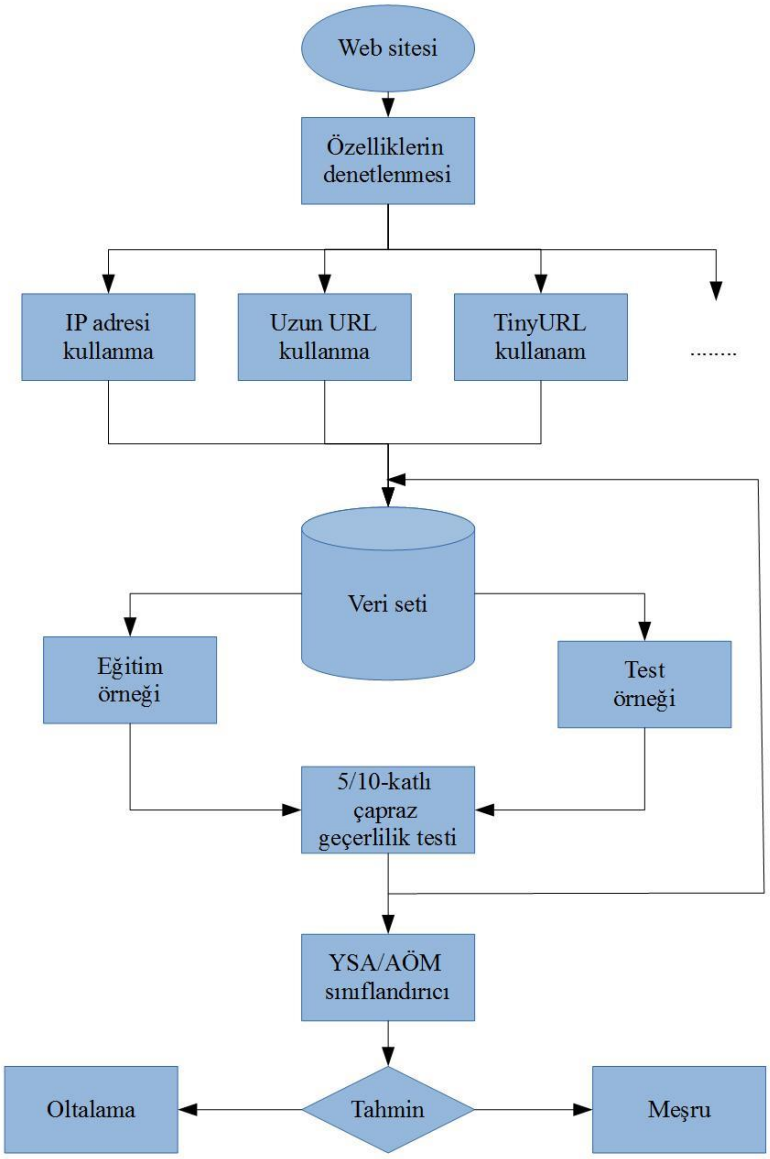
Basit çapraz geçerlilik testinde veri setinin %5 ile %33 arasındaki bir bölümü test verisi olarak belirlenmekte ve modelin eğitim aşamasında bu bölüm kullanılmamaktadır. Veri setinin geriye kalan bölümünde ise model oluşturulmakta ve gerçek değerler ile tahmin değerleri karşılaştırılarak modelin doğruluğu ölçülmektedir [91].

Bir sistem çalıştırıldıktan sonra çıkan sonuçların doğrulukları ölçülerek sistemin başarısı değerlendirilebilir. Bu değerlendirmeği yapmak için kullanılan

yöntemlerden biri k-lı çapraz geçerlilik testidir. Bu yöntemle bir veri kümesi her birinde aynı sayıda veri olacak şekilde alt veri kümelerine bölünür. Veri kümesi V, alt küme sayısı k olarak gösterilirse, alt kümeler de sırasıyla V_1, V_2, V_3, …, V_k olarak gösterilebilir. Yöntemin uygulanması için alt veri kümelerinden biri seçilip verilerin bir kısmı eğitim geri kalanı ise test verisi olacak şekilde işleme alınır. Bu işlem diğer tüm alt kümeler için tekrar edilir. Bu şekilde k sayısı kadar başarı ölçüsü elde edilmiş olur. Sistemin genel başarısını hesaplamak için bu başarıların ortalaması alınır [5].

4. SİSTEM MİMARİSİ

Şekil 4.1'de bu tez çalışması için genel bir sistem mimarisi sunulmaktadır. Bir web sitesi için özellikler denetlenir. Özelliklerin değerleri ile veri seti oluşturulur. Veri seti, eğitim örneği ve test örneği olmak üzere farklı oranlarda işleme alınır. 5/10-katlı çapraz geçerlilik testi ile sistemin doğruluğu ölçülür. YSA/AÖM sınıflandırıcı ile bir web sitesinin oltalama veya meşru olduğu tahmin edilir.



Şekil 4.1 Genel sistem mimarisi

5. ÖNERİLEN KURALLAR

Özellik 13 için oluşturulan kural meşru, şüpheli ve oltalama şeklinde sınıflandırılmıştır [62]. Ancak bu tez çalışmasında veri setinde yapılan inceleme sonucunda 13'üncü özniteliğin 1 ve -1 değerlerine sahip olduğu görülmüştür. Şekil 3.1'den de görüleceği gibi "URL isteği" özelliği 6560 adet meşru ve 4495 adet oltalama olmak üzere toplam 11055 adet örnekten oluşmaktadır. Bu nedenle özellik 13 için yeni bir kural önerilmiştir. Önerilen bu kural bu çalışmadaki uygulamada kullanılmıştır.

Özellik 19 için oluşturulan kural meşru, şüpheli ve oltalama şeklinde sınıflandırılmıştır [62]. Ancak bu tez çalışmasında veri setinde yapılan inceleme sonucunda 19'uncu özniteliğin 1 ve 0 değerlerine sahip olduğu görülmüştür. Şekil 3.1'den de görüleceği gibi "yönlendirme" özelliği 1279 adet meşru ve 9776 adet şüpheli olmak üzere toplam 11055 adet örnekten oluşmaktadır. Bu nedenle özellik 19 için yeni bir kural önerilmiştir. Önerilen bu kural bu çalışmadaki uygulamada kullanılmıştır.

