FBU-DAE 2021
1 (3) : 221-232

DDOS SALDIRILARININ MAKİNE ÖĞRENİMİ ALGORİTMALARIYLA TESPİTİ

DETECTION OF DDOS ATTACKS WITH MACHINE LEARNING ALGORITHMS

Serdar ASARKAYA*, Oğuz KAYNAR**, İlkay YELMEN***, Fazlı YILDIRIM****, Metin ZONTUL*****

Geliş Tarihi/Received: 20.10.2021
Kabul Tarihi/Accepted: 28.10.2021

Araştırma Makalesi/Research Article

*
Savunma Teknolojileri A.B.D.
Sivas Bilim ve Teknoloji Üniversitesi Sivas / Türkiye

Defense Technologies Department
Sivas Science and Technology University
Sivas / Turkey

ORCID: 0000-0002-4790-1709

**
Yönetim Bilişim Sistemleri Bölümü
Cumhuriyet Üniversitesi Sivas / Türkiye

Management Information Systems
Department Sivas / Turkey

ORCID: 0000-0003-2387-4053

***
Ar-Ge Merkezi, Turkcell Teknoloji
İstanbul / Türkiye

R&D Center, Turkcell Technology
İstanbul / Turkey

ORCID: 0000-0002-1684-9717

****
Yönetim Bilişim Sistemleri Bölümü
Fenerbahçe Üniversitesi İstanbul / Türkiye

Management Information Systems
Department, Fenerbahçe University
İstanbul / Turkey

ORCID: 0000-0002-8142-0466

*****
Bilgisayar Mühendisliği, İstanbul Arel
Üniversitesi, İstanbul / Türkiye

Computer Engineering Department
İstanbul Arel University, İstanbul / Turkey

ORCID: 0000-0002-7557-2981

ÖZET

DDoS saldırıları, network saldırıları içerisinde en sık rastlanan saldırı türüdür. Bu saldırılar sonucunda bireyler ve şirketler para, itibar ve zaman kaybı gibi sorunlarla uğraşmak zorunda kalmaktadırlar. Saldırıları önleme amaçlı farklı yöntem ve sistemler denenmekle birlikte sorunların tamamen ortadan kalktığı söylenemez. Sorunlara çözüm önerilerinden birisi saldırıların erken tespit edilmesidir. Bu çalışma; DDoS saldırılarının tespiti için saldırıların makine öğrenmesi yöntemleriyle sınıflandırılmasını amaçlamaktadır. Çalışmada, seçilen veri setindeki veriler optimize edilmiş ve K-Nearest Neighbours, Multi Layer Perceptron, Support Vector Machine ve Random Forest sınıflayıcı modelleri geliştirilmiştir. Değerlendirmede ROC eğrileri ile Precision, Recall, F1-Score ve Accuracy metriklerinden yararlanılmıştır. En yüksek doğruluk oranı olan %99'a Multi Layer Perceptron modelinde ulaşılmıştır.

Anahtar Kelimeler: DDoS, Network Saldırıları, Makine Öğrenimi, Sınıflandırma, Multi Layer Perceptron

ABSTRACT

DDoS attacks are the most common type of attack among network attacks. As a result of these attacks, individuals and companies have to deal with problems such as loss of money, reputation and time. Although different methods and systems have been tried to prevent attacks, it cannot be said that the problems have been completely eliminated. One of the solutions to problems is to detect attacks early. This study aims to classify attacks with machine learning methods to detect DDoS attacks. In the study, the data in the selected data set was optimized and K-Nearest Neighbors, Multi Layer Perceptron, Support Vector Machine and Random Forest classifier models were developed. ROC curves and Precision, Recall, F1-Score and Accuracy metrics were used in the evaluation. The highest accuracy rate of 99% was reached in the Multi Layer Perceptron model.

Keywords: DDoS, Network Attacks, Machine Learning, Classification, Multi Layer Perceptron

1. GİRİŞ

Günümüzde network giderek büyüyen bir şekilde veri, para, bilgi vb konularında transfer aracı olarak kullanılmaktadır. Bu durum hayatımızda büyük rol oynasa da network üzerinde hala büyük güvenlik açıkları bulunmaktadır. Bu açıklara yapılan saldırılar zaman, para ve itibar kaybı gibi durumlara yol açmaktadır (Gavaskar vd, 2010).

Ağ üzerinde birçok saldırı türüne rastlanmaktadır. Bu saldırılar sonucunda sistemlerde

yıkıcı, değiştirici, hizmetlerin aksamasına yol açan veya verilerin sızdırılmasına yol açan zararlar ortaya çıkmaktadır. Saldırılar zararlı yazılımlar, virüsler, solucanlar, truva atları, casus programlar, pishing vb. yöntemlerle gerçekleşmektedir (Kariyer Uygulama ve Araştırma Merkezi, 2021).

Saldırılara neden olabilecek açıklar ağ protokol yapılarından da kaynaklanabilmektedir. Ağ protokollerini kullanan uygulamalardaki hatalı veya eksik kullanım saldırıya uğrayan sistemlerde kayıplara yol açabilmektedir (Kothari vd, 2011: 26-37).

Cao vd. (2019), saldırıların sadece protokollerin eksik veya yanlış kullanımından değil, protokollere ait bazı açıklardan da kaynaklanabildiğini belirtmiştir. Örneğin TCP yan kanal güvenlik açıkları öngörülemeyen, bulunması zor olan ve alan uzmanları tarafından manuel olarak ortaya çıkarılan açıklardır.

Yerel network sistemlerinin yanı sıra günümüzde bulut bilişim sistemleri de benzer saldırılara maruz kalmaktadır. Bulut sistemlerine yatırım yapan şirketlerin güvenilirliğinin sarsılmaması ve maruz kaldıkları saldırı risklerini önleme adına daha fazla harcama yapmamaları için çözülmesi gereken problemlerden biri güvenlik sorunlarıdır. Bulut hizmeti sağlayıcılarından beklenen kullanılabilirlik ve bağlantı hizmetlerinde aksamalar meydana geldiğinde, hizmet sağlayıcıların büyük maliyetlerle karşılaşacağı düşünülmektedir (Lonea vd, 2013: 70-78).

İnternet veya aSğ ortamında sık karşılaşılan, hizmet veren sunuculara ve bulut bilişim hizmetlerine yapılan ve onları kullanılamaz hale getirmeyi amaçlayan saldırılardan biri DDoS (Distributed Denial of Service) saldırısıdır. DDoS saldırıları, toplam saldırıların %90' ını oluşturmaktadır (Maregeli, 2010)

DoS saldırılarının bu kadar sık olmasının nedeni, bu saldırıların oluşturma ve başlatma yöntemlerinin fazla olmasıdır. Bu nedenle saldırganlar, hedeflenen bir kurbana başarılı bir hizmet reddi saldırısı yapmanın birkaç farklı yolunu bulacaklardır (Aamir ve Zaidi, 2019).

