Journal of the Faculty of Engineering and Architecture of Gazi University 40:1 (2025) 179-188

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Convolutional neural network models using metaheuristic based feature selection method for intrusion detection

Maryam Salati*, İman Askerzade, Gazi Erkan Bostancı
Department of Computer Engineering , Faculty of Engineering, Ankara University, 06830, Ankara, Türkiye

Highlights:

- Investigation of the role of deep learning and classification algorithms in providing security in Internet networks
- Using a meta-heuristic-based feature selection method combined with convolutional neural networks
- The selected features are then fed into CNNs, to improve the accuracy of intrusion detection

Keywords:

- Intrusion detection
- Convolutional Neural Network
- Meta-heuristic algorithms
- Feature selection
- Decision Tree

Article Info:
Research Article
Received: 24.04.2023
Accepted: 12.12.2023

DOI:
10.17341/gazimmfd.1287186

Correspondence:
Author: Maryam Salati
e-mail: msalati@ankara.edu.tr
phone: +90 552 362 0847

Graphical/Tabular Abstract

The main idea behind this method is to find the most effective features in a database and reuse them in the final layers of CNN architectures to increase accuracy. The proposed method in this paper is shown in Figure A which includes 4 stages.

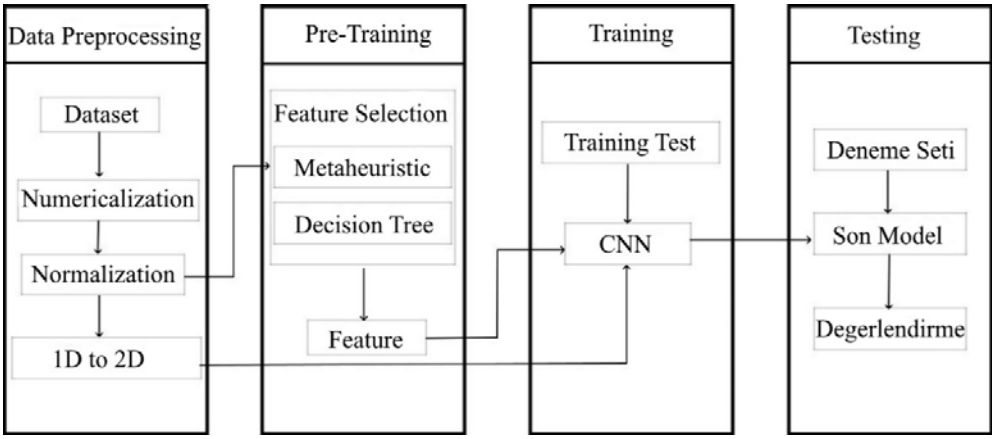


Figure A. Proposed method to combine metaheuristic algorithms and CNN for intrusion detection

Purpose: This study proposes to employ metaheuristic-based feature selection methods for Convolutional Neural Networks (CNNs) models for intrusion detection problem. This approach essentially aims to enhance intrusion detection accuracy for providing better security of network

Theory and Methods: This paper proposes a novel approach for intrusion detection using a metaheuristic-based feature selection method combined with convolutional neural networks (CNNs). We fed these features to CNNs including ResNet50, VGG16, and EfficientNet. The proposed feature selection method was able to find the strong input features and improve the accuracy of the CNN model. The main idea behind this method is to find the most effective features in a database and reuse them in the final layers of CNN architectures to increase accuracy. The four stages are data preprocessing, pre-training, training, and testing. The final goal is to train a CNN model to be used to detect intrusion in real-time.

Results: Results indicate that EfficientNet and ResNet50 performed far better than VGG16-16. While EfficientNet and ResNet50 performed well, EfficientNet wins the game as its performance is higher than ResNet50 in many criteria for the different datasets.

Conclusion: Our experimental results showed that the combination of the proposed feature selection method and CNN can be leveraged in some benchmark datasets and CNN architectures. Overall, our findings demonstrate that the proposed method has the potential to effectively identify and classify intrusions in network traffic. The proposed feature selection method can be used in online and real-time applications since the feature selection part is done in the pre-training part. Future research can investigate the applicability of the proposed method in other domains and explore other metaheuristic algorithms for feature selection.

Journal of the Faculty of Engineering and Architecture of Gazi University 40:1 (2025) 179-188

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Saldırı tespiti için metasezgisel tabanlı özellik seçim yöntemi kullanan evrişimli sinir ağı modelleri

Maryam Salati*, İman Askerzade, Gazi Erkan Bostancı
Ankara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06830, Ankara, Türkiye

ÖNEÇIKANLAR

- İnternet ağlarında güvenliği sağlamada derin öğrenme ve sınıflandırma algoritmalarının rolünün araştırılması
- Evrişimli Sinir Ağları (CNN'ler) ile birleştirilmiş meta-sezgisel tabanlı bir özellik seçim yöntemi kullanılması
- Seçilen özelliklerin daha sonra izinsiz giriş tespitinin doğruluğunu artırmak için CNN'leri beslemesi

Makale Bilgileri
Araştırma Makalesi
Geliş: 24.04.2023
Kabul: 12.12.2023

DOI:
10.17341/gazimmfd.1287186

Anahtar Kelimeler:
İzinsiz giriş tespiti, evrişimli sinir ağı, meta-sezgisel algoritmalar, özellik seçimi, karar ağacı