Özellik 13

URL isteği

Kural:
URL isteğinin %'si < %22 → meşru
URL isteğinin %'si ≥ %22 ve < %61→ şüpheli
aksi takdirde → oltalama

Önerilen Kural:
URL isteğinin %'si < %22 → meşru
aksi takdirde → oltalama

Özellik 19

Web sitesi yönlendirme

Kural:

yönlendirme sayfası sayısı ≤ 1 → meşru

yönlendirme sayfası sayısı ≥ 2 ve < 4 → şüpheli

aksi takdirde → oltalama

Önerilen Kural:

yönlendirme sayfası sayısı ≤ 1 → meşru

aksi takdirde → şüpheli

6. YSA İLE WEB TABANLI OLTALAMA SALDIRISININ TESPİTİ

Bu uygulamanın amacı oltalama (phishing) olarak adlandırılan ve bilgi güvenliğine yönelik tehditlerden biri olan sahte web sitelerinin tespit edilmesine yönelik bir model oluşturmaktır. Oltalama saldırısı artış göstermekte olan bir siber saldırı türü olduğundan [92] bu çalışmada ele alınmıştır. YSA kullanılarak oltalama saldırısının belirlenmesine yönelik bir model oluşturulmuştur. Bu uygulama ile sınıflandırma doğrulukları %87,97 - %90,64 - %91,04 - %90,95 - %92,45 olarak ölçülmüştür. Ortalama sınıflandırma doğruluğu ise %90,61 olarak ölçülmüştür. Bu uygulama için Matlab yazılımının Neural Network Toolbox'ı kullanılmıştır. Veri setindeki toplam 11055 adet gözlem kullanılmıştır. Oluşturulan modelin başarımını belirlemek için 5-li çapraz geçerlilik testi uygulanmıştır. Eğitilen YSA model parametreleri Tablo 6.1'de verilmiştir [5].

Tablo 6.1 YSA model parametreleri [5]

Ağ türü	İleri Beslemeli Geri Yayılımlı
Eğitim fonksiyonu	Trainlm
Adaptasyon öğrenme fonksiyonu	Learngdm
Performans fonksiyonu	Ortalama karesel hata
Katman sayısı	3
Katmanlardaki nöron sayısı	30-10-1
Katman 1 için transfer fonksiyonu	Tanjant Sigmoid
Tur Sayısı	1000
Doğruluk Değeri	0,001

Tablo 6.2'den de görüleceği gibi veri setinde toplam 11055 adet gözlem yer almaktadır. Veri setindeki örneklerin %80'ine karşılık gelen 8844 adet örnek eğitim veri seti olarak kullanılmıştır. Veri setinden geriye kalan ve veri setinin %20'sine karşılık gelen 2211 adet örnek de test veri seti olarak kullanılmıştır [5].

Tablo 6.2 Uygulamada kullanılan veri seti [5]

Veri Seti	**% Oranı**	**Örnek Adedi**
Toplam	100	11055
Eğitim	80	8844
Test	20	2211

Bu uygulamada 5-li çapraz geçerlilik testi uygulanmıştır. Bunun için veri setinin %80'i eğitim, %20'si ise test amaçlı olarak kullanılmıştır. Her kat için bu

oran korunarak veri setinin farklı bölümleri eğitim ve test amaçlı olarak kullanılmıştır. Örneğin kat-1 için 1-8844 (1 ve 8844 dahil) arasındaki örnekler eğitim için, 8845-11055 (8845 ve 11055 dahil) arasındaki örnekler de test için kullanılmıştır. Tablo 6.3'te sırası ile bu katlar ve kullanılan veri seti bölümleri görülmektedir [5].

Tablo 6.3 Çalışmada kullanılan 5-li çapraz geçerlilik testi [5]

Veri Seti Toplam Örnek Sayısı	11055				
Veri Seti Örnek Sayısı	2211	2211	2211	2211	2211
Veri Seti Örnek Aralığı	1-2211	2212-4422	4423-6633	6634-8844	8845-11055
kat-1	Eğitim	Eğitim	Eğitim	Eğitim	Test
kat-2	Eğitim	Eğitim	Eğitim	Test	Eğitim
kat-3	Eğitim	Eğitim	Test	Eğitim	Eğitim
kat-4	Eğitim	Test	Eğitim	Eğitim	Eğitim
kat-5	Test	Eğitim	Eğitim	Eğitim	Eğitim

Bu uygulamada YSA ile 5 sinir ağı oluşturulmuştur. Tablo 6.4'te bu 5 sinir ağının doğru sınıflandırma, yanlış sınıflandırma, doğruluk yüzdesi, hata yüzdesi belirlenmiştir. Daha sonra bu 5 ağın başarı ortalamaları alınıp genel başarı oranı ölçülmüştür. En yüksek sınıflandırma doğruluğu %92,45 olarak ölçülmüştür. Bu ağda doğru sınıflandırma sayısı 2044 iken yanlış sınıflandırma ise 167 olarak tespit edilmiştir. Ortalama sınıflandırma doğruluğu ise %90,61 olarak gözlenmiştir. Ağların ortalama doğru sınıflandırması 2003,4 ve yanlış sınıflandırması ise 207,6 olarak ölçülmüştür [5].

Tablo 6.4 Sinir ağlarının doğru-yanlış sınıflandırma ve doğruluk-hata yüzdeleri [5]

Sinir Ağı Adı	**Doğru Sınıflandırma**	**Yanlış Sınıflandırma**	**Doğruluk Yüzdesi**	**Hata Yüzdesi**
k1Network	1945	266	87,96924	12,03076
k2Network	2004	207	90,63772	9,36228
k3Network	2013	198	91,04478	8,95522
k4Network	2011	200	90,95432	9,04568
k5Network	2044	167	92,44686	7,55314
Ortalama	**2003,4**	**207,6**	**90,61058**	**9,38942**

6.1 Uygulama Sonucu

Uygulama 1'de, oltalama yöntemi ile internet sitelerine yönelik yapılan saldırıların YSA kullanılarak belirlenmesi amaçlanmıştır. Yapılan çalışmada kullanılan veriler UCI veri seti web sayfasından alınmıştır. 30 adet giriş özelliği ile 1 adet çıkış özelliği kullanılmıştır. Giriş özellikleri 1, 0, -1 değerlerini almakta çıkış özelliği ise 1, -1 değerlerini almaktadır. Sistemin performansını belirlemek için 5-li çapraz geçerlilik testi uygulanmıştır. Yapılan çalışmalarda en yüksek %92,45 ve ortalama %90,61 sınıflandırma doğruluğu elde edilmiştir.

