SETSCI Conference Indexing System,
Volume 3 (2018), 1384-1390

ISAS 2018-Winter
2nd International Symposium on Innovative Approaches in Scientific Studies
November 30 – December 2, 2018, Samsun, Turkey

Siber Savunma Alanında Yapay Zekâ Tabanlı Saldırı Tespiti ve Analizi

Burcu AYTAN[1], Necaattin BARIŞÇI[2]

Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ankara-TÜRKİYE

[*]Sorumlu Yazar:burcukalayciaytan@gmail.com
[+]Konuşmacı: burcukalayciaytan@gmail.com
Sunum/Makale Türü: Oral / Tam Metin

Özet – Bilgi ve bilgisayar teknolojilerinin hızlı gelişimi, hız ve verimlilik artışı ve kolaylık sağlaması nedeniyle birçok bilgi elektronik ortamlara aktarılmıştır. Elektronik ortamların yaygınlaşması; kişisel veya kurumsal açıdan önemli bir bilginin başkalarının eline geçmesi, maddi ve manevi zararlara yol açması gibi sorunları da ortaya çıkarmıştır.

Korunacak bilginin değerine göre farklılık gösterebilecek olan koruma sistemlerinin aslında tek amacı, saldırganlara ve saldırılara karşı önlem alarak, bilginin mahremiyetinin korunmasıdır. Özellikle kamu kurum ve kuruluşlarının itibarını kaybetmesine neden olabilecek bilginin gizliliği, bütünlüğü ve erişilebilirliğinin bozulması yönünde yapılan saldırılara karşı sistem güvenlik uzmanları önlem almaya çalışmakta ve sistemin kaynaklarını yetkisiz erişimden korumaktadır. Bilgiyi korurken, var olan sistemlerin sürekliliğinin sağlanması, yapılan saldırılara karşı alınan önlemlerin güncelliğinin korunması, değişen saldırı ve yöntemlerin bilinmesi ve var olan sisteme adapte edilmesi gerekmektedir.

Günümüzde bilgi ve bilgisayar güvenliğinin öneminin kavranmasıyla geliştirilen araçlardan biri olan Saldırı Tespit Sistemleri ile sistemlere yapılan yetkisiz erişimler ve kötüye kullanımlar tespit edilerek, bunların yol açabileceği zararlar engellenmeye çalışılmaktadır.

Bu çalışmada saldırı tespit sistemleriyle ilgili uygulamalarda en çok kullanılan veri setlerinden biri olan "KDD Cup'99" veri seti kullanılarak hizmet dışı bırakma saldırıları ve bilgi tarama saldırıları Weka aracında yer alan makine öğrenme algoritmaları ile tespit edilmeye çalışılmış ve yüzde doksan dokuz oranında başarı sağlanmıştır.

Anahtar Kelimeler – Saldırı Tespit Sistemleri, Bilgisayar Ağlarında Anormallik Tespiti, Siber Saldırılar, Makine Öğrenmesi, Yapay Zeka

Abstract - Vast amount of information has been transferred into electronic media due to the rapid development of computer technologies, increase of speed and efficiency as well as ease of use. The fact that the electronic media become widespread has also resulted in various problems such as taking the possession of information which have personal and corporate importance to third persons and causing pecuniary losses and intangible damages.

The sole purpose of the protection systems which may dffer according to value of the information to be protected is to protect the confidentiality of the information by taking measures against the attacks and attackers. In order to prevent public bodies and institutions from losing their reputation in particular, system security experts are trying to take measures against the attacks that aim to harm confidentiality, integrity and accessibility of the information and they protect the system resources from unauthorized access. While protecting the information, it is necessary to maintain the continuity of the existing systems, update the measures against the potential attacks, have knowledge of changing attacks and methods as well as adapting all these actions to the existing system.

Today, intrusion detection systems which are one of the tools developed in parallel to the understanding the importance of information and computer security, are utilized to detect unauthorized access and abuse of systems thereby preventing potential damages to be caused by them.

In this study, it has been tried to identify attacks for rendering inoperable and information retrieval thanks to the machine learning algorithms in Weka tool by using the "KDD Cup 99" data set that is one of the commonly used data sets in the applications for intrusion detection systems and so ninety-nine percent success has been achieved at the end of the study.

Keywords: *Intrusion Detection Systems, Anomaly Detection in Computer Networks, Cyber Attacks, Machine Learning, Artificial Intelligence*

I. GİRİŞ

Siber Güvenlik, siber ortamda; kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür [1]. Siber saldırı girişimlerinde düşman olarak belirlenen hedefe saldırıda bulunmak, karşı savunma yapmak, hedefteki siber uzayda istihbarat verileri toplamak siber savaş faaliyetlerini oluşturmaktadır. Siber savaşların ana hedefi ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık, kamu hizmetleri gibi kritik sektörlerinin bilgi sistem altyapılarıdır.