DoS saldırıları Volümetrik, Protokol ve Uygulama saldırıları olarak sınıflandırılabilir. Volümetrik saldırılar

TCP/UDP Flood, DNS/NTP/Mamcached amplifikasyonu örnek olarak verilebilir. Protokol saldırılarına SYN/SYN-ACK/ACK Flood, Ping of Dead vb. örnek olarak gösterilebilir. Uygulama saldırılarına HTTP, HTTPS, DNS ve SMTP protokollerine yapılan saldırılar örnek olarak gösterilebilir (LoDDoS, 2021).

Yapılan çalışmalarda DDoS saldırılarından korunma amaçlı erken uyarı ve algılama sistemleri geliştirmeye yönelik birçok çalışma bulunmaktadır (Deore ve Patil, 2016: 1739-1739). DDoS saldırılarında yapılan sınıflandırma sonuçlarının, protokol veya uygulama açıklarından (Kührer vd, 2014) kaynaklanan saldırılar için geliştirilecek saldırı algılama ve erken önleme sistemleri için referans oluşturabileceği düşünülmektedir.

Bu çalışmanın amacı, makine öğrenmesi sınıflandırma algoritmaları kullanarak DDoS saldırılarının tahmin edilmesidir. Çalışmada 4 farklı sınıflandırma modeli kullanılmış olup, modellerde elde edilen doğruluk oranlarındaki değişimi gözlemlemek amacıyla 0.00025 threshold değeri kullanılarak ExtaTreesClassifiers ile Feature Selection uygulanmıştır. Modelde kernel parametresine rbf değeri, gamma parametresine scale değeri atanmıştır. Farklı sınıflarda, K-Nearest Neighbours kullanılarak oluşturulan model ile %93, Support Vector Machine modeli ile %98, Multi Layer Perceptron Modeli ile %99 ve Random Forest Modeli ile %98 doğruluk oranları elde edilmiştir.

Bu makale toplam 4 bölümden oluşmaktadır. Makalenin 2. bölümünde DDoS saldırılarına yönelik literatür taraması, 3. bölümde yöntem, 4 bölümde deneylerin sonuçları ve bulgular, son olarak 5. bölümde ise makale sonuçları hakkında bilgi verilmiştir.

2. LİTERATÜR TARAMASI

Lonea vd. (2013) tarafından bulut bilişim hizmetlerinde DDoS saldırılarını saptamak ve analiz etmek amacıyla, Dempster-Shafer Teorisi (DST) süreçlerini ve sanal makine (VM) algılama sistemi (IDS) tabanlı saldırılar için Hata Ağacı Analizini (FTA) kullanan bir çözüm önerisi geliştirilmiştir. Çözüm nicel olarak belirsizliği temsil eder ve yanlış alarm oranlarını

azaltmak amacıyla IDS' lerde verimli bir şekilde kullanılmaktadır.

IoT tabanlı sensör ağları için iletişimin kuralları zamanla yeni standartlarla geliştirilmektedir. Ancak DDoS saldırıları sensör düğümlerini büyük hacimli ağ saldırıları ile tehdit ederek kaynakların kullanılabilirliğini tehdit etmektedir. Bunu önleyebilmek için Zubair vd. (2019) tarafından IoT sensörleri için ADE (Averaged Dependence Estimator) tabanlı bir DDoS tespit şeması sunulmuştur.

Tertytchny vd. (2020) networkte oluşan anormallikler incelenmiş ve bu durumun arıza veya ağ saldırılarından kaynaklanabildiğini belirtmiştir. Sınıflandırma yoluyla farklılaşma sağlamak amacıyla ML tabanlı yaklaşımlar kullanılmıştır. Sonuçlar denetimli makine öğrenmesi yöntemlerinin, arıza veya saldırıların sınıflandırılmasında yüksek doğruluk oranları elde edildiğini göstermektedir.

Network (Ağ) trafik tahmini, iletişim ağı anormalliklerini tespit ve analiz etmenin verimli bir yöntemidir. Kullanılan yapay sinir ağı (NARX) %5 bağıl hata oranı ile 62 tahmin adımına izin vermiştir. Bu sistem ağ içerisindeki sahte trafiğin saptanmasına yardımcı olmaktadır. Sonuçlar network trafiğinin analiz edilebilir olmasını, DDoS saldırı tespiti için etkili bir araç haline getirmektedir (Silva ve Coury, 2020).

KNN, SVM ve RF algoritmaları, DDoS saldırılarını sınıflandırmak için etiketli verilere uygulanmıştır. KNN, SVM ve RF modelleri kullanılarak optimize edilmiş parametrelerle, veri seti için %95, %92 ve %96,66 doğruluk oranları elde edilmiştir. Veri seti Riverbed Modeler olarak adlandırılan network trafik üreteci kullanılarak oluşturulmuştur (Aamir ve Zaidi, 2019).

Bir diğer çalışmada ise büyük veri setinden en iyi alt özellik kümesinin seçilebilmesi ve sınıflandırmada yüksek doğruluk oranlarına ulaşılabilmesi için bir yöntem sunulmuştur. Yüksek hacimli ağ trafiğinin üstesinden gelebilmek için daha az eğitim örneğiyle aktif öğrenme yaklaşımı kullanılmıştır. SVM sınıflandırıcısı ile veri seti olarak DARPA, CAIDA, ISCX ve TU-DDoS kullanılmıştır. 100 bin örnekte maksimum %99,9 doğruluk oranına ulaşılmıştır (Deka vd, 2019: 203-222).

Kötü amaçlı yazılım trafiğini tespit etmek amaçlanarak Arivudainambi vd. [15] tarafından yapay zekâ destekli trafik analiz sistemi önerilmiştir. Mevcut analiz sistemleri yapay zekâ destekli kötü amaçlı yazılımlar tarafından üretilen trafiği tespit edememektedir. ANN ile kullanılan PCA, Carl Pearson ve faktör analizi ile %99,2'ye ulaşan doğruluk oranlarında Malware tespiti yapılmıştır. Veri seti olarak indirilen 1000 örneğin 100 tanesi yapay zekâ destekli örneklerdir.