7. AÖM İLE WEB TABANLI OLTALAMA SALDIRISININ TESPİTİ

Veri setinde toplam 11055 örnek bulunmaktadır. Bu uygulamada ise veri setine 10-lu çapraz geçerlilik testi uygulandığından veri setindeki ilk 11050 örnek kullanılmıştır. Son 5 örnek kullanılmamıştır. Tablo 7.1'de bu uygulamada kullanılan veri setine ait bazı bilgiler yer almaktadır. Eğitim veri seti için veri setinin %90'ı kullanılmıştır. Eğitim veri seti bu şekilde 9945 örnekten oluşmuştur. Test veri seti için ise veri setinin %10'u kullanılmıştır. Test veri seti bu şekilde 1105 örnekten oluşmuştur.

Tablo 7.1 Model için kullanılan veri seti

Veri Seti	Oran (%)	Örnek Sayısı
Toplam	100	11050
Eğitim	90	9945
Test	10	1105

Tablo 7.2'de bu çalışma kapsamında eğitilen AÖM model parametrelerine ve açıklamalarına yer verilmiştir.

Tablo 7.2 AÖM model parametreleri ve açıklamaları

Parametre	Açıklama
Ağ türü	İleri Beslemeli
Katman sayısı	3
Giriş katman nöron sayısı	30
Gizli katman nöron sayısı	850
Çıkış katman nöron sayısı	2
Aktivasyon fonksiyonu	Hiperbolik Tanjant
Test veri sayısı	1105
Eğitim veri sayısı	9945
Toplam veri sayısı	11050

Sistemi doğrulamak için 10-lu çapraz geçerlilik testi uygulanmıştır. Veri setinin %90'ı eğitim, %10'u ise test için kullanılmıştır. Bu oran değiştirilmeden veri setinin diğer bölümleri eğitim ve test için kullanılmıştır.

Bu uygulamada AÖM ile oluşturulan modelde ortalama sınıflandırma doğruluğu %95,05 olarak gözlenmiştir. En yüksek sınıflandırma doğruluk oranı ise %95,93 ile elde edilmiştir. Tablo 7.3'te sınıflandırma doğruluk ve hata oranları görülmektedir.

Tablo 7.3 Sinir ağlarının sınıflandırma doğruluk ve hata oranları

Sinir Ağı	Doğruluk (%)	Hata (%)
1	95,1131	4,16290
2	95,1131	4,34389
3	95,9276	4,34389
4	94,2986	5,79186
5	95,6561	3,61991
6	95,2036	5,24887
7	94,1176	5,79186
8	95,0226	5,06787
9	94,8416	5,06787
10	95,2036	4,79638
Ortalama	**95,0498**	**4,82353**

7.1 Uygulama Sonucu

Uygulama 2'nin amacı oltalama diye adlandırılan ve siber tehditlerden biri olan saldırı türünün belirlenmesine yönelik bir sınıflandırma yapmaktır. Bu amaçla AÖM kullanılmıştır. Yapılan bu çalışmada UCI web sitesinden alınan veri seti kullanılmıştır. Bu veri setindeki giriş özellikleri 30, çıkış özelliği ise 1 adet olarak düzenlenmiştir. Giriş özellikleri 1, 0 ve -1 olmak üzere 3 farklı değer alabilmektedir. Çıkış özelliği ise 1 ve -1 olmak üzere 2 farklı değer alabilmektedir. Bu çalışmada oluşturulan sistemin performansını ölçmek için 10-lu çapraz geçerlilik testi uygulanmıştır. Yapılan çalışma sonucunda ortalama %95,05 ve en yüksek %95,93 sınıflandırma doğruluğu görülmüştür.

8. SONUÇLAR VE ÖNERİLER

8.1 Sonuçlar

Uygulama 1 ile oluşturulan ağların 5-li çapraz geçerlilik testi sonucu ortalama sınıflandırma doğrulukları %90,61 olarak ölçülmüştür. En yüksek sınıflandırma doğruluğu ise %92,45 olarak gözlenmiştir [5].

Uygulama 2 ile 10-lu çapraz geçerlilik testi sonucunda %95,05 ortalama sınıflandırma doğruluğu gözlemlenmiştir. En yüksek sınıflandırma doğruluğuna ise %95,93 ile ulaşılmıştır.

Uygulama 1 ile oltalama web sitelerinin tespit edilmesine yönelik bir sınıflandırma yapılmıştır. Araştırmacılar tarafından bu çalışma referans alınarak internete bağlı bir makineden ziyaret edilen web sitelerinin güvenli olup olmadığının anlık olarak tespit edilmesine yönelik bir uygulama geliştirilebilir [5].

Uygulama 2 ile oltalama yöntemi olarak adlandırılan sahte web sitelerinin tespit edilmesine yönelik bir AÖM tabanlı sınıflandırma yapılmıştır. Bu konu ile ilgili olarak araştırma ve geliştirme çalışmaları yapanlar tarafından bu çalışma örnek alınabilir. Bu sayede bir bilgi işlem makinesinin bağlandığı bir web sitesinin güvenli olup olmadığının anlık olarak tespit edilmesi ile ilgili olarak bir uygulama yapılabilir. Diğer akıllı sistem yöntemleri kullanılarak farklı performans sonuçları elde edilebilir.

Özellik 13 ve özellik 19 için tarafımızdan yeni iki kural önerilmiştir. Önerilen bu kurallar bu tez çalışması kapsamındaki uygulamalarda kullanılmıştır.

Özellik 13 için oluşturulan kuralda [62] meşru, şüpheli ve oltalama olmak üzere bir sınıflandırma yapılmıştır. Ancak veri seti incelendiğinde 13'üncü özniteliğin 1 ve -1 değerlerine sahip olduğu tarafımızdan tespit edilmiştir. Özellik 13 6560 adet meşru ve 4495 adet oltalama olmak üzere toplam 11055 adet örnekten oluşmaktadır. Bu sebeple özellik 13 için yeni bir kural tarafımızdan önerilmiştir. Özellik 13 için önerilen bu kural bu tez çalışması kapsamındaki uygulamalarda kullanılmıştır.