ÖZ

Bu çalışma, evrişimli sinir ağları (CNN'ler) ile birleştirilmiş meta-sezgisel tabanlı bir özellik seçim yöntemi kullanarak izinsiz giriş tespiti için yeni bir yaklaşım önermektedir. Önerilen seçme yöntemi, farklı veri kümelerinden en önemli özellikleri seçmek için bir karar ağacı ve metasezgisel bir algoritma kullanmaktadır. Seçilen özellikler daha sonra izinsiz giriş tespitinin doğruluğunu artırmak için sırasıyla ResNet50, VGG16 ve EfficientNet modelleri için veri girişi sağlamaktadır. Veri setindeki deneysel sonuçlar, önerilen yöntemin farklı kriterler açısından referans olabileceğini göstermektedir. Nihai sonuçlar EfficientNet ve ResNet50'nin VGG16'dan çok daha iyi performans sergilediğini kanıtlamaktadır. EfficientNet ve ResNet50 algoritmaları NSL-KDD, DEFCON ve CDX veri setlerine uygulandığında, en iyi doğruluk oranları uygun olarak %96.2 ve %81,3 gibidir. Bunun yanısıra EfficientNet özgüllük kriterine göre en yüksek orana 98,6 % sahip iken, ResNet50 95,1% duyarlılık oranı ve F1 skor için 95,2% oranı ile öne çıkmaktadır.

Convolutional neural network models using metaheuristic based feature selection method for intrusion detection

HIGHLIGHTS

- Investigation of the role of deep learning and classification algorithms in providing security in internet networks
- Using a meta-heuristic-based feature selection method combined with convolutional neural networks (CNNs)
- The selected features are then fed into CNNs, to improve the accuracy of intrusion detection

Article Info
Research Article
Received: 24.04.2023
Accepted: 12.12.2023

DOI:
10.17341/gazimmfd.1287186

Keywords:
Intrusion detection, convolutional neural network, meta-heuristic algorithms, feature selection, decision tree

ABSTRACT

This paper proposes a novel approach for intrusion detection using a metaheuristic-based feature selection method combined with convolutional neural networks (CNNs). The feature selection method employs a decision tree and a metaheuristic algorithm to select the most important features from different datasets. The selected features are then feed into CNNs, including ResNet50, VGG16, and EfficientNet, to improve the accuracy of intrusion detection. Experimental results on several benchmark datasets show that the proposed method can be promising in terms of different criteria. The final results prove that EfficientNet and ResNet50 perform much better than VGG16. When EfficientNet and ResNet50 algorithms are applied to NSL-KDD, DEFCON and CDX datasets, the best accuracy rates are 96.2% and 81.3% correspondingly. In addition, while EfficientNet has the highest rate of 98.6% according to the specificity criterion, ResNet50 stands out with a recall rate of 95.1% and a rate of 95.2% for F1score.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *msalati@ankara.edu.tr, imasker@eng.ankara.edu.tr, ebostanci@ankara.edu.tr / Tel: +90 552 362 0847

1. Giriş (Introduction)

Siber saldırılar, kişisel, finansal ve resmi bilgilerimizin giderek daha fazla çevrimiçi olarak saklandığı günümüz dünyasında artan bir endişe kaynağıdır. İzinsiz Giriş Tespit Sistemi (IDS), kullanıcı kimlik doğrulamasını destekleyerek, güvenli erişim sağlayarak gizlilik kaybını önlemektedir. IDS bilgisayar ağlarını saldırılardan korumayı hedeflediğinden, bilgisayar ve ağ güvenliğinin kritik bir yönüdür. Bir IDS'nin işlevi, verileri toplamak, analiz etmek ve daha sonra ek inceleme için bir insan ağ analistine iletilen uyarılar oluşturmak için bir algılama mekanizmasına dayanmaktadır [1]. İnternetin ve iletişimin hızlı büyümesi iletilen verilerde büyük bir artışa neden olmuştur. Saldırganlar bu verilere göz dikmekle, çalmak veya bozmak için sürekli olarak yeni saldırılar oluşturmaktadırlar. Bu saldırıların artması, sistemlerin güvenliği için bir sorundur ve izinsiz giriş tespiti için en büyük zorluklardan birini meydana getirmektedir. IDS, ağ trafiğini inceleyerek izinsiz girişleri tespit etmeye yardımcı olan bir araçtır. Birçok araştırmacı yeni IDS çözümleri üzerinde çalışmış ve bu çözümleri oluşturmuş olsa da, yanlış alarm oranlarını azaltırken iyi bir algılama doğruluğuna sahip olmak için IDS'nin hala iyileştirilmesi gerekmektedir. Ek olarak, birçok IDS sıfırıncı gün saldırılarını tespit etmekte zorlanmaktadır. Son zamanlarda, bu alanda çalışılan makine öğrenimi (Machine Learning, ML) algoritmaları, ağ izinsiz girişini verimli bir şekilde ve yüksek doğrulukla tespit etmek için yapılan araştırmacılar arasında popüler bir çalışma alanı olarak öne çıkmaktadır [2].

IDS'ler saldırıları tespit etmek için çeşitli algoritmalar kullanmaktadır. Bu algoritmalar üç sınıfa ayrılır:

1. Tespit için bir dizi kural oluşturmak üzere önceki saldırı ve veri dağıtım bilgilerini kullanan kural tabanlı algoritmalar.
2. İzinsiz giriş modellerinin istatistiksel bir dağılımını oluşturarak anormallikleri tanımlayan istatistik tabanlı algoritmalar.
3. Farklı saldırı türleri arasında ayrım yapabilen sınıflandırıcıları eğitmek için öğrenme algoritmalarının benimsendiği ML tabanlı yaklaşımlar.