Siber saldırı; dünyanın herhangi bir yerindeki bilgisayar kontrolü altındaki sistemlere internet ortamından izinsiz erişip kritik alt yapının yönetimini ele geçirmeye çalışmaktır. Siber saldırının silahları ise internet ortamına bağlı bir bilgisayarın tuşları, bu tuşlara dokunan parmaklar ve yazılımlardır [2]. Etkin ağlarda siber saldırı ile tüm alt yapılar bir anda yerle bir edilebilir, en güçlü ülke bile hareket edemez hale getirilebilir. Etkin ağlarda dinamik olarak gelişen saldırılara karşı savunmak için geleneksel sabit algoritmalar ile yazılım geliştirmek güçtür. Bu durum, yazılım esnekliği ve öğrenme yeteneği sağlayan yapay zekâ yöntemleri uygulanarak ele alınabilir [3].

Bilgisayar sistemlerinde karşılaşılan birçok saldırı türü mevcuttur. Sistem kesintisi, erişim kısıtlama, verileri bozma veya çalma, içerik değiştirme gibi amaçlar edinilerek saldırılar düzenlenmektedir. Hizmet kesintisi saldırıları, sistemin yoğun istekler sonucu cevap veremez hale gelmesini sağlayan saldırılardır. Yetkisiz veya izinsiz erişim ile yapılan saldırılar, şifre kırıcılar ve keylogger gibi araçlar ile yapılan ve bilgi ifşa eden saldırılardır.

Bilgisayar veya ağ sistemlerine yapılan saldırıları tespit ederek güvenliğin sağlanması için geliştirilen sistemler, her ne kadar yapılan saldırıların büyük bir çoğunluğunu tespit edebilseler de daha önce hiç karşılaşılmamış olan saldırıların büyük çoğunluğunu tespit edememektedir [4]. Bu saldırıların sistemlerde büyük zararlara yol açması, yeni saldırı çeşitlerinin tespit edilebilmesi, hızla değişen saldırı tiplerinin karşısında, bilgi ve bilgisayar güvenliğinin sağlanması amacıyla bu sistemlerin geliştirilmesinde yapay zekâ yöntemleri kullanılması hedeflenmektedir.

Saldırı tespit sistemlerinde, saldırı tespit yöntemi olarak anormallik tespiti ve kötüye kullanım tespiti olmak üzere iki farklı yaklaşım kullanılmaktadır. Anormallik tespitine dayanan yaklaşım; sistemdeki kullanıcıların davranışlarını modellerken, kötüye kullanım tespitine dayanan yaklaşım saldırganların davranışlarını modeller [5].

Saldırıların tanınması ve önceden tespit edilmesi, ayrıca gelebilecek saldırıların tahmin edilerek uyarı verilmesi veri madenciliği ve yapay zekâ gibi yöntemler ile sağlanabilir.

Zeki yaklaşımların kullanılmaya başlaması ile birlikte anormallik tespiti yaklaşımı biraz daha ön plana çıkmış ve bu sayede anormallik tespitinin yeni saldırıları tespit edebilme yeteneği arttırılmıştır. Yapay zekâ araştırmacılarının baştan beri ulaşmak istediği ideal, insan gibi düşünen ve davranan sistemler geliştirmektir.

Son yıllarda ağ teknolojilerinde yaşanan baş döndürücü gelişmeler hemen her işin bilgisayar ağları üzerinden yapılmasını mümkün hale getirmiştir. Bilgisayar sistemleri ve bilgisayar ağlarının gelişmesi ile aya insan göndermek, uluslararası ticaret yapmak, pilotsuz uçakları savaştırmak gibi işler yapılabilir hale gelmiştir. Fakat insanlar bunlara rağmen bilgisayar sistemleri ve bilgisayar ağlarına tam olarak güvenememektedirler. Güvensizliğin temelinde ise bilgi-işlemin saldırılar karşısında tam başarılı olamaması vardır. Güvenlik, sağlam bir mühendislik ve sosyal altyapı gerektirmektedir [6].

Ağ üzerinden gelen saldırıları tespit etmek için imza tabanlı saldırı tespiti ve anormal durum tespiti olmak üzere iki temel yöntem kullanılmaktadır. İmza tabanlı yaklaşımda veri tabanında yer alan yani önceden bilinen saldırılara ait imzalar kullanılır. Bu yöntemdeki en önemli problem imzaların saldırganlar tarafından değiştirilebilme durumudur. Bu nedenle bilinen saldırıları tespit ederken iyi sonuç üretmesine rağmen veri tabanında yer almayan saldırı tiplerini bulmakta yetersiz kalmaktadır. Saldırı, sistemin normal davranışından farklıdır. Anormallik tabanlı Saldırı tespit sistemleri normal ağ trafiği ile şüpheli trafiği birbirinden ayıracak mekanizmalara sahiptir. İlk önce hangi trafiğin normal olduğu tanımını yaparak başlarlar, arkasından gelen ağ paketleri bu tanıma göre normal veya anormal (saldırı) olarak sınıflandırırlar [7]. Bu yaklaşımlar, bilinen saldırılar kadar bilinmeyen saldırıları da tespit edebilirler. Bundan ötürü, ağ saldırılarını tespit için anormal durumu belirlemeye yönelik makine öğrenmesi tabanlı sistemlerin kullanılması son yıllarda önem kazanmıştır.