Özellik 19 için oluşturulan kuralda [62] meşru, şüpheli ve oltalama olmak üzere bir sınıflandırma yapılmıştır. Ancak veri seti incelendiğinde 19'uncu özniteliğin 1 ve 0 değerlerine sahip olduğu tarafımızdan tespit edilmiştir. Özellik 19 1279 adet meşru ve 9776 adet şüpheli olmak üzere toplam 11055 adet örnekten oluşmaktadır. Bu sebeple özellik 19 için yeni bir kural tarafımızdan önerilmiştir.

Özellik 19 için önerilen bu kural bu tez çalışması kapsamındaki uygulamalarda kullanılmıştır.

Web siteleri aracılığı ile bilgi işlem sistemlerine bilgi girişi yapılabilmekte, girilen bu bilgiler işlenebilmekte ve işlenen bilgiler çıktı olarak alınabilmektedir. Web siteleri günümüzde bilim, teknik, iş, eğitim, ekonomi vb. birçok alanda kullanılmaktadır. Bu yoğun kullanımından ötürü bilgisayar korsanları tarafından kötü amaçlar için de bir araç olarak kullanılabilmektedir. Bu kötü amaçlardan biri oltalama saldırısı olarak karşımıza çıkmaktadır. Oltalama saldırısı ile çeşitli yöntemler kullanılarak bir web sitesi veya sayfası taklit edilebilmektedir. Taklit edilen bu sahte web sitesi veya sayfası ile kullanıcıya ait kredi kartı bilgileri, kimlik bilgileri gibi bazı bilgiler elde edilebilmektedir.

Siber silahlarla yapılabilecek saldırılar gerekli tedbirler alınmadıkça klasik anlamda bildiğimiz savaşlar kadar etkili olabilecektir. Örnek olarak; baraj kapaklarının açılıp o bölgenin sular altında kalması, nükleer santrallerin kontrolünün ele geçirilmesi, elektrik santrallerinin çalışamaz bir duruma getirilmesi, doğal gaz tesislerindeki boruların basıncının arttırılıp havaya uçurulması, kara-deniz-hava ulaşımında aksaklıkların yapılması, haberleşmenin devre dışı bırakılması verilebilir. Bilişim dünyası günümüzde hızlı bir şekilde gelişmektedir. Donanımsal ve yazılımsal yeni ve etkili araçlar ortaya çıkmaktadır. Bu araçlar kullanılarak bir kuruma çok büyük zararlar verilebilir. Buna karşın bu araçlar kullanılarak yapılacak olan saldırılara karşı çok etkili önlemler alınabilir. Bilişim alanındaki gelişmeler özellikle kurum içerisindeki bilgi işlem personeli tarafından yakından takip edilmelidir. Onlara bu bağlamda çok büyük bir görev düşmektedir. Bilişim teknolojilerindeki hızlı ilerlemeler sonucunda yeni yeni kavramlar ortaya çıkmakta olduğundan bunların terim tanımlamaları ve kapsamları bir zorluk olarak karşımıza çıkabilir. Sanal dünyada işlenen suçların cezası net olarak ortaya konmalıdır. Bilgi güvenliği konusu çocukların bilgi iletişim araçlarıyla ilk tanıştığı andan itibaren başlamalıdır. Bilişim teknolojileri sürekli geliştiği için çocukların okula başladıkları andan itibaren tüm öğrenim hayatları boyunca her dönem teorik ve uygulamalı bir Bilgi Güvenliği Dersi verilmelidir. İş hayatına başlanıldığında ise temelden elde edilmiş olunan Bilgi Güvenliği Disiplini ile çalışılan kurumda bilgi güvenliği konusunda daha bilinçli, etkili, verimli ve dikkatli olunabilir. Tehditlerin önceden sezilip önlem alınabilmesi sağlanabilir [1].

8.2 Öneriler

Bu bölümde kurumsal bilgi güvenliğine yönelik bazı öneriler sunulmuştur. Şüphesiz bu öneriler tek başına yeterli değildir ve bu öneriler zamanla güncelliğini kaybedebilir. Daha önceden siber bir tehdide karşı alınmış bir önlem zamanla önemini kaybediyorsa daha etkili önlemlerin alınması gerekir. Örneğin kişisel bilgilerin güvenliği için her bilgisayarın bir şifresi olmalıdır. Bu şifre güçlü değilse bazı yazılımlarla kolayca çözülebilir. Güçlü bir şifre kullanılmasına rağmen klavyedeki tuş hareketlerini kaydeden bir yazılımla bu güçlü şifre de çözülebilir. Buna engel olmak için bilgisayara klavyedeki tuş hareketlerini kaydeden yazılımı tespit eden bir yazılım yüklenmelidir. Bu defa video kaydetme özellikli bir cep telefonu ya da gizli bir video kamera ile bilgisayara şifresi ile girmeye çalışan kişinin video kaydından o bilgisayarın şifresi de kolaylıkla öğrenilebilir. Bu ve bunun gibi konularda kurumdaki çeşitli birimler için birbirinden farklı kurumsal bilgi güvenliği politikaları uygulanabilir [1].

Kurumsal bilgi güvenliğine yönelik bazı öneriler [1]:

- Bir kurumda bilgi güvenliği konusunda bilgili, deneyimli ve bu konuda güncel gelişmeleri devamlı takip edebilen bir ekibin bulunması gereklidir.
- Bir kurumdaki çalışanlar, belirli zaman dilimlerinde bilgi güvenliği konusunda yapılacak çeşitli toplantılarla kurumdaki uzman bilgi işlem personeli tarafından bilgilendirilmelidir.
- Bir kurumdaki personel tarafından normal iş akışı için gerekli olan dosya gönderme ve almanın dışında özel olarak gönderilen ve alınan video, müzik, resim vb. gibi dosyalar gereksiz yere veri trafiği oluşturabilmekte ve o kurumdaki birçok sunucunun işlevini azaltabilmektedir.
- Bir kurumdaki gereksiz dosya trafiğini engellemenin önemli nedenlerinden biri sanayi casusluğu için özel olarak geliştirilmiş olan tuzak dosyalardır.
- Türkiye'deki birçok kurum ve kuruluştaki bilgisayarlarda ulusal işletim sistemimiz olan Pardus kullanılmaktadır [93]. Eğer kurumdaki bilgisayarlarda yüklü olan mevcut işletim sistemini kullanmak yerine

Pardus'un kullanılmasının önünde herhangi bir neden yoksa mümkün olduğu sürece daha çok bilgisayara Pardus'un kurulması önerilir.