Kural tabanlı yöntemler, basit ve yürütülmesi hızlı olmakla birlikte, eksik veya gürültülü verileri telafi edemez ve güncellenmesi zordur. Bu sorunların üstesinden gelmek için, kesin olmayan bilgilerin işlenmesini sağlamak için istatistik temelli yaklaşımlar önerilmiştir; bununla birlikte, bu tür yöntemler yüksek bir hesaplama maliyeti gerektirir ve büyük miktarlarda veriyi işlemek için sınırlı bir yeteneğe sahiptir. Son zamanlarda, ML tabanlı yaklaşımlar üzerinde karmaşık izinsiz giriş modellerini tespit etmek için büyük miktarda veri üzerinde eğitilebilen karmaşık çıkarım modellerini kullanma yetenekleri nedeniyle giderek daha fazla çalışılmaktadır. Yeni ağ paradigmalarının ve karmaşık çıkarım modellerinin ortaya çıkmasına yol açan, internet üzerinden iletilen artan veri miktarı nedeniyle, bu makalede siber güvenlik ve IDS'lere yönelik makine öğrenimi tabanlı yaklaşımlara odaklanılmıştır [3].

Bu araştırmada, izinsiz giriş tespiti için yeni bir metasezgisel tabanlı özellik seçme yöntemi önerilmiş ve tespit doğruluğunu daha da artırmak için Evrişimli Sinir Ağları (CNN) ile kombinasyonu kullanılmıştır. CNN, karmaşık verileri işlemek için tasarlanmış iyi bilinen bir yapıdır. CNN, geleneksel makine öğrenimi yaklaşımlarının tipik sınırlamalarının üstesinden gelir ve çoğunlukla IDS'lerde kullanılır. Gizlilik sorunlarını ve güvenlik tehditlerini ele almak için IDS'lerde birkaç CNN tabanlı yaklaşım uygulanmıştır. Bundan dolayı, bu makalede izinsiz ağ girişlerini, anormallikleri ve diğer saldırı türlerini tespit etmek için CNN'nin çeşitli kullanımları önerilmiştir. Önerilen yöntem, birkaç veri seti kullanılarak değerlendirilmiş ve elde olunan sonuçlar, çeşitli siber tehdit türlerini tespitinde etkinliğini göstermiştir. Geleneksel izinsiz giriş tespit sistemleri genellikle, etkinlikleri sınırlı olabilen ve hızla gelişen tehditlere ayak uydurmak için mücadele edebilen kural tabanlı yaklaşımlara veya imza tabanlı yöntemlere güvenirler. Bu sınırlamaların üstesinden gelmek için araştırmacılar, izinsiz giriş tespitinin doğruluğunu ve verimliliğini artırmak için makine öğrenimi tekniklerinin kullanımı üzerine geniş araştırmalar yapmışlardır [4-6].

Elde edilen sonuçların, ilgili yöntemin doğruluk, duyarlılık, F1 skor ve özgüllük açısından diğer son teknoloji yöntemlerden daha iyi performans gösterdiği kanıtlanmıştır. Bu iş izinsiz giriş tespitini iyileştirme yaklaşımımızın potansiyelini vurgulamaktadır.

Böylece, bu çalışmanın özgün değerleri aşağıdakilerden oluşmaktadır:

1. Saldırı tespiti için evrişimli algoritmalardan yararlanan uzman görüşleri ile birlikte metasezgisel tabanlı bir özellik seçme yöntemi önerilmektedir.
2. Bu yaklaşımların etkinliği CNN'le birleştirilmiş ve veri kümeleri üzerinde performansları değerlendirilerek uygulanmıştır.
3. Seçilen özellikler daha sonra izinsiz giriş tespitinin doğruluğunu artırmak için ResNet50, VGG16 ve EfficientNet dahil olmak üzere farklı CNN modelleri ile eğitilmişlerdir.

Bu çalışma organizasyonu şu şekildedir: 2. bölümde, alanyazın taraması sonuçlarına yer verilmiştir. Burada farklı veri kümeleri, CNN mimarileri ve meta-sezgisel algoritmalar tartışılarak çalışmanın geri kalanı için temel ve gerekli girdiler sağlanmıştır. Bölüm 3 bu çalışmada önerilen yöntemi ayrıntılı olarak tanıtmaktadır. Sonraki bölümler, çalışmanın bulguları üzerine kısa bir tartışma ve ardından deney sonuçlarını göstermektedir. Nihai olarak, sonuç bölümü ve gelecek çalışmalar için öneriler verilmektedir.

2. Alanyazın Taraması (Literature Review)

Saldırı tespit sistemleri, bilgisayar ağlarının güvenliğinin sağlanmasında kritik bir rol oynamaktadır. IDS oluşturmaya yönelik yaygın bir yaklaşım, özellik seçimi ve derin öğrenme algoritmaları gibi makine öğrenimi tekniklerini kullanmaktır. Bu bölümde, izinsiz giriş tespiti, farklı CNN ve metasezgisel algoritmalar için veri kümelerinin incelemesi sunulmuştur.

Yapılan çalışmalarda IDS'ler için çeşitli özellik seçim yöntemleri önerilmiştir. Örneğin, Saidi vd. [7] çalışmasında bir genetik algoritmaya (GA) dayalı bir öznitelik seçim yöntemi önerirken, Alzaqebah vd. [8] parçacık sürü optimizasyonu (PSO) algoritması kullanmıştır. Temel bileşen analizi (PCA) [9] ve ortak bilgi [10] gibi diğer yöntemler de araştırılmıştır. Bu yöntemler, hesaplama maliyetlerini en aza indirirken izinsiz girişleri tespit etmek için en uygun olan bir özellik alt kümesini tanımlamayı amaçlamaktadırlar.