Tekerek (2021), çalışmasında CSIC2010v2 http veri seti kullanılarak http web trafiğindeki anormallikleri algılayabilmek için CNN derin öğrenme algoritmasından yararlanılarak web saldırısı algılama mimarisi önerilmiştir. Belirtilen veri seti kullanılarak CNN modelinde test verileri üzerinde http verileri normal ve anormal olarak sınıflandırılarak %97,07'lik bir doğruluk oranı elde edilmiştir.

Dimitrios vd. (2020) mobil enerji dağıtıcıları ve dinamik kablosuz şarj sistemlerine yapılan saldırıları tespit etmek ve azaltmak amaçlı makine öğrenmesi algoritmaları temel alınarak bir saldırı tespit sistemi geliştirmişlerdir. Önerilen katmanlı yapı (IDS), KNN veya RF algoritmalarını kullanarak saldırı tespitinde %91 oranında doğruluk oranı üretmişlerdir.

Liu vd. (2019) çalışmalarında saldırı tespitinde CNN ve RNN makine öğrenmesi modellerini tanıtmış ve PL-CNN, PL-RNN yaklaşımlarını önerilmiştir. Çalışmada CNTC-2017 web Shell, Darpa-1998, CSIC-2010 HTTP veri setleri kullanılmıştır. Bu yaklaşımlar orijinal network paketlerinden özellik temsillerini öğrenmektedir. Böylece modeller özellik mühendisliğinden ve ağ güvenliği alan bilgisinden bağımsız olarak çalışmaktadır.

İş birliğini temel alan saldırı tespit ağları, bir saldırı tespit sisteminin bilgi toplamasına ve deneyim öğrenmesine olanak tanırken içeriden yapılacak saldırılara karşı savunmasızdır. Bu nedenle çalışmada uzman bilgisine dayalı olarak izinsiz giriş hassasiyeti değerlerini otomatik olarak belirlemek amacıyla denetimli bir makine öğrenimi yaklaşımı geliştirilmiştir. Li vd. (2017) çalışmalarında KNN, BPNN ve DT modellerini kullanmışlardır.

Singh vd. (2018) GET Flood saldırısı stratejilerini belirlemek amacıyla önerilen dört özelliği

kullanan makine öğrenimini temel alan algılama sistemi oluşturmuş ve sistem sahte kullanıcılar(bot) ile yasal kullanıcıları ayırmaktadır. Worldcup98, NASA, Clarknet verileri ile çalışılan sistemde NaiveBayes, RandomForest, SVM vb. sınıflandırıcılar kullanılmıştır.

SaiSindhuTheja ve ekibi (2021) tarafından bulut bilişim hizmetlerinde OCSA ve RNN tabanlı bir saldırı tespit sistemi önerilmiştir. OBL ve CSA algoritmalarını temel alan özellik seçimi için kullanılabilecek meta sezgisel OCSA algoritması oluşturulmuştur. KDDcup99 veri seti, RNN ile oluşturulan modelde %94,12 doğruluk oranı ile sınıflandırılmıştır.

Volkov vd. (2020) ağ saldırılarını tanımlama amacıyla yapay sinir ağlarının uygulanabilirliğini temel alan çalışmada 7 farklı sınıf içeren veri setinde LSTM modeli ile sınıflandırma yapmışlardır. Veri seti içerisinden seçilen 2 sınıflı yapıda LSTM modelinin network saldırılarını sınıflamada MLP modeline göre daha başarılı olduğu gözlemlenmiştir.

Branitskiy vd. (2017) tarafından yapılan çalışmada ağ saldırılarının tespit edilmesinde hibrit yaklaşımların incelenmesi gerçekleştirilmiştir. KDDcup99 ve NSL-KDD veri setleri ile çalışılmıştır. Önerilen sınıflandırma modelinde ANN, ID, NFC ve SVM kombinasyonlarından yararlanılmıştır. Farklı sınıflandırıcılardan gelen veriler en sonunda yeni bir sınıflayıcıya verilerek, hibrid modeller oluşturulmuştur.

CICIDS2017 veri setinin kullanıldığı çalışmada network akış verileri kullanılarak http DoS tespiti için makine öğrenmesini temel alan bir sınıflandırıcı oluşturulmuştur. Sınıflandırmada %99,61 oranında doğruluk elde edilmiştir (Muraleedharan ve Janet, 2021).

Bu çalışmada veri seti olarak kullandığımız network logs kayıtları kullanılarak makine öğrenmesi sınıflandırma algoritmalarıyla saldırı türü tahmin edilmiştir. Literatürde network saldırılarının sınıflandırılması amacıyla farklı veri setleri üzerinde çalışmalar bulunmaktadır. Bulut bilişim sistemlerinden, IoT ağ sistemlerinin güvenliğinin sağlanmasına yönelik makine öğrenmesi modelleri geliştirilmiştir (Tertytchny vd, 2020). Literatürdeki çalışmalarda, CICID (Muraleedharan ve Janet, 2021), KDDcup99 (Branitskiy ve Kotento, 2017), CNTC-2017 (Liu vd, 2019) veri setleri kullanılırken bu çalışmada network log kayıtları içeren bir veri seti kullanılmıştır (“DDoS Attack Network Logs Dataset”, 2021).

3. YÖNTEM

3.1. Veri Seti

Çalışmada Kaggle sayfasından indirilen DDoS Attack Network Logs [25] veri seti kullanılmıştır. Veri seti içerisinde ‘Normal’, ‘Http-Flood’, ‘SIDDOS’, ‘Smurf’, ‘UDP-Flood’ sınıflarına ait 902.186 adet kayıt bulunmaktadır.

Veri seti .csv formatında olup içerisinde 27 farklı öznitelik bulunmaktadır. Son sütunda ise veriye ait sınıf bilgisi bulunmaktadır.

3.2. Veri Ön İşleme

Sınıfların dengeli dağılımını sağlamak amacıyla en az veriye sahip sınıf baz alınarak her bir sınıftan 1700’er kayıt seçilmiş olup toplam kayıt sayısı 8500’e indirgenmiştir.

Sınıflar ‘Normal’-0, ‘Http-Flood’-1, ‘SIDDOS’-2, ‘Smurf’-3, ‘UDP-Flood’-4 olacak şekilde etiketlenmiştir. Veri seti içerisinde yer alan özellikler numerik veya kategoriktir. FLAGS alanı boş olduğu için veri setinden çıkarılmıştır.