- Kurum içerisinde iş akışı gereği sosyal ağ uygulamaları kullanılıyorsa sosyal mühendislik tehditlerine karşı dikkatli olunmalıdır. Çeşitli sosyal mühendislik teknikleri kullanılarak kurum dışından biri sahte bir hesapla kurumda çalışan biriyle iletişime geçip kurumla ilgili bazı gizli bilgileri elde edebilir. Saldırgan, elde ettiği bu bilgiler ile kurumda çalışan farklı bir kişi ile sahte bir hesap kullanarak iletişime geçebilir. Bu şekilde o kurumda çalışan kişinin güvenini kazanıp kurumla ilgili başka gizli bilgilere de ulaşabilir.
- Modern steganografi tekniği, bir mesajı veya veriyi farklı bir nesnenin içerisine gizli biçimde yerleştirmeyi esas almaktadır [94]. Bu mesajın dosya şekli; metin, ses, resim veya video biçiminde olabilir. Bu teknik kullanılarak bir kurumdan dışarıya bilgi sızdırılabilir. Bunu engellemek için taşınabilir veri depolama aygıtlarının kullanımının kurumdaki belirli yerlerde kısıtlanması gerekir.
- Belirli zaman aralıklarında bir kurumdaki ağa sızma testleri yapılmalıdır. Sızma testleri; iç ağ, dış ağ, web uygulamaları ve kablosuz ağlar üzerinde yapılmalıdır. Sızma testlerine, fiziksel güvenlik ve sosyal mühendislik testleri de dahil edilmelidir.
- Ulusal Siber Güvenlik Tatbikatları; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülmektedir. Kurumlar, bu tatbikatlara katılmalıdır.
- Secure Socket Layer (SSL), İnternet üzerinden gerçekleştirilen bilgi alışverişi aşamasında gizliliğin ve güvenliğin sağlanması için geliştirilmiş olan bir protokoldür. Bu protokol ile İnternet'te güvensiz ve saldırılara açık bir ortamda güvenli bir iletişim sağlanır. Veri, SSL protokolüyle karşı tarafa gönderilmeden önce belirli bir şifreleme algoritmasıyla şifrelenir. Bu sayede sadece doğru alıcı tarafından bu şifrenin çözülerek asıl verinin elde edilmesi sağlanmış olur [95]. Bir kurumdaki veri trafiği için SSL kullanılmalıdır.

- Bir kurum dışından kurum içindeki bilgi ve iletişim araçlarına erişilmek istenildiğinde Sanal Özel Ağ (Virtual Private Network (VPN)) bağlantıları kullanılmalıdır. Bu bağlantılar güçlü şifreler içermelidir.
- Windows işletim sistemi yüklü olan bir bilgisayardan, CD (Compact Disc) veya DVD (Digital Versatile Disc)'den açılabilen bir Linux işletim sistemi ile kolay bir şekilde bilgisayardaki veriler kopyalanabilir. Bir kurumdaki bilgisayarlardan veri sızdırılmasını engellemek için Veri Kaçağı Önleme (Data Leakage Prevention (DLP)) çözümleri kullanılmalıdır.
- Bir kurumdaki ağa bağlı olan tüm cihazların olay günlükleri bir merkezden gerçek zamanlı olarak toplanmalıdır.
- Yapay zekâ temelli Bilgi Güvenliği Yönetim Sistemi (BGYS) kullanılarak bir kuruma yapılabilecek olası bir saldırıya karşı anında kendi kendine müdahale geliştirebilen etkili sistemler oluşturulmalıdır.

9. KAYNAKLAR

[1] M. Kaytan ve D. Hanbay, "Kurumsal Bilgi Güvenliğine Yönelik Tehditler ve Alınması Önerilen Tedbirler", 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (1st International Symposium on Digital Forensics and Security, ISDFS'13), pp.267-270, 2013, Fırat Üniversitesi, Elazığ.

[2] Y. Vural ve Ş. Sağıroğlu, "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), pp.507-522, 2008.

[3] K. Geers, "The challenge of cyber attack deterrence", Computer Law & Security Review, 26(3), pp.298-303, 2010.

[4] D. Hanbay, A. Baylar ve M. Batan, "Prediction of aeration efficiency on stepped cascades by using least square support vector machines", Expert Systems with Applications, 36(3), pp.4248-4252, 2009.

[5] M. Kaytan ve D. Hanbay, "Oltalama Yöntemi ile İnternet Sitelerine Yapılan Saldırıların Yapay Sinir Ağı Temelli Akıllı Sistem ile Belirlenmesi", Uluslararası Doğa Bilimleri ve Mühendislik Konferansı (International Conference on Natural Science and Engineering, ICNASE'16), pp.3221-3226, 2016, Kilis 7 Aralık Üniversitesi, Kilis.

[6] M. He, S.-J. Horng, P. Fan, M. K. Khan, R.-S. Run, J.-L. Lai, R.-J. Chen ve A. Sutanto, An efficient phishing webpage detector, Expert Systems with Applications, 38(10), pp.12018-12027, 2011.

[7] K. L. Chiew, E. H. Chang, S. N. Sze ve W. K. Tiong, "Utilisation of website logo for phishing detection", Computers & Security, 54, pp.16-26, 2015.

[8] R. Singh, H. Kumar ve R. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine", Expert Systems With Applications, 42(22), pp.8609-8624, 2015.

[9] J. M. Fossaceca, T. A. Mazzuchi ve S. Sarkani, "MARK-ELM: Application of a novel Multiple Kernel Learning framework for improving the robustness of Network Intrusion Detection", Expert Systems with Applications, 42(8), pp.4062-4080, 2015.

[10] Y. Wang, D. Li, Y. Du ve Z. Pan, "Anomaly detection in traffic using L1-norm minimization extreme learning machine", Neurocomputing, 149, pp.415-425, 2015.