II. LİTERATÜR ARAŞTIRMASI

Hanifi ve arkadaşları [8] ağ saldırılarının tespiti için KDD 99 veri seti kullanılarak k-ortalama algoritması ile yarı eğitmenli yeni bir anomallik tespit sistemi tasarlamış ve gerçekleştirmişlerdir. Eğitim aşamasında, normal örnekler k-ortalama algoritması uygulanarak kümelere ayrılmıştır. Sistem sadece normal veri tipleri ile eğitilmiştir. Çalışmanın sonunda, yarı-eğitmenli yaklaşımda k-ortalama kümeleme algoritması ile tasarlanan sistem yüzde 80.119 oranında doğruluk verisine ulaşmış ve sistem farklı algoritmalar ile de

denenmiştir. Rastgele Orman algoritması ile yüzde 80,67 oranında doğruluk elde edilmiştir.

Hasan ve arkadaşları [9] KDD 99 veri setindeki 41 özelliği 25'e indirmiş ve daha iyi sonuçlar elde etmişlerdir. Özelliklerin indirgenmesi doğru sonuç elde edilmesinde daha az zaman harcanmasını sağlamıştır. Bu yazıda, giriş özelliklerini azaltarak Rasgele Orman algoritması ile saldırı tespiti için performans iyileştirmesi yapılmıştır. Daha az sayıda özellik, işlem süresi açısından her zaman avantajlıdır. Elde edilen sonuçlar, Rasgele Orman sınıflandırmasının azaltılmış özelliklerle (25 özellik) kabiliyetinin, tüm özelliklerle (41 özellik) sınıflandırılmasından elde edilen sonuçtan daha doğru sonuç verdiğini göstermektedir. Ayrıca, Rasgele Orman ile 25 özelliği işlemek için gereken süre, 41 özellikli işlem süresinden daha küçüktür. 41 özellikli sınıflandırma ile 10.62 dakikalık eğitim süresinde %91.41 oranında doğruluk elde edilirken, 25 özellikli sınıflandırmada 7.98 dakikalık eğitim süresinde %91.90 oranında doğruluk elde edilmiştir.

Özgür ve Erdem çalışmalarında [10] sınıflandırıcı başarısını artırmak için, tek sınıflandırıcının yerine sınıflandırıcı füzyonu kullanımını önermektedir. Bu çalışmada; nitelik seçme ve sınıflandırıcı füzyonu ile ağırlık belirleme işlemlerinin, genetik algoritma (GA) kullanılarak yapılması önerilmektedir. Çoklu sınıflandırıcı füzyonunda sınıflandırıcı sayısının 2 ile 8 arasında olduğu doğrusal ağırlıklı birleştirme yöntemi kullanılmıştır. Kullanılan sınıflandırıcılar: Adaboost, Karar Ağacı, Lojistik Regresyon, Saf Bayes, Rastgele Orman, Gradient Boosting, En Yakın K Komşu ve Yapay Sinir Ağları (Çok Katmanlı Perseptron) olmuştur. Genetik Algoritma-Nitelik Sınıflandırma-Ağırlık Belirlemenin birlikte kullanımının tek sınıflandırıcı sonuçlarından daha başarılı olduğunu göstermiştir. Bu yöntem ile eğitim ve test süresi azaltılarak, doğruluk oranı değerleri daha yüksek bir sınıflandırıcı füzyonu elde edilmiştir. KDD99 veri setindeki 41 özellik yerine daha az özellik kullanılarak Nitelik Sınıflandırma yapılabileceği ve bu şekilde daha kısa sürede saldırıların tespit edilebileceği, tek bir algoritma kullanmak yerine birden fazla algoritmanın birleştirilerek doğruluk oranının arttırılabileceği belirtilmiştir.

Phyu Thi Htun ve Kyaw Thet Khaing [11] KDD99 veri setindeki DoS (Hizmet Reddi) saldırılarının (smurf, land, pod, teardrop, neptune, back) Random Forest algoritması ile tespit edilmesi sağlanmış ve %99.87 oranında doğruluk tespit edilmiştir. Bunu takip eden diğer sınıflandırıcı algoritma k-en yakın komşu algoritması %99.85 doğruluk oranına ulaşmıştır

III.MATERYAL VE METOD

Bilişim sistemlerinin gelişmesiyle, saldırı tespit sistemlerinin kullanımı önem kazanmıştır. Bu sistemlerin çalışması, genellikle sınıflandırma problemi çerçevesinde değerlendirilebilir. Günümüzde makine öğrenmesi yöntemleri bilgisayarların daha doğru eylemler gerçekleştirmesi amacıyla birçok farklı şekilde kullanılmaktadır. Makine öğrenmesi, bilgisayarların gerçekleştirdikleri eylemleri daha doğru bir hale getirmek üzere değiştirmesi veya uyarlaması olarak tanımlanabilir.