ÖZELLİK	TÜR	ÖZELLİK	TÜR
SRC_ADD	Numeric	PKT_IN	Numeric
DES_ADD	Numeric	PKT_OUT	Numeric
PKT_ID	Numeric	PKT_R	Numeric
FROM_NODE	Numeric	PKT_DELAY_NODE	Numeric
TO_NODE	Numeric	PKT_RATE	Numeric
PKT_TYPE	Categorical	BYTE_RATE	Numeric
PKT_SIZE	Numeric	PKT_AVG_SIZE	Numeric
FID	Numeric	UTILIZATION	Numeric
SEQ_NUMBER	Numeric	PKT_DELAY	Numeric
NUMBER_OF_PKT	Numeric	PKT_SEND_TIME	Numeric
NUMBER_OF_BYTE	Numeric	PKT_RESEVED_TIME	Numeric
NODE_NAME_FROM	Categorical	FIRST_PKT_SENT	Numeric
NODE_NAME_TO	Categorical	LAST_PKT_RESEVED	Numeric
		PKT_CLASS	Numeric

Tablo 1. Veri Setinde Yer Alan Özellikler

Hazırlanan veri setinde yer alan özellikler ve veri türleri Tablo 1' de gösterilmiştir. Uygulamada kategorik veriler nümerik verilere dönüştürülmüştür. İlk 26 özellik eğitim ve test amacıyla kullanılmış, son PKT_CLASS alanı ise sınıf etiketlerinin bulunduğu alan olarak kullanılmıştır.

Veriler eğitim amaçlı modellere verilmeden önce veri seti içerisinde farklı aralık değerlerinde veriler bulunduğu için değer aralıklarındaki farklılık bozulmadan normalize edilmiştir. Bu işlemin modellerin ağırlıkları öğrenmesini kolaylaştıracağı söylenebilir. Bunun için sklearn kütüphanesindeki Min Max Scaler yöntemi kullanılmış ve veriler [0,1] aralığında ölçeklendirilmiştir.

Veri setindeki özellikler sklearn kütüphanesindeki Extra Tree Classifier yöntemi kullanılarak threshold (0.00025) değerleriyle seçilmiştir. Threshold değerinin altında kalan özellikler eğitim ve test verilerinde yer almamıştır.

3.3. Sınıflandırma

Bu bölümde Random Forest, K-Nearest Neighbours, Support Vector Machine ve Multi Layer Perceptron sınıflandırma algoritmalarıyla ilgili bilgiler verilmiştir.

3.3.1. Random Forest

Random Forest algoritması her biri aynı düğümlere sahip, ancak farklı yapraklara yol açan farklı verileri kullanan farklı karar ağaçlarından oluşmaktadır. Bu yapı içerisinde tüm karar ağaçlarına ait bir cevaba ulaşmak için çoklu karar ağaçlarının çıktılarını birleştirir.

Karar ağaçlarında dallanmanın nasıl gerçekleştiğini belirlemek amacıyla Gini veya Entropy kullanılabilir (Schott, 2021).

$$\text{Gini}=1-\sum_{i=1}^{c}(p_i)^2 \quad (1)$$

Denklem 1'de p_i veri setinde gözlemlenen sınıfın göreceli frekansını c ise sınıf sayısını temsil etmektedir.

$$\text{Entropy}=\sum_{i=1}^{c}-p_i * log_2(p_i) \quad (2)$$

Denklem 2'de gösterilen Entropy, düğümlerin nasıl dallanacağına karar verirken belirli bir sonucun olasılığını kullanmaktadır.

3.3.2. K-Nearest Neighbours

KNN, veri noktalarını kendisine en çok benzeyen noktalara göre sınıflandıran bir modeldir. Sınıflandırılacak noktaların ne olarak sınıflandırılacağına yönelik tahmin yapmak içi test verilerinden yararlanmaktadır.

KNN'de sınıflandırma yapılırken veri noktaları arasındaki uzaklık Denklem 3'te gösterilen Euclidean yöntemi ile hesaplanmaktadır (Schott,2021).

$$d(p,q) = d(q,p) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n}(q_i - p_i)^2} \quad (3)$$

3.3.3. Support Vector Machine

SVM, ayırıcı bir hiper düzlem ile tanımlanan ayırt edici bir sınıflandırıcıdır. Yani, etiketli eğitim verileri verildiğinde, algoritma yeni örnekleri kategorize eden optimal bir hiper düzlem üretir.

Patel (2020)'e göre iki boyutlu uzayda bu düzlem, bir düzlemi her bir sınıfın her iki tarafta da bulunduğu iki parçaya bölen bir çizgidir.

Problemin doğrusal cebir kullanılarak dönüştürülmesiyle, doğrusal SVM'de hiper düzlemin öğrenilmesi sağlanır. Bu noktada 'kernel' parametresi seçimi yapılmaktadır. Doğrusal 'kernel' için girdi(x) ile her destek vektörü(xi) arasındaki iç çarpımı kullanan yeni bir girdi için tahmin denklemi Denklem 4'te gösterilmiştir.

$$f(x) = B(0) + sum(ai * (x, xi)) \quad (4)$$

Denklem 4' te verilen B(0) ve ai katsayıları öğrenme algoritması tarafından eğitim verilerinden tahmin edilmelidir.

$$K(x, xi) = 1 + sum(x * xi)\text{^}d \quad (5)$$

$$K(x, xi) = \exp(-gamma * sum(x - xi^2)) \quad (6)$$

Polynomial kernel için Denklem 5, exponential kernel için Denklem 6 kullanılmaktadır.

3.3.4. Multi Layer Perceptron

MLP, ileri beslemeli bir yapay sinir ağı sınıfıdır. Yapı olarak en az 1 giriş katmanı 1 gizli katman ve 1 çıkış katmanından oluşur. Giriş düğümleri dışında her düğüm, doğrusal olmayan bir aktivasyon işlevi kullanan bir nörondur.

MLP, eğitim için geri yayılım adı verilen denetimli bir öğrenme tekniği kullanır. Çoklu katman yapısı ve doğrusal olmayan aktivasyon fonksiyonlarıyla MLP doğrusal algılayıcılardan ayrışmaktadır. Doğrusal olarak ayrılamayan verileri ayırt edebilmektedir.

Skalski (2021)'ye göre MLP öğrenme modelinde geri yayılım işlemi, hatanın geri yayılımıyla parametrelerin güncellenmesini ifade eder.

Ağırlık parametreleri güncellenirken, $w = w - \propto dW$ bias parametreleri güncellenirken $b = b - \propto db$ formülleri kullanılır. dW ve db değerleri zincir kuralı ile hesaplanırken kayıp fonksiyonunun W ve b' ye göre kısmi türevlerini ifade eder.