[11] C. R. Pereira, R. Y. Nakamura, K. A. Costa ve J. P. Papa, "An Optimum-Path Forest framework for intrusion detection in computer networks", Engineering Applications of Artificial Intelligence, 25(6), pp.1226-1234, 2012.

[12] Á. Herrero, M. Navarro, E. Corchado ve V. Julián, "RT-MOVICAB-IDS: Addressing real-time intrusion detection", Future Generation Computer

Systems, 29(1), pp.250-261, 2013.

[13] P. Wang ve Y.-S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier", Journal of Computer and System Sciences, 81(6), pp.1012-1026, 2015.

[14] N. N. El-Emam ve R. A. S. AL-Zubidy, "New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm", The Journal of Systems and Software, 86(6), pp.1465-1481, 2013.

[15] K. Singh, S. C. Guntuku, A. Thakur ve C. Hota, "Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests", Information Sciences, 278, pp.488-497, 2014.

[16] S. Mukherjee ve N. Sharma, "Intrusion Detection using Naive Bayes Classifier with Feature Reduction", Procedia Technology, 4, pp.119-128, 2012.

[17] W. Wang, H. Wang, B. Wang, Y. Wang ve J. Wang, "Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks", Information Sciences, 220, pp.580-602, 2013.

[18] G.-Y. Chan, C.-S. Lee ve S.-H. Heng, "Discovering fuzzy association rule patterns and increasing sensitivity analysis of XML-related attacks", Journal of Network and Computer Applications, 36(2), pp.829-842, 2013.

[19] G. Suarez-Tangil, E. Palomar, A. Ribagorda ve I. Sanz, "Providing SIEM systems with self-adaptation", Information Fusion, 21, pp.145-158, 2015.

[20] M. Baykara, R. Daş ve İ. Karadoğan, "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (1st International Symposium on Digital Forensics and Security, ISDFS'13), pp.231-239, 20-21 May 2013, Fırat Üniversitesi, Elazığ.

[21] M. Kartal, Ş. Sağıroğlu ve H. İ. Bülbül, "IPV6'da Güvenlik Açıklarına Genel Bir Bakış", Politeknik Dergisi, 16(3), pp.119-127, 2013.

[22] F. Ertam, T. Tuncer ve E. Avcı, "Adli Bilişimde Ağ Cihazlarının Önemi Ve Güvenilir Yapılandırmaları", E-Journal of New World Sciences Academy, 8(3), pp.171-181, 2013.

[23] H. Şentürk, C. Z. Çil ve Ş. Sağıroğlu, "Siber Güvenlik Yatırım Kararları Üzerine Literatür İncelemesi", Politeknik Dergisi, 19(1), pp.39-51, 2016.

[24] O. Can ve Ö. K. Şahingöz, "Yapay Sinir Ağı Tabanlı Saldırı Tespit Sistemi", 23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı (23nd Signal Processing and Communications Applications Conference, SIU'15), IEEE (Institute of Electrical and Electronics Engineers) Conference Publications, pp.2302-2305, 2015, İnönü Üniversitesi, Malatya.

[25] E. N. Yılmaz, H. İ. Ulus ve S. Gönen, "Bilgi Toplumuna Geçiş ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, 8(3), pp.133-146, 2015.

[26] E. B. Ceyhan ve Ş. Sağıroğlu, "Kablosuz Algılayıcı Ağlarda Güvenlik Sorunları ve Alınabilecek Önlemler", Politeknik Dergisi, 16(4), pp.155-163, 2013.

[27] A. Saied, R. E. Overill ve T. Radzik, "Detection of known and unknown DDoS attacks using Artificia Neural Networks", Neurocomputing, 172, pp.385-393, 2016.

[28] D. Grzonka, J. Kołodziej, J. Tao ve S. U. Khan, "Artificial Neural Network support to monitoring of the evolutionary driven security aware scheduling in computational distributed environments", Future Generation Computer Systems, 51, pp.72-86, 2015.

[29] V. Santhana Lakshmi ve M. Vijaya, "Efficient prediction of phishing websites using supervised learning algorithms", Procedia Engineering, 30, pp.798-805, 2012.

[30] C. K. Olivo, A. O. Santin ve L. S. Oliveira, "Obtaining the threat model for e-mail phishing", Applied Soft Computing, 13(12), pp.4841-4848, 2013.

[31] R. Islam ve J. Abawajy, "A multi-tier phishing detection and filtering approach", Journal of Network and Computer Applications, 36(1), pp.324-335, 2013.

[32] X. Chen, I. Bose, A. C. M. Leung ve C. Guo, "Assessing the severity of phishing attacks: A hybrid data mining approach", Decision Support Systems, 50(4), pp.662-672, 2011.

[33] Y. Li, L. Yang ve J. Ding, "A minimum enclosing ball-based support vector machine approach for detection of phishing websites", Optik, 127(1), pp.345-351, 2016.

[34] R. Gowtham ve I. Krishnamurthi, "A comprehensive and efficacious architecture for detecting phishing webpages", Computers & Security, 40, pp.23-37, 2014.

[35] Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, "Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu", 2015 Yılı 4. Çeyrek Ekim – Kasım – Aralık, Bilgi Teknolojileri ve İletişim Kurumu, Mart 2016, Ankara.

[36] M. Tekerek, "Bilgi Güvenliği Yönetimi", Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11(1), pp.132-137, 2008.

[37] G. Canbek ve Ş. Sağıroğlu, "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23(1-2), pp.1-12, 2007.

[38] M. N. Öğün ve A. Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri Dergisi, (18), pp.145-181, 2013.

[39] Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu, Nihai Rapor, Sürüm 1.0, Kamu Bilişim Platformu 17, Kamu Bilişim Merkezleri Yöneticileri Birliği (Kamu-BİB), Türkiye Bilişim Derneği (TBD), 5 Ekim 2015.

[40] ENISA Threat Landscape 2015, European Union Agency for Network and Information Security (ENISA), Ocak 2016.

[41] Phishing Activity Trends Report, Anti Phishing Working Group (APWG), 1st-3rd Quarters 2015.

[42] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya ve J. Kalita, "Network attacks: Taxonomy, tools and systems", Journal of Network and Computer Applications, 40, pp.307-324, 2014.