Makine öğrenmesini bilgisayarların bir başarım ölçütünü, örnek veri veya geçmiş deneyim kullanarak eniyilemesi olarak da tanımlayabiliriz [12].

Bir saldırı tespit sistemi hem kurumun hem de kurumun içinden gelen tehditleri içeren olası güvenlik tehditlerini tanımlamak için bir bilgisayardaki veya bir ağdaki farklı alanlardaki bilgileri toplar ve analiz eder. Uygulamaların güvenliklerinin test edildiği, kötü yazılım içerenlerinin tespit edilerek silindiği, kötü niyet içeren bağlantıların tespit edilerek reddedildiği güvenlik duvarı ve virüs programları gibi yazılımlar saldırıları büyük ölçüde engellemektedir; ancak olası saldırıların çeşitliliği ve büyüklüğü göz önüne alındığında bu yazılımlar yeterli olmamaktadır. Çözüm olarak öne çıkan Saldırı Tespit Sistemleri, bir ağın ya da sistemin yaptığı aktiviteleri kontrol ederek saldırıları tespit etmeye çalışan, engellemek için karşı girişimde bulunmayan gerçek zamanlı çalışan yazılım ürünleridir.

A. KDD99 Veri Kümesi

KDD 99; 1999 yılında DARPA veri kümesinin bazı önişlemlerden geçirilmesi ile elde edilmiş 41 özellikten oluşan bir veri kümesidir. Bu veri kümesinin amacı, son yıllarda farklı tekniklerle gerçekleştirilen Saldırı Tespit Sistemleri için eğitim ve test işlemlerinde kolaylık sağlamaktır. KDD veri kümesi ile eğitim ve test sonuçlarının daha hızlı alınabilmesi yapılan çalışmaların sonuca ulaşmasını kolaylaştıran bir faktör olmuştur. Bu nedenle bildiride sunulan çalışma KDD99 veri seti üzerinde gerçekleştirilmiştir.

KDD99 veri seti 4,8 milyon civarında kayıttan oluşmaktadır. Bu kayıtlar 22 tip saldırı ve normal ağ trafik paketlerinden oluşmaktadır. Veri setinin içerisinde 41 adet bağımsız 1 adet bağımlı değişken bulunmaktadır. Bu değişkenler 4 temel saldırı tipine ait kayıtlar içerir. Bağımsız değişkenler; ağa gelen bağlantı ile ilgili protokol türü, kullanılan servisler, bağlantının normal bir şekilde sonlanıp sonlanmadığı gibi bağlantı hakkındaki bilgiler, bir bağlantı içerisinde çalıştırılan komut sayısı ve yanlış giriş işlemi sayısı gibi gerçekleştirilen bağlantılarla ilgili çeşitli değerleri tutmaktadır. Bağımlı değişken ise kaydın normal bir bağlantı mı saldırı mı olduğunu belirtir. Bu veri setindeki her saldırı 4 ana gruba dahildir. Bu saldırı türlerini aşağıdaki şekilde ifade edebiliriz:

• *Hizmet Engelleme Saldırısı (Denial of Service Attack – DoS):* Bu saldırılar genel olarak TCP/IP protokol yapısındaki açıklardan faydalanılarak sistemin tüm kaynaklarını tüketip hizmet veremez hale getirmeye ve bir sunucuya birden çok bağlantı isteği göndererek yasal kullanıcıların hizmet almasını engellemeye yöneliktir.

• *Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi (User to Root Attack – U2R):* Bu tip saldırılarda sisteme erişim yetkisi olan fakat yönetici yetkilerine sahip olmayan bir

kullanıcının yönetici haklarını elde etmesidir. Genellikle sistem açıklarını kullanarak gerçekleştirilir.

• *Yönetici Hesabı ile Yerel Oturum Açma (Remote to Local Attack – R2L):* Kullanıcı yetkisine sahip olunmadığı durumda hedef ağdaki bilgisayara bazı paketler gönderilerek misafir ya da başka bir kullanıcı olarak izinsiz erişim yapılmasıdır.

• *Bilgi Tarama Saldırısı (Probing Attack):* Bu tür saldırılar bir sunucunun ya da herhangi bir makinanın geçerli IP adreslerini, ağdaki bilgisayar sayısını, bilgisayardaki kullanıcı sayısını ve kullanıcı bilgilerini, aktif giriş kapılarını (port) veya işletim sistemini öğrenmek için yapılırlar [13].