Metasezgisel algoritmalar, izinsiz giriş tespit sistemlerinde özellik seçimi için kullanılabilen bir optimizasyon algoritmaları ailesidir. Özellikle GA'lar bu bağlamda yaygın olarak kullanılmaktadır [11]. Örneğin, Vijayanand vd. [12] çalışmasında GA tabanlı öznitelik seçimini bir destek vektör makine sınıflandırıcısı ile birleştiren melez izinsiz giriş IDS önermiştir. Benzetimli tavlama (simulated annealing) ve tabu arama gibi diğer metasezgisel algoritmalar da araştırılmıştır [13]. Bu yöntemler, geniş bir arama alanında en uygun özellik alt kümesini aramak için esnek ve ölçeklenebilir yol önermektedirler. Makine öğrenimi algoritmaları, güçleri ve esneklikleri nedeniyle, yetkisiz erişim tespiti uygulamasında büyük ilgi görmektedir. Örneğin, ML algoritmaları saldırı kaynağının ve yerinin belirlenmesine yardımcı olmaktadırlar ([14]).

Son yıllarda, CNN algoritmalar izinsiz girişleri tespit etmek için güçlü bir araç olarak ortaya çıkmıştır [15, 16]. CNN'ler, saldırı tespit sistemlerinin doğruluğunu ve verimliliğini artırabilen ham girdi verilerinden ilgili özellikleri otomatik olarak öğrenebilmektedirler. Bu doğrultuda özellik seçimi ve CNN'leri birleştirmek için çeşitli yaklaşımlar önerilmiştir. Örneğin, Rafique vd. [17], bir CNN sınıflandırıcısına beslenen özelliklerin bir alt kümesini seçmek için sarmalayıcı tabanlı bir özellik seçme yöntemi kullanmıştır.

Bilindiği gibi izinsiz giriş tespit sistemleri için metasezgisel tabanlı öznitelik seçiminin kullanılmasına ilişkin sınırlı sayıda çalışma yapılmıştır. Çalışma [18], GWO (Gri Kurt) optimizasyon algoritmasına dayalı bir özellik seçme yöntemi önerirken, Wang vd. [19] hibrit bir PSO ve yapay arı kolonisi algoritması kullanmıştır. Ancak, bu yöntemler izinsiz giriş tespiti için CNN'lerle birleştirilmemiştir. Önerdiğimiz yaklaşım önceki çalışmalardan farklı olarak metasezgisel tabanlı öznitelik seçme yöntemini CNN tabanlı bir model ile birleştiren hibrit bir yaklaşım önermekte olduğundan özgün değer sunar.

Genel olarak, mevcut alanyazın taramasından elde edilen bulgu metasezgisel tabanlı özellik seçiminin verimli ve doğru IDS oluşturmak için güçlü bir araç olabileceği yönündedir. Bu çalışmada, ilgili yaklaşımı CNN'lerle birleştirerek IDS performansının daha da geliştirilmesi, ayrıca eğitim ve test süreçlerinin hesaplama maliyetinin azaltılması amaçlanmıştır.

2.1. Veri kümeleri (Datasets)

Siber güvenlik saldırı tespiti araştırma ve geliştirmesi için yaygın olarak kullanılan birkaç veri kümesi vardır. Popüler veri kümelerinden bazıları şunlardır: KDD Cup 1999, NSL-KDD, DEFCON, CDX, Kyoto 2006+, DARPA IDS, CICIDS2017, ISCX-IDS2012 ve UNSW-NB15. Bu bölümde araştırma için kullanacağımız Veri kümesinin arka planı ve özellikleri özetlenmiştir ve bu veri setlerini seçmemizin nedeni, araştırma alanındaki popülerliklerinden kaynaklanmaktadır:

NSL-KDD: Bu veri kümesi, KDD Cup 1999 veri setinin, orijinal veri setinin bazı sınırlamalarını gidermek için çeşitli modifikasyonlarla geliştirilmiş bir versiyonudur. Normal ve saldırı verilerinin daha dengeli bir karışımını içerir ve daha az gereksiz ve ilgisiz özelliğe sahiptir [20].

DEFCON: DEFCON veri seti, her yıl dünyanın en büyük hacker konferanslarından biri olan DEFCON konferansında ortaya çıkmıştır. Bu veri seti DEFCON ağ trafiği analizi yarışmasının bir parçası olarak yayınlanmaktadır. Veri kümesi, hem normal hem de kötü amaçlı trafik dahil olmak üzere konferans sırasında yakalanan ağ trafiği verilerini içermektedir. Ancak, DEFCON veri kümesinin nispeten küçük bir veri kümesi olduğunu ve gerçek senaryolarda meydana gelebilecek tüm olası saldırı ve tehdit türlerini temsil etmediğini göz önünde bulundurmak gerekmektedir. Herhangi bir veri setinde olduğu gibi, DEFCON veri setindeki IDS performansı gerçek performansla uyuşmayabilir [21].

CDX: CDX (Siber Savunma Tatbikatı) veri seti, DARPA (Savunma İleri Araştırma Projeleri Ajansı) Siber Genom Programı için üretilmiş bir ağ trafiği veri setidir. Veri seti, IDS ve kötü amaçlı yazılım analizi araştırmalarını desteklemek için oluşturulmuştur. CDX veri seti, gerçek dünyadaki bir siber saldırı senaryosunu simüle eden bir siber savunma tatbikatı sırasında toplanan ağ trafiği verilerinden oluşur. Veri kümesi, SQL enjeksiyonu (veri tabanına dayalı uygulamalara saldırmak için kullanılan bir atak tekniğidir), siteler arası komut dosyası çalıştırma ve arabellek taşması saldırıları gibi çeşitli saldırı türleri ve izinsiz girişlerle birlikte hem normal hem de saldırı trafiğinin bir karışımını içermektedir [22].