[43] M. Albanese, E. Battista ve S. Jajodia, "A Deception Based Approach for Defeating OS and Service Fingerprinting", Conference on Communications and Network Security (CNS), IEEE (Institute of Electrical and Electronics Engineers) Conference Publications, pp.317-325, 2015.

[44] Siber Güvenliğe İlişkin Temel Bilgiler, Ulusal Siber Olaylara Müdahale Merkezi, Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, pp.10, 2014.

[45] ESET Smart Security 6 Kullanıcı Kılavuzu, ESET, 2013.

[46] Ö. Can ve M. F. Akbaş, "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", Türk Bilim ve Araştırma Vakfı (TUBAV) Bilim Dergisi, 7(2), pp.16-31, 2014.

[47] AVG Anti-Virus 2012 Kullanıcı Kılavuzu, AVG Technologies, pp.50, 2012.

[48] A. Arış, S. F. Oktuğ ve S. B. Ö. Yalçın, "Nesnelerin Interneti Güvenliği: Servis Engelleme Saldırıları", 23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı (23nd Signal Processing and Communications Applications Conference, SIU'15), IEEE (Institute of Electrical and Electronics Engineers) Conference Publications, pp.903-906, 2015.

[49] O. Osanaiye, K.-K. R. Choo ve M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework", Journal of Network and Computer Applications, 67, pp.147-165, 2016.

[50] U. Yavanoğlu, Ş. Sağıroğlu ve İ. Çolak, "Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler", Politeknik Dergisi, 15(1), pp.15-27, 2012.

[51] Ş. Sağıroğlu, E. N. Yolaçan ve U. Yavanoğlu, "Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi", Gazi Üniversitesi Mühendislik-Mimarlık

Fakültesi Dergisi, 26(2), pp.325-340, 2011.

[52] G. Bölük, "Akıllı Şebekelerde Ağ Güvenliği", 2. Uluslararası İstanbul Akıllı Şebekeler ve Şehirler Kongre ve Fuarı (2nd International Istanbul Smart Grids and Cities Congress and Fair, ICSG) Bildiri Kitabı, pp.222-229, 2014, İstanbul.

[53] H. Holm, "Performance of automated network vulnerability scanning at remediating security issues", Computers & Security, 31(2), pp.164-175, 2012.

[54] S. Alneyadi, E. Sithirasenan ve V. Muthukkumarasamy, "A survey on data leakage prevention systems", Journal of Network and Computer Applications, 62, pp.137-152, 2016.

[55] İnternet:http://www.scmagazine.com/2015-sc-awards-us-finalists-round-four/article/392362/, Erişim Tarihi: 01.03.2016.

[56] M. Lichman, UCI Machine Learning Repository Phishing Websites Data Set, School of Information and Computer Sciences, University of California, Irvine, İnternet:http://archive.ics.uci.edu/ml/datasets/Phishing+Websites#, Erişim Tarihi: 24.03.2016.

[57] R. M. Mohammad, F. Thabtah ve L. McCluskey, "An Assessment of Features Related to Phishing Websites using an Automated Technique", The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), 2012, London.

[58] R. M. Mohammad, F. Thabtah ve L. McCluskey, "Predicting phishing websites based on self-structuring neural network", Neural Computing and Applications, 25(2), pp.443-458, 2014.

[59] R. M. Mohammad, F. Thabtah ve L. McCluskey, "Intelligent rule-based phishing websites classification", IET Information Security, 8(3), pp.153-160, 2014.

[60] M. Lichman, İnternet:http://archive.ics.uci.edu/ml/machine-learning-databases/00327/, School of Information and Computer Sciences, University of California, Irvine, Erişim Tarihi: 24.03.2016.

[61] University of California, Irvine, School of Information and Computer Sciences, İnternet:http://archive.ics.uci.edu/ml/machine-learning-databases/00327/Training%20Dataset.arff, School of Information and Computer Sciences, University of California, Irvine, Erişim Tarihi: 24.03.2016.

[62] University of California, Irvine, School of Information and Computer Sciences, İnternet:http://archive.ics.uci.edu/ml/machine-learning-databases/00327/Phishing%20Websites%20Features.docx, School of Information and Computer Sciences, University of California, Irvine, Erişim Tarihi: 24.03.2016.

[63] R. B. Basnet, A. H. Sung ve Q. Liu, "Rule-Based Phishing Attack Detection", International Conference on Security and Management (SAM'11), Las Vegas,

Nevada, USA, July 18-21, 2011.

[64] İnternet:http://w3techs.com/, Erişim Tarihi: 05.04.2016.

[65] İnternet:http://who.is/, Erişim Tarihi: 19.04.2016.

[66] Y. Pan ve X. Ding, "Anomaly Based Web Phishing Page Detection", 22nd Annual Computer Security Applications Conference (ACSAC'06), IEEE (Institute of Electrical and Electronics Engineers) Conference Publications, pp.381-392, 2006, Miami Beach, Florida, USA.

[67] İnternet:http://www.alexa.com/, Erişim Tarihi: 19.04.2016.

[68] İnternet:http://backlinko.com/google-ranking-factors, Erişim Tarihi: 19.04.2016.

[69] İnternet:http://www.phishtank.com/stats.php, Erişim Tarihi: 19.04.2016.

[70] İnternet:https://www.stopbadware.org/top-50, Erişim Tarihi: 19.04.2016.

[71] İnternet:https://www.phishtank.com/stats/2012/10/, Erişim Tarihi: 22.04.2016.

[72] E. B. Ceyhan, Ş. Sağıroğlu ve E. Akyıl, "Parmak İzi Öznitelik Vektörleri Kullanılarak YSA Tabanlı Cinsiyet Sınıflandırma", Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 29(1), pp.201-207, 2014.

[73] R. Tekin, Y. Kaya ve M. E. Tağluk, "K-means ve YSA temelli Hibrit Bir Model ile Epileptik EEG İşaretlerinin Sınıflandırılması", Elektrik-Elektronik ve Bilgisayar Sempozyumu (FEEB 2011), pp.277-283, 2011, Fırat Üniversitesi, Elazığ.

[74] D. Hanbay, I. Turkoglu ve Y. Demir, "An expert system based on wavelet decomposition and neural network for modeling Chua's circuit", Expert Systems with Applications, 34(4), pp.2278-2283, 2008.