B. WEKA (Waikato Environment for Knowledge Analysis) Uygulaması

Yapılan testler WEKA (Waikato Environment for Knowledge Analysis) uygulaması üzerinde gerçeklenmiştir. WEKA, kullanımı ücretsiz, açık kaynak kodlu, içerisinde pek çok sınıflandırma, regresyon, demetleme, bağıntı kuralları, yapay sinir ağları algoritmaları ve önişleme metotları barındıran, yaygın kullanılan bir veri madenciliği aracıdır.

Model başarımının ölçülmesinde kullanılan en yaygın ölçüt, modele ait doğruluk oranıdır. Doğru sınıflandırılmış örnek sayısının (TP+TN), toplam örnek sayısına (TP+FP+FN+TN) oranıdır. Hata oranı ise bu değerin 1'e tamlayanıdır. Diğer bir ifadeyle yanlış sınıflandırılmış örnek sayısının (FP+FN), toplam örnek sayısına (TP+FP+FN+TN) oranıdır.

Burada;

• TP: True Positive – Doğru örneklerin doğru olarak sınıflandırılması
• TN: True Negative – Doğru örneklerin yanlış olarak sınıflandırılması
• FP: False Positive – Yanlış örneklerin doğru olarak sınıflandırılması
• FN: False Negative – Yanlış örneklerin yanlış olarak sınıflandırılmasını ifade etmektedir [14].

C. Makine Öğrenme Algoritmaları

Veri sınıflandırma için kullanılabilecek birçok makine öğrenme tekniği vardır.

1) Geri Yayılma (Back-Propagation) Algoritması

Geri yayılma algoritması, basitliği ve uygulamadaki görüş açısı gibi başarılarından dolayı ağ eğitimi için en popüler algoritmalardan biridir. Back-Propagation Neural Network (BPNN) modeli denetimli öğrenme modelidir. Bu algoritma; hataları geriye doğru çıkıştan girişe azaltmaya çalışmasından dolayı geri yayılım ismini almıştır. Geri yayılmalı öğrenme kuralı ağ çıkışındaki mevcut hata düzeyine göre her bir tabakadaki ağırlıkları yeniden hesaplamak için kullanılmaktadır. Çok katlı ağlarda hesap işlerini öğrenmede de kullanılabilmektedir. Geri yayılım ağında hatalar, ileri besleme aktarım işlevinin türevi tarafından, ileri besleme mekanizması içinde kullanılan aynı bağlantılar aracılığıyla, geriye doğru yayılmaktadır. Öğrenme işlemi, bu ağda basit çift yönlü hafıza birleştirmeye dayanmaktadır [15]. Back Propagation Algoritması, birçok pratik uygulama için çok geri kalmaktadır. Bu algoritmasının en büyük problemi, çok uzun eğitim süresine sahip olmasıdır.

2) Karar Ağacı

Karar ağacı verimli bir şekilde veri sınıflandırmak için kullanılan bir sınıflandırma algoritmasıdır. Karar Ağacı terminal olmayan düğümler (bir kök ve iç düğümleri) ve terminal düğümlerden (yaprak) oluşur. Karar ağacının hazırlanırken başlangıç noktası (kök), vereceğimiz karara, ağaç hazırlanırken her karar düğümünden çıkan dallar ise karar alternatiflerine karşılık gelmektedir. C4.5, Karar Ağacı oluşturmak için verimli ve popüler bir algoritmadır.

3) Ripper Kuralı

Ripper Kuralı, çeşitli gürültülü veri setlerini işleyebilen verimli bir kural-tabanlı öğrenme algoritmasıdır. Ripper Kural algoritması iki aşamadan oluşmaktadır. İlk aşama kural koşullarını başlatmak içindir. Bir sonraki aşama, bir kural optimizasyon tekniğini kullanır. Kurallar, if-then-else şeklindedir. Bir kural, koşul sağlanıncaya kadar her sınıf tek tek kabul edilir veya veri bir sınıf içinde sınıflandırılır.

4) Rasgele Orman Sınıflandırması

Rasgele Orman Sınıflandırması birden fazla karar ağacını kullanarak daha uyumlu modeller üreterek daha isabetli sınıflandırma yapmaya çalışan bir sınıflandırma modelidir [16].

Rastgele orman, her biri birbirinden bağımsız olarak ve aynı dağılım kullanılarak eğitim verisinden rastgele elde edilmiş bir örnekleme dayanan karar ağaçlarından oluşan bir topluluktur. Bu yöntem eğitim sırasında birçok karar ağacı oluşturur ve daha sonra kestirim sırasında bu karar ağaçlarının sınıflandırma sonuçlarından yararlanılarak, girdinin sınıfına çoğunluk oyu aracılığıyla karar verilir. Rastgele ormanın en önemli avantajı, karar ağaçlarındaki aşırı uyum sorununa bir çözüm getirmiş olmasıdır [12].