Özellik çıkarma yöntemleri, orijinal özellikleri birleştirerek boyut azaltmayı sağlar. Bu nedenle, genellikle daha ayırt edici özelliklere sahip bir dizi yeni özellik yaratabilirler. NSL-KDD, DEFCON ve CDX'in her biri sırasıyla 41, 10 ve 874 özelliğe sahiptirler.

2.2. CNN Mimarisi (CNN Architecture)

Son yıllarda, günümüzde bilgisayar sistemlerinin sunduğu güçlü hesaplama hızı varlığında iyi bir performans sağlayan çeşitli CNN mimarileri geliştirilmiştir. Bu araştırmada bu alanda önde gelen üç popüler önceden eğitilmiş mimari deneylerde kullanılmıştır.

VGG16: VGG16, Oxford Üniversitesi'nde Visual Geometry Group (VGG) tarafından 2014 yılında tanıtılan derin bir evrişimli sinir ağı mimarisidir. Görüntü sınıflandırma görevleri için popüler bir mimaridir ve üzerinde iyi sonuçlar elde etmiştir. VGG16 mimarisi 16 katmandan oluşur, ilk 13 katman evrişimli katmanlar ve geri kalan 3 katman tamamen bağlantılı katmanlardır. Ağın derinliklerine inildikçe evrişimli katmanlardaki filtre sayısı artar. VGG16 mimarisinin en önemli özelliklerinden biri sadeliği ve tekdüzeliğidir. Evrişimli katmanlar, sabit bir filtre boyutuna sahiptir ve sıralı bir şekilde düzenlenerek farklı veri kümeleri ve görevler için mimarinin çoğaltılmasını kolaylaştırır. Mimari ayrıca giriş görüntüsündeki karmaşık özellikleri yakalayacak ölçüde derindir, ancak kaybolan gradyan (ağı güncellemek için kullanılan gradyanların çıkış katmanlarından önceki katmanlara geri yayıldığı için çok küçük hale geldiği veya "yok olduğu" derin sinir ağlarının eğitimi sırasında ortaya çıkan bir olgudur), probleminden muzdarip olmayacak kadar derin değildir [23]. ResNet50: ResNet50, Microsoft Research tarafından 2015 yılında tanıtılan derin bir evrişimli sinir ağı mimarisidir. "Artık Ağ" anlamına gelen ResNet mimarisinin bir çeşididir ve çok derin sinir ağlarında kaybolan gradyanlar sorununu çözmek için tasarlanmıştır. ResNet50 mimarisi, katmanların çoğu evrişimli katmanlar olan 50 katmandan oluşur. Mimari, çok derin ağların eğitimini sağlamak için tasarlanmış artık bloklar içerir. Her artık blok, bir veya daha fazla katmanı atlayan kısayol bağlantılarıyla iki veya daha fazla evrişimli katman içerir. Kısayol bağlantıları, gradyanların ağ üzerinden daha kolay yayılmasına izin vererek yok olan gradyan sorununu çözmeye yardımcı olur [24]. ResNet50 mimarisinin en önemli özelliklerinden biri, derin sinir ağlarını eğitebilme yeteneğidir.

EfficientNet: EfficientNet, Google tarafından 2019'da kullanıma sunulan bir derin sinir ağı mimarileri ailesidir. EfficientNet mimarisi, hesaplama ve bellek gereksinimleri açısından son derece verimli olurken görüntü sınıflandırma görevlerinde son teknoloji performans elde etmek için tasarlanmıştır. EfficientNet mimarisi, ağın derinliğini, genişliğini ve çözünürlüğünü ilkeli bir şekilde ölçeklendiren bileşik bir ölçeklendirme yöntemine dayanır. Ölçeklendirme, optimum performans ve verimlilik elde etmek için dengeli bir şekilde gerçekleştirilir. Mimari, ağın hesaplama ve bellek gereksinimlerini azaltmak için tasarlanmış evrişimli katmanlar, darboğaz katmanları ve ters artık blokları içermektedir [25, 26].

2.3. Metasezgisel Algoritmalar (Metaheuristic Algorithms)

Metasezgisel algoritmalar, karmaşık optimizasyon problemlerine polinom zamanda çözümler bulmak için kullanılan optimizasyon algoritmaları sınıfıdır. Bu algoritmalar, evrim, sürü davranışı ve fiziksel süreçler gibi doğal olaylardan esinlenmiştir. Çözülmekte olan problemin matematiksel modellerine dayanan geleneksel optimizasyon algoritmalarının aksine, metasezgisel algoritmalar modelden bağımsızdır ve problemin herhangi bir özel yapısını varsaymazlar. Bu, onları daha sağlam ve daha geniş bir sorun yelpazesine uygulanabilir hale getirir. Bu çalışmada aşağıda belirtilen metasezgisel algoritmalar kullanılmıştır.

MOPSO: MOPSO (Çok-Amaçlı Parçacık Sürü Optimizasyonu), çok amaçlı optimizasyon problemlerini çözmek için kullanılan metasezgisel bir algoritmadır. Çok amaçlı optimizasyon, hedeflerin birbiriyle çelişebileceği durumlarda birden çok hedefi aynı anda optimize etmeyi amaçlamaktadır.

GWO: GWO (Gri Kurt Optimizasyonu), gri kurtların sosyal davranışlarından ilham alan metasezgisel bir algoritmadır. Gri Kurt optimizasyonu algoritması, Mirjalili vd. (2014) tarafından toplu avlanmalarına dayalı olarak önerilmiştir. GWO, tek amaçlı bir optimizasyon algoritmasıdır.