[75] D. Hanbay, I. Turkoglu ve Y. Demir, "Prediction of wastewater treatment plant performance based on wavelet packet decomposition and neural networks", Expert Systems with Applications, 34(2), pp.1038-1043, 2008.

[76] D. Hanbay, I. Turkoglu ve Y. Demir, "Modeling switched circuits based on wavelet decomposition and neural networks", Journal of the Franklin Institute, 347(3), pp.607-617, 2010.

[77] D. Hanbay, İ. Türkoğlu ve Y. Demir, "Chua Devresinin Yapay Sinir Ağı ile Modellenmesi", Fırat Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 19(1), pp.67-72, 2007.

[78] G.-B. Huang, Q.-Y. Zhu ve C.-K. Siew, "Extreme learning machine: Theory and applications", Neurocomputing, 70(1-3), pp.489-501, 2006.

[79] M. Luo ve K. Zhang, "A hybrid approach combining extreme learning machine and sparse representation for image classification", Engineering Applications of

Artificial Intelligence, 27, pp.228-235, 2014.

[80] G.-B. Huang ve L. Chen, "Convex incremental extreme learning machine", Neurocomputing, 70(16-18), pp.3056-3062, 2007.

[81] J. Tang, C. Deng, G.-B. Huang ve B. Zhao, "Compressed-Domain Ship Detection on Spaceborne Optical Image Using Deep Neural Network and Extreme Learning Machine", IEEE Transactions on Geoscience and Remote Sensing, 53(3), pp.1174-1185, 2015.

[82] G.-B. Huang, "An Insight into Extreme Learning Machines: Random Neurons, Random Features and Kernels", Cognitive Computation, 6(3), pp.376-390, 2014.

[83] X.-g. Zhao, G. Wang, X. Bi, P. Gong ve Y. Zhao, "XML document classification based on ELM", Neurocomputing, 74(16), pp.2444-2451, 2011.

[84] G. Wang, Y. Zhao ve D. Wang, "A protein secondary structure prediction framework based on the Extreme Learning Machine", Neurocomputing, 72(1-3), pp.262-268, 2008.

[85] B. Lu, G. Wang, Y. Yuan ve D. Han, "Semantic concept detection for video based on extreme learning machine", Neurocomputing, 102, pp.176-183, 2013.

[86] Y. Xu, Z. Y. Dong, J. H. Zhao, P. Zhang ve K. P. Wong, "A Reliable Intelligent System for Real-Time Dynamic Security Assessment of Power Systems", IEEE Transactions on Power Systems, 27(3), pp.1253-1263, 2012.

[87] K. Choi, K.-A. Toh ve H. Byun, "Incremental face recognition for large-scale social network services", Pattern Recognition, 45(8), pp.2868-2883, 2012.

[88] L. An ve B. Bhanu, "Image Super-Resolution by Extreme Learning Machine", 19th IEEE (Institute of Electrical and Electronics Engineers) International Conference on Image Processing (ICIP), pp.2209-2212, 2012, Orlando, ABD.

[89] G.-B. Huang, Q.-Y. Zhu ve C.-K. Siew, "Extreme Learning Machine: A New Learning Scheme of Feedforward Neural Networks", Proceedings of IEEE (Institute of Electrical and Electronics Engineers) International Joint Conference on Neural Networks, 2, pp.985-990, 2004.

[90] D. Serre, "Matrices:Theory and Applications", Springer, New York, 2002.

[91] G. Orekici Temel, S. Erdoğan ve H. Ankaralı, "Sınıflama Modelinin Performansını Değerlendirmede Yeniden Örnekleme Yöntemlerinin Kullanımı", Bilişim Teknolojileri Dergisi, 5(3), pp.1-7, 2012.

[92] The European Union Agency for Network and Information Security (ENISA), "Overview of current and emerging cyber-threats", ENISA Threat Landscape (ETL) 2014, The European Union Agency for Network and Information Security (ENISA), pp.39, Aralık 2014.

[93] İnternet:http://www.tubitak.gov.tr/tr/haber/pardusun-2013-surumu-kullanima-sunuldu, Erişim Tarihi: 07.04.2013.

[94] Y. Yalman ve İ. Ertürk, "Kişisel Bilgi Güvenliğinin Sağlanmasında Steganografi Biliminin Kullanımı", Bilgi Çağında Varoluş: "Fırsatlar ve Tehditler" Sempozyumu, Üniversite ve Araştırma Kütüphanecileri (ÜNAK) Derneği, pp.215, 2009, İstanbul.

[95] İnternet:http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/sertifika-sertifika-olusturma-sertifika-turleri.html, Erişim Tarihi: 16.04.2016.

ÖZGEÇMİŞ

Ad Soyad : Mustafa KAYTAN

Doğum Yeri ve Tarihi : ŞANLIURFA - 07.02.1974

Adres : Harran Üniversitesi
Teknik Bilimler Meslek Yüksekokulu
Bilgisayar Teknolojileri Bölümü
Bilgisayar Programcılığı Programı, ŞANLIURFA

E-Posta : mkaytan@harran.edu.tr

Lisans : Lefke Avrupa Üniversitesi
Mimarlık ve Mühendislik Fakültesi
Bilgisayar Mühendisliği, (K.K.T.C.-2002)

Mesleki Deneyim : Harran Üniversitesi Öğretim Görevlisi (2009-)

Yayın Listesi:

TEZDEN TÜRETİLEN YAYINLAR

- M. Kaytan, D. Hanbay, "Kurumsal Bilgi Güvenliğine Yönelik Tehditler ve Alınması Önerilen Tedbirler", 1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu (1st International Symposium on Digital Forensics and Security, ISDFS'13), Fırat Üniversitesi, 2013
- M. Kaytan, D. Hanbay, "Oltalama Yöntemi ile İnternet Sitelerine Yapılan Saldırıların Yapay Sinir Ağı Temelli Akıllı Sistem ile Belirlenmesi", Uluslararası Doğa Bilimleri ve Mühendislik Konferansı (International Conference on Natural Science and Engineering, ICNASE'16), Kilis 7 Aralık Üniversitesi, 2016
- D. Hanbay, M. Kaytan, "Effective Classification of Phishing Web Pages Based on New Rules by Using Extreme Learning Machines", (Uluslararası hakemli dergi yayını olarak hazırlanmış ve değerlendirilmek üzere dergiye gönderilmiştir.)