IV. ARAŞTIRMA BULGULARI

KDD99 veri kümesinde her veri 41 özelliğe sahiptir. Eğitim veri kümesi ve test veri kümesi olarak farklı veri setleri kullanılmıştır.

Tablo 1: Eğitim Veri Seti

Normal Kayıt Sayısı	Hizmet Engelleme Saldırılarından Oluşan Kayıt Sayısı	Bilgi Tarama Saldırılarından Oluşan Kayıt Sayısı
5000	Back: 250	Satan: 1000
	Teardrop: 100	Ipsweep: 750
	Neptune: 600	Nmap: 0
	Land: 20	Portsweep:750
	Smurf: 1400	
	Pod: 130	

Yapılan çalışmada KDD99 veri setinden eğitim için 10.000 kayıt alınmıştır. Bunların 5.000'i normal kayıt, 5.000'i ise saldırı verilerinden oluşan kayıtlardır. Saldırı verilerinin 2500 tanesi hizmet engelleme (DoS) saldırılarından, 2500 tanesi ise ağ tarama (Probe) saldırılarından oluşmaktadır.

KDD99 veri setinden seçilen test veri setlerinin her biri ise 5.000 kayıttan oluşmaktadır. Bunların 2.500 tanesi saldırı kaydı ve 2.500 tanesi ise normal kayıttan oluşmaktadır. Her veri kümesi içindeki saldırı kayıtları Hizmet Reddi ve Bilgi Tarama saldırı çeşitlerini içermektedir. Diğer saldırı türleri veri setinden silinmiştir.

Tablo 2: Test Veri Seti

Normal Kayıt Sayısı	Hizmet Engelleme Saldırılarından Oluşan Kayıt Sayısı	Bilgi Tarama Saldırılarından Oluşan Kayıt Sayısı
2500	Back: 200	Satan: 375
	Teardrop: 80	Ipsweep: 475
	Neptune: 70	Nmap: 0
	Land: 10	Portsweep: 400
	Smurf: 865	
	Pod: 25	

A. Geri Yayılma (Back-Propagation) Algoritması ile Saldırı Tespiti

Çalışmamızda ilk olarak Geri Yayılma (Back-Propagation) sınıflandırma tekniği kullanılmıştır. WEKA aracında bu sınıflandırma Multilayer Perceptron sınıflandırma olarak geçmektedir.

Eğitim veri kümesi eğitildikten sonra bir model olarak kaydedilir ve bu model Weka aracına yüklendikten sonra Test Veri Seti seçilerek test edilmeye başlanır. Test veri setinin oluşturulması önemlidir. Test veri seti, Eğitim veri setinden ayrı olmalıdır. Eğitim veri setinden seçilen veriler ile test yapılırsa %100'e çok yakın belki de %100 performans sağlanır. Çünkü bu şekilde gerçekleşen öğrenme çıkarımlardan oluşmaz. Bu nedenle KDD99 veri setinden rastgele alınan 2500 normal 1250 Hizmet Engelleme ve 1250 Bilgi Tarama saldırı verisi test için seçilmiştir.

- Toplam Algılama Oranı (TAO), Gerçek Zamanlı Saldırı Tespit Sisteminde doğru algılanabilen Hizmet Engelleme saldırıları, Bilgi Tarama saldırıları ve normal ağ verilerinin yüzdesidir.
- Normal Algılama Oranı (NAO), Gerçek Zamanlı Saldırı Tespit Sisteminde doğru algılanabilen normal sınıf yüzdesidir.
- Saldırı Tespit Oranı (STO), Gerçek Zamanlı Saldırı Tespit Sisteminde doğru algılanabilen tüm saldırı sınıflarının yüzdesidir.

Tablo 3: Geri Yayılma Algoritması İle Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Geri Yayılma	**99.8**	**100**	**99.8**	**828.48**

Geri Yayılma Algoritması çok katmanlı olduğu için eğitim süresi ve test süresi çok yüksektir. Algoritma normal verilerin tamamını doğru bulurken saldırı verilerinin bazılarını yanlış sınıflandırmıştır. Saldırı verisi olmasına rağmen 3 adet veri normal olarak gösterilmiştir. Test verilerinde kullanılan saldırı türleri ile eğitim verisinde kullanılan saldırı verileri aynı türdendir. Eğer test verisinde kullanılan verilerde saldırı türleri eğitim verisinden farklılık gösterirse alınan tespit oranlarında düşme yaşanır.

B. Karar Ağacı Algoritması ile Saldırı Tespiti

Weka aracında karar ağacı ile eğitim süresinin hesaplanması için J48 sınıflandırıcı seçilir. Karar ağaçlarının performansı yani eğitim süresi Geri Yayılma Algoritmasına göre çok daha iyidir.