4. YÖNTEM

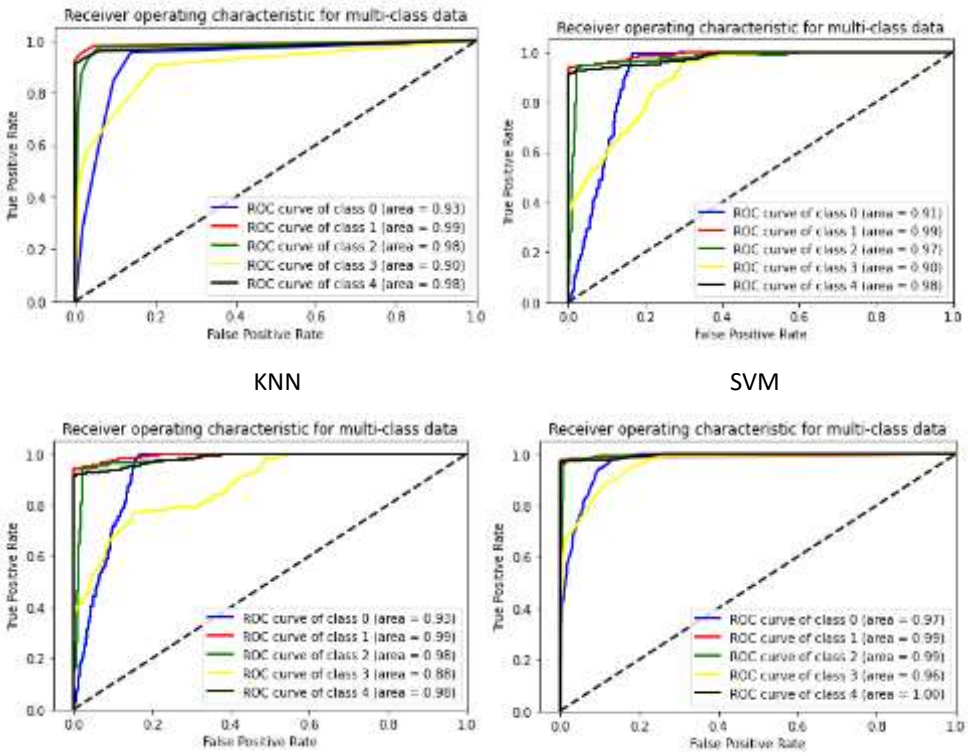
Deneysel çalışmada KNN, SVM, MLP ve RF sınıflandırıcıları kullanılmıştır. Modellerden ne kadar iyi performans alınacağını görmek amacıyla cross validation uygulanmıştır. Bunun için sklearn kütüphanesinden KFold yöntemi kullanılmış ve n_splits=5 değeriyle eğitim sırasında veri seti 5 parçaya ayrılmıştır. Verilerin gruplara ayrılmadan önce karıştırılması için shuffle değeri True olarak ayarlanmıştır. Cross validation ile her bir fold için elde edilen doğruluk oranı grafikleri Şekil 3'te gösterilmiştir.

KNN ile oluşturulan modelde k (en yakın komşuluk) değeri 4 olarak seçilmiş ve en yüksek doğruluk oranı %93 olarak bulunmuştur.

MLP ile oluşturulan modelde alpha 1e-005, hidden_layer (20,10), random_state=20, solver 'sdg' ve max_iter=1000 değerleri ile eğitim yapılmış ve en yüksek doğruluk oranı %99 olarak bulunmuştur.

SVM ile oluşturulan modelde kernel 'rbf', gamma 'scale', degree=3 ve random_state=15 parametre değerleriyle eğitim yapılmış ve en yüksek doğruluk oranı %98 olarak bulunmuştur.

RF ile oluşturulan modelde criterion parametresi 'gini' olarak seçilmiştir ve en yüksek doğruluk oranı %98 olarak bulunmuştur.



Şekil 1. Multiclass Roc Curves

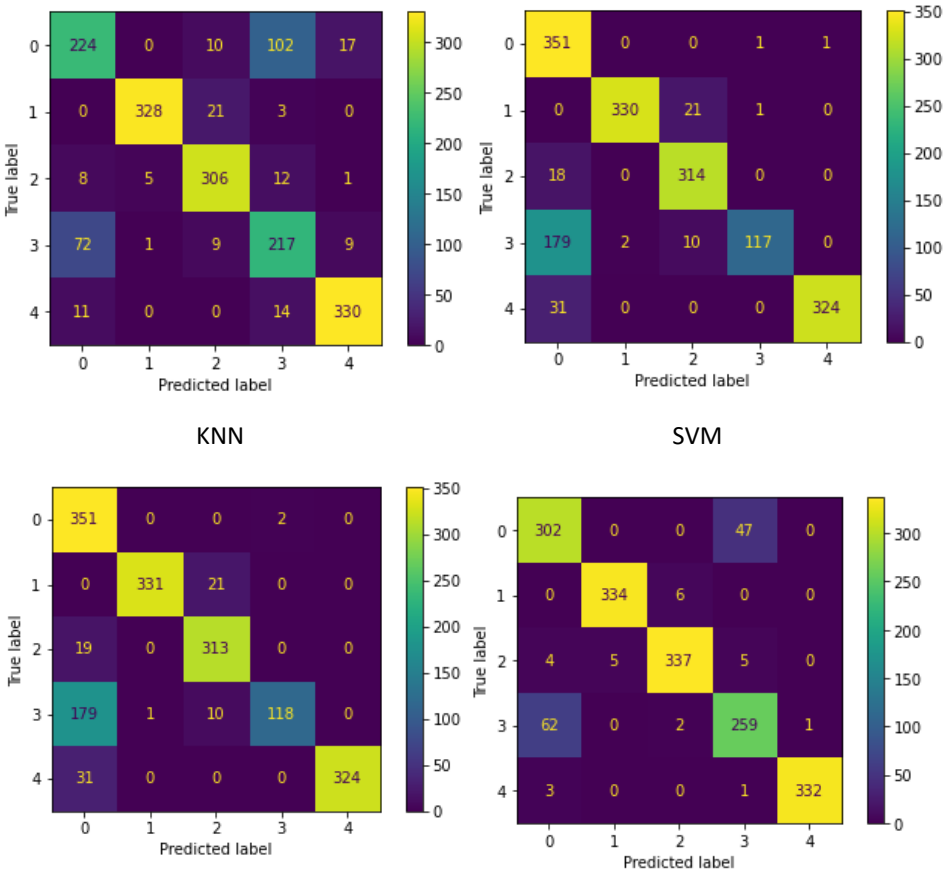
ROC curve eğrileri bir test değerini tanılamak için kullanılmaktadır. Makul doğrulukta bir test verisinin grafikteki sol üst üçgende, referans çizgisinin üzerinde bir ROC eğrisine sahip olması beklenir. ROC eğrilerinin altında kalan alan (AUC) test verisinin belli bir durumu olup olmadığını belirleyen genel geçer bir ölçüdür (Hoo vd, 2017).