NSGA-II: NSGA-II (Bastırılmamış Sınıflandırmalı Genetik Algoritma II), çok amaçlı optimizasyon problemlerini çözmek için kullanılan genetik algoritmaya dayalı popüler bir metasezgisel algoritmadır.

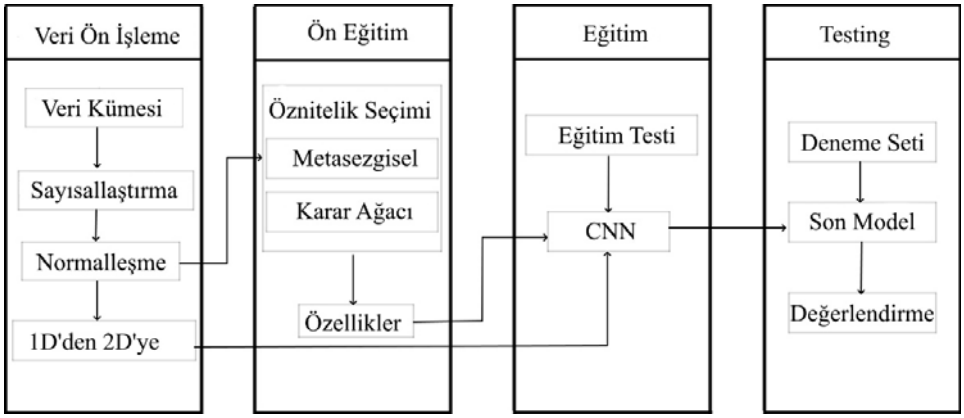
3. Önerilen Yöntem (Proposed Method)

Bu bölümde makalede kullanılan yöntem açıklanmaktadır. Önerilen yöntem 4 aşamayı içermektedir ve Şekil 1'de gösterilmiştir. Bu yöntemin arkasındaki ana fikir, bir veritabanındaki en etkili özellikleri bulmak ve doğruluğu artırmak için bunları CNN mimarilerinin son katmanlarında yeniden kullanmaktır. Dört aşamalı yöntem ön işleme, ön eğitim, eğitim ve testten oluşmaktadır. Nihai hedef, saldırıyı tespit etmek için kullanılacak bir CNN modeli eğitmektir. Veri ön işleme aşamasında, veri seti özellik seçme algoritmasına ve ayrıca CNN algoritmasına beslenmek üzere hazırlanmalıdır. Seçilen veri kümelerinin özellik vektörü, dizi, tamsayı veya boolean gibi farklı veri türlerini içerir. Bu bağlamda tüm özellikleri sayısallaştırma gerekliliği ortaya çıkmıştır. Ayrıca değişken aralıklara sahip olabildikleri için, özelliklerin normalleştirilmesi de gerekmektedir. Normalleştirilmiş özellikler, özellik seçim algoritmaları tarafından kullanılacaktır. Ancak 1 boyutlu özellik vektörü, CNN algoritmaları için uygun değildir. Böylece, tek boyutlu özellikleri iki boyutluya dönüştürmek için bir dönüşüm gerçekleştirilir.

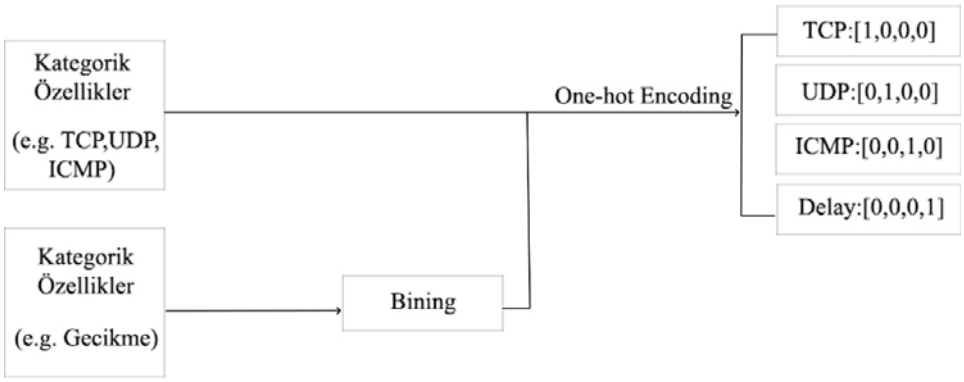
Ön eğitim aşamasında, CNN'nin son katmanına eklenmek üzere en değerli özellikler seçilmektedir. Bu, metasezgisel ve karar ağaçlarını birleştiren bir algoritma tarafından gerçekleştirilmiştir. Daha sonra eğitim veri seti üzerinden eğitim yapılmış ve son olarak, elde edilen sonuçları değerlendirmek ve incelemek için test setinden yararlanılmıştır.

3.1. Veri Ön İşleme (Data Preprocessing)

Her veri kümesinin, bir makine öğrenimi algoritmasını beslemeden önce ön işlemeye ihtiyacı vardır. NSL-KDD veri setini örnek alırsak hem sayısal hem de kategorisel özelliklere sahiptir. Temelde, kategorik özelliklerin sayısala çevrilmesinin gerekliliği durmaktadır. Diğer bir konu da bazı sayısal özelliklerin kesikli, bazılarının ise sürekli olmasıdır. Ayrıca, 1D giriş verilerini 2D görüntülere dönüştüren yeni bir CNN algoritması uygulanmıştır. Bu nedenle, kategorik ve sürekli özellikleri ayrık özelliklere dönüştürmek gerekmektedir. Bunu yapmak için, sürekli özellikleri ayrık olanlara dönüştürmek için "binning" işlemi ve ardından özellikleri sayısal uzaya eşlemek için "one-hot" kodlama algoritması kullanılmıştır. Şekil 2 sayısallaştırma sürecini göstermektedir [14].