Tablo 4: Test Veri Seti İle Eğitim Veri Setindeki Saldırı Türleri Aynı Olduğunda Karar Ağacı Algoritması İle Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Karar Ağacı	**99.8**	**99.8**	**99.8**	**0.69**

Test Veri Seti ile Eğitim Veri Setindeki saldırı türleri aynı olduğunda toplamda elde edilen tespit oranı ile normal ve atak tespit oranları aynıdır.

Eğitim veri kümesinde bilgi tarama saldırılarından olan Nmap yoktur. Ancak test veri kümesine Nmap taraması dahil edildiğinde algılama oranlarında farklılık oluşmaktadır.

Tablo 5: Test Veri Seti İle Eğitim Veri Setindeki Saldırı Türleri Farklı Olduğunda Eğitim Veri Seti

Normal Kayıt Sayısı	Hizmet Engelleme Saldırılarından Oluşan Kayıt Sayısı	Bilgi Tarama Saldırılarından Oluşan Kayıt Sayısı
5000	Back: 250	Satan: 1000
	Teardrop: 100	Ipsweep: 750
	Neptune: 600	Nmap: 0
	Land: 20	Portsweep:750
	Smurf: 1400	
	Pod: 130	

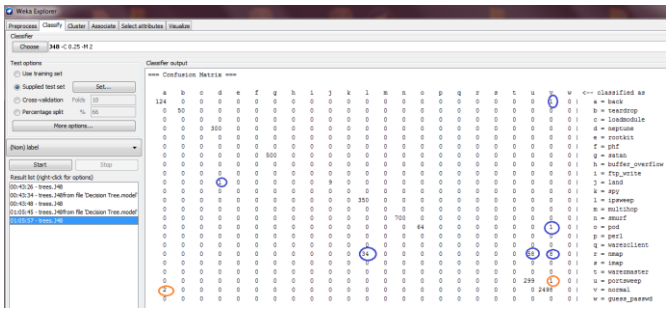
Tablo 6: Test Veri Seti İle Eğitim Veri Setindeki Saldırı Türleri Farklı Olduğunda Test Veri Seti

Normal Kayıt Sayısı	Hizmet Engelleme Saldırılarından Oluşan Kayıt Sayısı	Bilgi Tarama Saldırılarından Oluşan Kayıt Sayısı
2500	Back: 125	Satan: 500
	Teardrop: 50	Ipsweep: 350
	Neptune: 300	**Nmap: 100**
	Land: 10	Portsweep: 300
	Smurf: 700	
	Pod: 65	

Tablo 7: Test Veri Seti İle Eğitim Veri Setindeki Saldırı Türleri Farklı Olduğunda Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Karar Ağacı	**97.88**	**99.92**	**95.84**	**0.41**

Veri kümesi Nmap ile eğitilmediği için Nmap verilerinin büyük bir bölümü diğer bilgi tarama saldırılarına benzetilmiştir. 8 tanesi ise normal veri olarak algılanmıştır. Saldırı verilerini algılamada bu nedenle azalma gerçekleşmiştir.



Şekil 1: Test Veri Seti İle Eğitim Veri Setindeki Saldırı Türleri Farklı Olduğunda Hata Matrisi

C. Ripper Kuralı ile Saldırı Tespiti

Weka aracında Ripper Kuralı ile eğitim süresinin hesaplanması için JRip sınıflandırıcı seçilir. Ripper Kuralının performansı yani eğitim süresi Geri Yayılma Algoritmasına göre çok daha iyidir. Ancak Karar Ağaçlarına göre daha iyi bir performans sergileyememiştir.

Tablo 8: Ripper Kuralı İle Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Ripper Kuralı	99.7	99.8	99.6	2.37

D. Rasgele Orman Algoritması ile Saldırı Tespiti

Weka aracında Rasgele Orman Algoritması ile eğitim süresinin hesaplanması için RandomForest sınıflandırıcı seçilir. Rasgele Orman Algoritmasının algılama yüzdeleri diğer sınıflandırıcılara göre daha iyi bir performans sergilemiştir.

Tablo 9: Rasgele Orman Algoritması İle Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Rasgele Orman	99.94	100	99.88	0.44

V. *SONUÇLAR* VE *TARTIŞMA*

Yapılan çalışmada Hizmet Engelleme saldırıları ve Bilgi Tarama saldırılarının sınıflandırılmasında 6 çeşit Hizmet Engelleme (DoS), 4 çeşit Bilgi Tarama (Probe) saldırısı mevcuttur. Sınıflandırmanın doğru yapılması yalnızca Hizmet Engelleme ve Bilgi Tarama şeklinde değil saldırının türü şeklindedir. Örneğin Smurf saldırısı da Teardrop saldırıları da Hizmet Engelleme saldırısıdır. Ancak bazı Smurf saldırıları Teardrop olarak algılanabilmektedir. Bu durumda yanlış sınıflandırma yapılmıştır. Deneysel çalışmamızda her bir saldırı çeşidini ayrı ayrı sınıflandırıp bu kapsamda hesaplamalar yapılmıştır.