1,0 değerine yakın AUC değeri iyi bir test sonucunu ifade ederken, 0.5 e yakın değerler ayırt etme yeteneği olmayan bir testi ifade ettiği değerlendirilebilir. Sınıflandırma modellerinin uygunluğu ROC eğrileri ile Şekil 1'de gösterilmiştir. ROC eğrilerinde y ekseni TP (True Positive), x ekseni ise FP (False Positive) oranlarını göstermektedir.

MultiClass sınıflandırması sonucu dört farklı modelde oluşan roc curve grafikleri Şekil 1'te gösterilmiştir. Test verilerinin makul ROC eğrilerine sahip olduğu Şekil 1'de görülmektedir. Diğer modellerde daha düşük sınıflandırma oranına sahip class 3 (Smurf) verilerinin RF ile daha yüksek oranda (area=0,96) AUC değeri ile sınıflandırılabildiği görülmüştür.

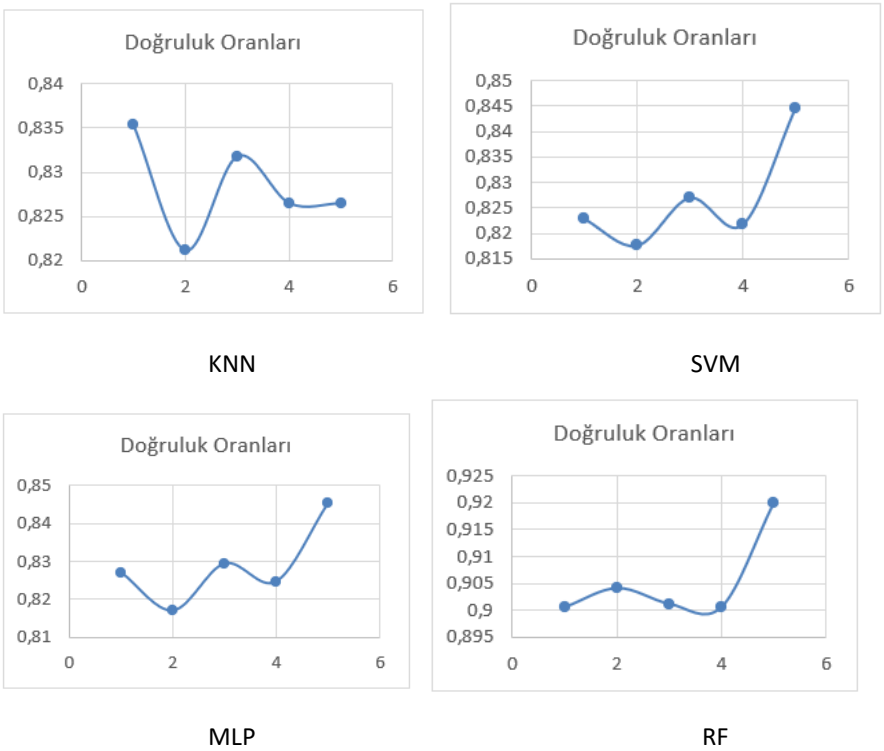
Çalışılan modellerde değerlerin doğru (True label) ve tahmin (Predicted label) sayılarını gösteren confusion matrix (karmaşıklık matrisi) yapıları Şekil 2'de gösterilmiştir.

Confusion matrixte en büyük sapmanın class 3 (Smurf) sınıfında yaşandığı görülmektedir. Bu sınıftaki en yüksek başarım oranın RF modelinde elde edildiği gözlenmiştir.



Şekil 2. Multiclass Confusion Matrix

Confusion matrix'te görülen sonuçların ROC eğrileri ile paralel sonuçları gösterdiği söylenebilir. Eğitim sırasında uygulanan cross validation ile her bir grup (fold) için elde edilen sonuçlar Şekil 3'te gösterilmiştir. KNN modeli ile elde edilen doğruluk oranları %83,5-82, MLP modeli ile elde edilen sonuçlar %82-84.5, SVM modeli ile elde edilen sonuçlar %82.5-84.5, RF ile elde edilen sonuçlar %90-92 arasında değişmektedir.



Şekil 3. Cross Validation Doğruluk Oranları

DDoS saldırıları sınıflandırma sonuçları değerlendirilirken Precision, Recall, F1-Score ve Accuracy metriklerinden de yararlanılmıştır.

Precision metriği, Denklem 7'de gösterilen normal veri miktarının, normal ve anormal verilerin toplamına oranı olarak adlandırılır.

$$P=TP/(TP+FP) \quad (7)$$

Recall metriği, Denklem 8'de gösterilen test verisinde tespit edilen normal veri miktarının test verisinde bulunan toplam veri miktarına oranıdır.

$$R=TP/(TP+FN) \quad (8)$$

F1-Score metriği, Denklem 9'da gösterilmiştir ve Precision ve Recall metriklerinin harmonik ortalamasıdır.

$$F=2PR/(P+R) \quad (9)$$

Accuracy metriği test verisinde bulunun doğru tahminlerin toplam tahmin sayısına oranıdır. Denklem 10'da gösterilen Accuracy değeri 1'e yaklaştıkça modelin doğruluk başarı oranı artarken, 0'a yaklaştıkça azalmaktadır.

$$A=(TP+TN)/(TP+TN+FP+FN) \quad (10)$$

SINIFLAR	METRİKLER	KNN %	SVM %	MLP %	RF %
Normal[0]	Precision	0.71	0.61	0.61	0.81
	Recall	0.63	0.99	0.99	0.87
	F1-Score	0.67	0.75	0.75	0.84
	Accuracy	0.63	0.98	0.99	0.87
HTTP-Flood[1]	Precision	0.98	1.00	0.99	0.99
	Recall	0.93	0.94	0.94	0.98
	F1-Score	0.96	0.97	0.96	0.98
	Accuracy	0.93	0.94	0.93	0.98
SIDDOS[2]	Precision	0.88	0.91	0.91	0.98
	Recall	0.92	0.94	0.95	0.96
	F1-Score	0.90	0.93	0.93	0.97
	Accuracy	0.92	0.93	0.94	0.96
SMURF[3]	Precision	0.62	0.98	0.98	0.83
	Recall	0.70	0.38	0.38	0.80
	F1-Score	0.66	0.55	0.55	0.81
	Accuracy	0.70	0.38	0.38	0.80
UDP-Flood[4]	Precision	0.92	1.00	1.00	1.00
	Recall	0.93	0.91	0.91	0.99
	F1-Score	0.93	0.95	0.95	0.99
	Accuracy	0.92	0.91	0.91	0.98

Tablo 2. Sınıflayıcılar ve Test Sonuçları

Eğitim verileri ile eğitilen modeller, test verileri ile tahmin yaptıklarında elde edilen sonuçlar Tablo 2'de gösterilmiştir.