Şekil 1. Saldırı tespiti için metasezgisel algoritmaları ve CNN'i birleştirmek için önerilen yöntem
(Proposed method to combine metaheuristic algorithms and CNN for intrusion detectio)



Şekil 2. Binning ve one-hot kodlama kullanarak sayısallaştırma ((Digitization using binning and one-hot coding))

"Binning", sayısal değişkenleri kategorik karşılıklarına dönüştürme işlemidir. Bu süreç, veri kümesindeki gürültüyü veya doğrusal olmamayı azaltarak tahmine dayalı modellerin doğruluğunu artırır. One-hot kodlama, kategorik girdi özelliklerini bir vektörle ifade etmenin bir yoludur; burada kategorinin konumu yer tutucu olarak "1" olarak işaretlenir. Ayrıca, CNN modellerini beslemek için özelliklerden görüntüler çıkarılması gerekir. Bunu yapmak için her 8 bitlik gri tonlamalı görüntü bir piksel olarak değerlendirilir.

3.2. Ön eğitim (Pre-training)

Ön eğitim aşamasının temel amacı, bir veri kümesindeki en etkili özellikleri bulmaktır. Bu bağlamda, doğruluğu en üst düzeye çıkarmak ve seçilen özelliklerin sayısını en aza indirmek için bir karar ağacının döngüsünde metasezgisel algoritmalar kullanılmıştır. Böylece, Eş. 1 ve Eş. 2 ile verilen bir hedef fonksiyonu tanımlanmıştır.

$$F = \alpha_1 * (1 - Doğruluk) + \alpha_2 * SF, \quad (1)$$

$$SF = \frac{seçilen\ özelliklerin\ sayısı}{tüm\ özelliklerin\ sayısı} \quad (2)$$

Burada α_1 ve α_2, doğruluk ve seçilen özelliklerin sayısı arasında değiş tokuş yapmak için kullanılan ayar parametreleridir. Bu aşamanın çıktısı, vektör formatındaki en etkili özellikleri içermektedir.

3.3. Eğitim (Training)

Karar Ağacı ve metasezgisel algoritmaların kombinasyonunun sunduğu en etkili özelliklere sahip olduktan sonra, CNN model eğitimine geçilmiştir. Burada dikkat edilmesi gereken husus, 1D (ön eğitim aşamasından gelen) ve 2D (orijinal veri setinden gelen) özelliklerin birleştirilmesidir. Makine öğreniminde ve derin öğrenmede birleştirme, daha büyük bir tensör oluşturmak için iki veya daha fazla tensörü veya vektörü belirli bir boyut boyunca birleştirme işlemidir. Örneğin, sırasıyla (2, 3) ve (2, 4) şekillerine sahip iki A ve B tensörün varlığı halinde, bunları ikinci boyut boyunca birleştirerek (2, 7) şeklindeki yeni bir tensör elde etmek mümkündür. Birleştirmenin avantajları şunları içerir:

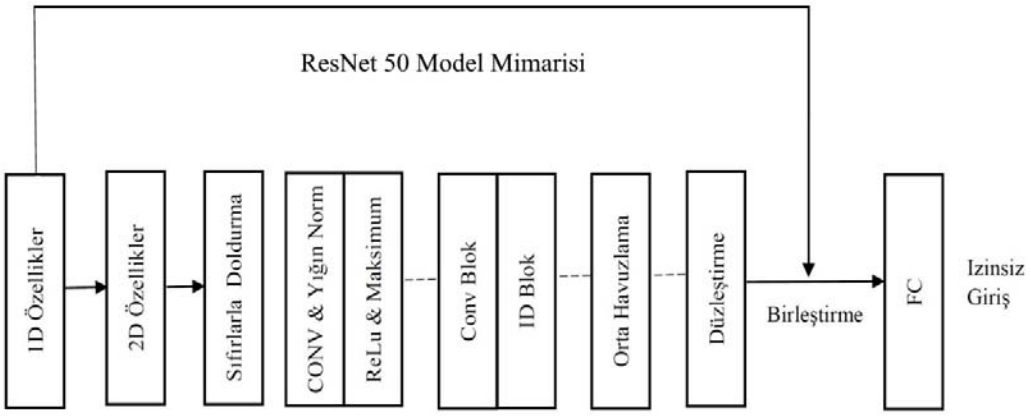
1. Artırılmış Model Kapasitesi: Birden çok tensörü veya vektörü birleştirerek, elde edilen tensör daha büyük bir boyuta sahip olur ve bu da modelin kapasitesini artırabilir. Bu, modelin girdiler ve çıktıları arasındaki daha karmaşık ilişkileri öğrenmesini sağlayabilir.
2. Özellik Kombinasyonu: Birleştirme, girdi verilerinin birden çok özelliğini veya temsilini birleştirmek için kullanılabilir, bu da daha bilgilendirici ve anlamlı özelliklerin yakalanmasına yardımcı olabilir. Bu, modelin performansını artırabilir ve daha iyi genellemeye yol açabilir.
3. Bilginin Korunması: Birleştirme, ortaya çıkan tensöre tüm öğeler dahil edildiğinden, orijinal tensörler veya vektörlerdeki bilgileri korur. Bu, girdilerin sırasını ve bağlamını korumanın önemli olduğu doğal dil işleme veya zaman serisi verileri gibi sıralı verilerle çalışırken faydalı olabilir.
4. Esneklik: Birleştirme, çeşitli şekillerde ve modelin farklı aşamalarında kullanılabilir. Örneğin, bir sinir ağının birden çok katmanının çıktısını birleştirmek veya bir topluluk modeli oluşturmak için farklı modellerin çıktılarını birleştirmek için kullanılabilir.