Tablo 10: Farklı Algoritmalar Kullanılarak Elde Edilen Sonuçlar

Sınıflandırma Türü	TAO (%)	NAO (%)	STO (%)	Eğitim süresi (s)
Geri Yayılma	99.8	100	99.8	828.48
Karar Ağacı	99.8	99.8	99.8	0.69
Ripper Kuralı	99.7	99.8	99.6	2.37
Rasgele Orman	99.9	100	99.8	0.44

Weka uygulamasında yer alan çeşitli makine öğrenme algoritmaları denenerek en iyi sonuç elde edilmeye çalışılmıştır. Sonuç olarak büyük veri setleri için Geri Yayılma Algoritmasının kullanımı eğitim süresinin uzun sürmesinden dolayı uygun değildir. Bizim çalışmamızda en iyi tespiti Rasgele Orman Algoritması yapmıştır. Buna en yakın değerler Geri Yayılma Algoritması ile elde edilmiştir. Ancak buna rağmen eğitim süresinin çok uzun sürmesi zaman açısından maliyeti büyük ölçüde arttırmıştır.

VI. ÇIKARIM

Bir çıkarım yapmak gerekirse büyük veri setleri için Rasgele Orman Algoritması eğitim süresinin çok iyi olmasından ötürü ve iyi bir tespit, öğrenme yüzdesi vermesi nedeniyle kullanılabilir. Büyük veri setlerinde Geri Yayılma Algoritması kullanımı uygun değildir. Küçük veri setleri için kullanılabilir.

KAYNAKLAR

[1] M. Ünver, C. Canbay, A. G. Mirzaoğlu, *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,* Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Mayıs 2009

[2] C. Karakuş, *Kritik Alt Yapılara Siber Saldırı,* İstanbul Kültür Üniversitesi

[3] Y. Şenkaya, U. G. Adar, *Siber Savunmada Yapay Zeka Sistemleri Üzerine İnceleme,* Akademik Bilişim 2014 Konferansı Mersin

[4] Ş. Sağiroğlu, E. N. Yolaçan, U. Yavanoğlu, *Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi,* Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2011

[5] M. Z. Yıldırım, A. Çavuşoğlu, B. Şen, İ. Budak *Yapay Sinir Ağları ile Ağ Üzerinde Saldırı Tespiti ve Paralel Optimizasyonu,* XVI. Akademik Bilişim Konferansı Bildirileri 2014

[6] H. Takci, *Veri Madenciliği İle Saldırı Tespiti* Cumhuriyet Üniversitesi Bilgisayar Mühendisliği Bölümü

[7] Y. Özen ve B. Mert, *Saldırı Tespit Sistemlerinde Kullanılan Makine Öğrenmesi Algoritmalarının Karşılaştırılması, ICONCS 2018*

[8] K. Hanifi, H. Bank, M. E. Karsligil, A. G. Yavuz ve M. A. Güvensan, *Makine Öğrenmesi Anormal Durum Belirleme Yaklaşımı ile Ağ Üzerinde Saldırı Tespiti, Bilgisayar Mühendisli˙gi Bölümü Yıldız Teknik Üniversitesi, IEEE 2016*

[9] Md. Al Mehedi Hasan, M. Nasser, S. Ahmad, K. I. Molla, *Feature Selection for Intrusion Detection Using Random Forest, Journal of Information Security, 2016*

[10] A. Özgür, H. Erdem, *Saldırı Tespit Sistemlerinde Genetik Algoritma Kullanarak Nitelik Seçimi ve Çoklu Sınıflandırıcı Füzyonu,* Journal of the Faculty of Engineering and Architecture of Gazi University 2018

[11] P. T. Htun, K. T. Khaing, *Detection Model for Daniel-of-Service Attacks Using Random Forest and k-Nearest Neighbors,* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) May 2013

[12] T. E. Kalaycı, *Kimlik Hırsızı Web Sitelerinin Sınıflandırılması İçin Makine Öğrenmesi Yöntemlerinin Karşılaştırılması,* Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi 2018

[13] H. Tanrıkulu ve Dr. M. H. Sazlı, *Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması,* XII. Türkiye'de İnternet Konferansı 2007, Ankara

[14] C. Coşkun, Yrd. Doç. Dr. A. Baykal**, "***Veri Madenciliğinde Sınıflandırma Algoritmalarının Bir Örnek Üzerinde Karşılaştırılması***"** Dicle Üniversitesi, Bilgi İşlem Daire Başkanlığı, Diyarbakır

[15] Ö. Keleşoğlu, A. Fırat, *Tuğla Duvardaki ve Tesisattaki Isı Kaybının Yapay Sinir Ağları İle Belirlenmesi,* Fırat Üniversitesi Fen ve Müh. Bil.Der.2006

[16] http://www.datascience.istanbul/tag/random-forest-siniflandirma/