Tablo 2'ye göre saldırı içermeyen verilerin bulunduğu Normal sınıfında KNN modelinde %63, SVM modelinde %98, MLP modelinde %99 ve RF modelinde %87 accuracy

değerlerine ulaşılmıştır.

HTTP-Flood saldırı sınıfında KNN modelinde %93, SVM modelinde %94, MLP modelinde %93 ve RF modelinde %98 accuracy değerlerine ulaşılmıştır.

SIDDOS saldırı sınıfında KNN modelinde %92, SVM modelinde %93, MLP modelinde %94 ve RF modelinde %96 accuracy değerlerine ulaşılmıştır.

SMURF saldırı sınıfında KNN modelinde %70, SVM modelinde %38, MLP modelinde %38 ve RF modelinde %80 accuracy değerlerine ulaşılmıştır.

UDP-Flood saldırı sınıfında KNN modelinde %92, SVM modelinde %91, MLP modelinde %91 ve RF modelinde %98 accuracy değerlerine ulaşılmıştır.

En yüksek Recall değeri Normal sınıfında %99 oranında SVM ve MLP modelleriyle elde edilmiştir. En düşük değerler ise %38 ile Smurf sınıfında %38 ile SVM ve MLP modellerinde görülmüştür.

SMURF saldırı sınıfına ait Recall değerlerinin SVM ve MLP modellerinde düşük çıkmasının nedeni, sınıfa ait verilerin saldırı içermeyen Normal sınıfı verileri ile ayrımının yapılamamasıdır. Şekil 2'de gösterilen hata matrisleri incelendiğinde MLP modelinde 296 Smurf sınıfı verisinin 179'u Normal sınıfına ait veri olarak tahmin edilmiştir.

SVM modelinde ise aynı şekilde 296 Smurf sınıfı verilerinin 179'unun Normal sınıfına ait veriler olarak tahmin edildiği görülmektedir.

Hata matrisleri incelendiğinde Smurf ve Normal sınıflarına ait verilerle yapılan tahminlerde KNN modelinin 326 Normal sınıfına ait verinin 102'sini Smurf saldırısı olarak tahmin ettiği görülmektedir.

En düşük Precision değeri %61 ile Normal sınıfında MLP ve SVM modelleriyle elde edilirken, en yüksek değerler SVM, MLP ve RF modelleriyle Http-Flood ve UDP-Flood sınıflarında elde edilmiştir.

Smurf ve Normal sınıflarında gözlemlenen sapmalar, veri setinde normalizasyon ve özelik seçimi sorunları olduğunu düşündürmektedir.

İki sınıf arasındaki sapmalar Şekil 1'deki ROC eğrilerinde de görülebilmektedir. Özelik seçimi uygulaması Extra Tree Classifier metodu ile gerçekleştirilmiştir. Recall değerlerinin artırılması amacıyla özelik seçimi uygulanırken farklı threshold değerlerinin seçilebileceği veya farklı özelik seçimi yöntemlerinin uygulanabileceği düşünülmektedir.

5. SONUÇ

Ağ sistemleri güvenliği, yapılandırılan ağın ve kullanıcıların oluşturabileceği açık ve zafiyetlere yönelik önlem alınmasıyla sağlanmaktadır. Ağ ortamlarındaki açıklar kapatılsa dahi, farklı yöntemlerle yapılan saldırılar sistem güvenliğine zarar verebilmektedir. Günümüzde, oluşabilecek zararların önüne geçmek amacıyla geliştirilen erken uyarı ve önleme sistemleri geliştirilmeye devam etmektedir.

Çalışmamızda erken uyarı sistemlerinden birisi olan DDoS saldırılarını tahmin eden "sınıflayıcı modeller" üzerine araştırma yapılmıştır. Geliştirilen modellerin saldırıları izlemek, tespit etmek ve önlemek amacıyla daha az insan müdahalesi gerektiren yazılımlara dönüştürülme imkanlarını yaratmıştır.

Literatür taramasında Singh vd. (2018) makine öğrenmesi önerilmiş ve Branitskiy vd. (2017) tarafından yapılan çalışmada ağ saldırılarının tespit edilmesinde, hibrit yaklaşımların incelenmesi konusunda destek sunulmuştur.

Bu çalışmada, DDoS saldırılarının sınıflandırılması ve tahmini için geliştirdiğimiz modeller KNN, MLP, SVM ve RF sınıflandırıcılarını temel almaktadır. Modellerle çalışmaya başlamadan önce veri setindeki veriler normalize edilip, optimizasyon yapılmıştır.

Yapılan tahminlerde, Accuracy metriği açısından SVM, MLP ve RF sınıflandırıcılarının genelde daha iyi performans gösterdikleri sonucuna ulaşılmıştır. Daha düşük metriklere ve Accuracy değerlerine sahip Smurf saldırı sınıfının tahmininde en iyi sonuçları RF modeli ile

vermiştir. Smurf sınıfında RF modelinin en iyi sonucu vermesinin nedeni, modelin bir özellik alt kümesi arasında en iyi özelliği araması ve seçmesi olarak düşünülebilir.

Sonuç olarak, en iyi sınıflandırma yöntemini bulma amacıyla izlenen ve ilgili modellerin incelediği araştırmada SVM, MLP ve RF sınıflandırıcılarının iyi performans gösterdikleri irdelenmiş olup, Smurf saldırılarına yönelik olarak RF modelinin kullanılması tavsiye edilmektedir.

Gelecekte yapılacak çalışmalarda, farklı özelik seçimi yöntemleri ve derin öğrenme algoritmaları kullanılarak daha etkili sonuçlar çıkabileceği öngörülmektedir.

KAYNAKLAR

Aamir, M., & Zaidi, S. A., "Clustering based semi-supervised machine learning for DDoS attack classification", Journal of King Saud University, Feb. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S131915781831067X?via%3Dihub

Arivudainambi, D., Varun, K. K., Sibi, C. S., & Visu, P., "Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance", Computer Communications, vol. 147, pp. 50-57, Nov. 2019, doi: 10.1016/j.comcom.2019.08.003

Branitskiy, A., & Kotenko, I., "Hybridization of computational intelligence methods for attackdetection in computer networks", Journal of Computational Science, vol. 23, pp. 145-156, Nov. 2017, doi: 10.1016/j.jocs.2016.07.010

Cao, Y., Wang, Z., Qian, Z., Song, C., Krisnamurhy, S., & Yu, P., "Principled Unearthing of TCP Side Channel Vulnerabilities", presented at 2019 ACM SIGSAG Conference on Computer and Communication Security, London, UK, Nov. 11-15, 2019

DDoS attack network logs dataset, www.kaggle.com, [Online]. Available: https://www.kaggle.com/jacobvs/ddos-attack-network-logs (Erişim 1 Ocak 2021)

Deka, R. K., Bhattacharyya, D. K., & Kalita, J. K., "Active learning to detect DDoS attack using ranked features", Computer Communications, vol. 145, pp. 203-222, Sep. 2019, doi: 10.1016/j.comcom.2019.06.010

Deore, S., & Patil, A., "Survey Denial of Service classification and attack with Protect Mechanism for TCP SYN Flooding Attacks.", International Research Journal of Engineering and Technology (IRJET) , vol. 3, no. 5, pp. 1736-1739, May, 2016.

Dimitrios, K., Apostolos, P., Maglaras, L., Moschoyiannis, S., Aparicio-Navarro, F. .., Argyriou, A., & Janicke, H., "A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles", Array, vol. 5, March 2020, Art. no. 100013.

Gavaskar, S., Surendiran, R., & Ramaraj, D., "Three Counter Defense Mechanism for TCP SYN Flooding Attacks", International Journal of Computer Applications, vol. 6, no.6 Sep, 2010

Hoo, Z. H., Candlish, J., & Teare, D., "What is an ROC curve?", Emergency Medicine J, vol. 34, Mar. 2017, Art. no. 206735. doi: 10.1136/emermed-2017-206735

Kariyer Uygulama ve Araştırma Merkezi. "FileHandler2.ashx". http://kariyer.istanbul.edu.tr. http://cdn.istanbul.edu.tr/FileHandler2.ashx?f=bilisimdekariyer2.pdf (Erişim 3 Ocak 2021)

Kothari, N., Mahajan, R., Millstein, T., Govindan, R., & Musuvathi, M., "Finding Protocol Manipulation Attacks", Association for Computing Machinery , presented at SIGCOMM'11 , Toronto, Aug. 2011, pp. 26-37, doi: 10.1145/2018436.2018440

Kührer, M., Hupperich, T., Rossow, C., & Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks.", presented at Woot'14, San Diego CA, USA, Aug 19, 2014

Li, W., Meng, W., Kwok, L.-F., & Ip, H., "Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model", Journal of Network and Computer Applications, vol. 77, pp. 135-145, Jan, 2017, doi: 10.1016/j.jnca.2016.09.014

Liu, H., Lang, B., Liu, M., & Yan, H., "CNN and RNN based payload classification methods for attack detection", Knowledge-Based Systems, vol. 163, pp. 332-341, Jan. 2019, doi: 10.1016/j.knosys.2018.08.036

LoDDoS, "DDoS Saldırıları Değerlendirme Raporu", barikat.com.tr,

https://www.barikat.com.tr/docs/LoDDoS_ddos_degerlendirme_raporu.pdf (Erişim 6 Ocak 2021)

Lonea, A., Popescu, D., & Tianfield, H., "Detecting DDoS Attacks in Cloud Computing Environment", International Journal of Computers Communications & Control, vol. 8, no. 1, pp. 70-78, Feb. 2013, doi: 10.15837/ijccc.2013.1.170

Maregeli, C. N., "A Study On TCP {SYN Attacks And Their Effects on A Network Infrastructure.", M.S. Thesis, Dept. Computer Engineering, Delft Unv. of Tech., Delft, Netherlands, 2010

Muraleedharan, N., & Janet, B., "A deep learning based HTTP slow DoS classification approach using flow data.", ICT Express Available:https://www.sciencedirect.com/science/article/pii/S2405959520300965?via%3Dihub (Erişim 10 Ocak 2021)

Patel, S. "Chapter 2: SVM (Support Vector Machine) — Theory". medium.com. https://medium.com/machine-learning-101/chapter-2-svm-support-vector-machine-theory-f0812effc72 (Erişim 24 Aralık 2020)

SaiSindhuTheja, R., & Shyam, G. K., "An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment", Applied Soft Computing, vol. 100, Mar. 2021, Art. no. 106997, doi: 10.1016/j.asoc.2020.106997

Schott, M. "K-Nearest Neighbors (KNN) Algorithm for Machine Learning". medium.com. https://medium.com/capital-one-tech/k-nearest-neighbors-knn-algorithm-for-machine-learning-e883219c8f26 (Erişim 6 Ocak 2021)

Schott, M. "Random Forest Algorithm for Machine Learning". medium.com. https://medium.com/capital-one-tech/random-forest-algorithm-for-machine-learning-c4b2c8cc9feb (Erişim 4 Ocak 2021)

Silva, L., & Coury, D., "Network traffic prediction for detecting DDoS attacks in IEC 61850 communication networks", Computers and Electrical Engineering, vol. 87, Oct. 2020, Art. no. 106793, doi: 10.1016/j.compeleceng.2020.106793

Singh, K., Singh, P., & Kumar, K., "User behavior analytics-based classification of application layer HTTP-GET flood attacks", Journal of Network and Computer Applications, vol. 112, pp. 97-114, June. 2018, doi: 10.1016/j.jnca.2018.03.030

Skalski, P. "Deep Dive into Math Behind Deep Networks". towardsdatascience.com. https://towardsdatascience.com/https-medium-com-piotr-skalski92-deep-dive-into-deep-networks-math-17660bc376ba (Erişim 8 Ocak 2021)

Tekerek, A., "A novel architecture for web-based attack detection using convolutional network", Computers&Security, vol. 100, Jan. 2021, Art. no. 102096.

Tertytchny, G., Nicolaou, N., & Michael, M., " Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning", Microprocessors and Microsystems, vol. 77, Sep. 2020, Art. no. 103121, doi: 10.1016/j.micpro.2020.103121

Volkov, S. S., & Kurochkinc, I. I., "Network attacks classification using Long Short-term memory based neural networks in Software-Defined Networks", Procedia Computer Science, vol. 178, pp. 394-403, Nov. 2020, doi: 10.1016/j.procs.2020.11.041

Zubair, A., Surasak, S., Firdous, S. N., Vo, V. N., Nguyen, T. G., & Chachai, S.-I., "Averaged dependence estimators for DoS attack detection in IoT networks", Future Generation Computer Systems, vol. 102, pp. 198-209, Jan. 2020, doi: 10.1016/j.future.2019.08.007