Şekil 3, genel birleştirme prosedürünü göstermektedir. Burada özellikleri düz veya tek boyutlu olduklarında birleştirdiğimiz Şekil 3'ten görülebilmektedir. Bu nedenle, CNN modellerinde birleştirmenin gerçekleştiği tam bağlantılı katmandan önce bir düzleştirme katmanı eklenmiştir. İlgili şekil, özellik haritaları düz veya tek boyutlu olduğunda birleştirmenin nasıl uygulandığını gösterir. Başka bir deyişle, özellik haritaları, muhtemelen havuzlama veya alt örnekleme işlemleri yoluyla, tek boyutlu bir temsille sonuçlanan bir miktar uzamsal azalmaya maruz kalmıştır.

Burada birleştirme sürecini kolaylaştırmak için CNN modellerinde bir "düzleştirme katmanı" sunulmaktadır. Bu düzleştirme katmanı, evrişim ve havuzlama katmanlarından sonra uygulanır ve mekânsal olarak indirgenmiş özellik haritalarını tek boyutlu bir formata dönüştürür. Bunu yaparak, farklı katmanlardan gelen özellikler tek bir boyuta göre hizalanabilir ve bu da bunların birleştirilmesini mümkün kılar.

Birleştirme, düzleştirilmiş özellik haritalarının tam bağlı katmana ulaştığı noktada gerçekleşir. Tam bağlı katman, birleştirilmiş özellik vektörünü işleyen ve son sınıflandırma veya regresyon görevlerini gerçekleştiren geleneksel sinir ağı mimarilerinde tipik bir bileşendir.

Model, tam bağlı katmandan önce farklı katmanlardaki özellikleri birleştirerek, birden çok soyutlama düzeyinden gelen bilgileri kullanabilir. Bu, CNN'nin veriler içindeki daha karmaşık kalıpları ve ilişkileri öğrenmesini sağlayarak görüntü sınıflandırma veya nesne algılamada gelişmiş performansa yol açar. Genel olarak, makaledeki Şekil 3, önerilen CNN modelindeki kritik birleştirme adımını göstermektedir. Düzleştirme katmanının tanıtılması, modelin çok



Şekil 3. Birleştirme işlemi: Bağlı katmandan önce bir düzleştirme katmanı ekleyerek, özellikler birleştirmiştir
(Concatenating process. By adding a flattening layer before fully connected layer, it is possible to concatenate features)

düzeyli özellikleri verimli bir şekilde birleştirmesine ve kullanmasına olanak tanıyarak nihai olarak hedef sorunu çözmeye katkıda bulunur.

4. Deneysel Metot (Experimental Method)

4.1. Ön eğitim (Pre-training)

Tablo 1, meta-sezgisel algoritmalar ve Karar Ağacı algoritmasını birleştirerek en etkili özelliklerin seçilmesini içeren ön eğitim sonuçlarını göstermektedir. Denklem 1'de ifade edilen hedef fonksiyonu ayar parametreleri α_1=1 ve α_2=0,75'e göre tanımlanmıştır. Bu testler, GWO, MOPSO ve NSGA-II dahil olmak üzere üç meta-sezgisel algoritma için yapılmıştır.

Seçilen özellikler listesinde 2. ve 11. özellikler ortaktır. Toplam öznitelik sayısının %30'undan azı her üç algoritma için seçilmiştir. Tablo 2, aynı deneyi, ancak CDX olan farklı bir veri kümesi için göstermektedir. Aynı şekilde, Tablo 3 DEFCON veri seti için eğitim öncesi aşama sonuçlarını göstermektedir. Bu aşamanın amacı, tamamen bağlı katmandan önce CNN algoritmaları tarafından üretilen özelliklerle birleştirilecek güçlü özellikleri belirlemektir.

4.2. Test

Eğitilmiş modelleri doğrulamak için, test veri seti kullanılmıştır. Değerlendirmek için temel metrikler kullanılmıştır. Bu metriklerde, Gerçek Pozitif (TP), Yanlış Pozitif (FP), Yanlış Negatif (FN) ve True Negative (TN) ile ifade edilirken metrikler aşağıda listelenmiştir.

a) Doğruluk (accuracy) bir modelin başarısını ölçmek için çok kullanılan ancak tek başına yeterli olmadığı görülen bir metriktir.

Doğruluk değeri modelde doğru tahmin ettiğimiz alanların toplam veri kümesine oranı ile hesaplanmaktadır.

b) Kesinlik (Precision) ise pozitif olarak tahminlediğimiz değerlerin gerçekten kaç adedinin pozitif olduğunu göstermektedir.
c) Özgüllük (spesifite): Testin, gerçek sağlamlar içinden sağlamları ayırma yeteneğidir.
d) F1 Skor değeri bize Kesinlik (Precision) ve Duyarlılık (Recall) değerlerinin harmonik ortalamasını göstermektedir.

Basit bir ortalama yerine harmonik ortalama olmasının sebebi ise uç durumları da gözardı etmememiz gerektiğidir. Eğer basit bir ortalama hesaplaması olsaydı Precision değeri 1 ve Recall değeri 0 olan bir modelin F1 Skor'u 0,5 olacaktır ve bu sonuç yanıltıcıdır. Doğruluk (Accuracy) yerine F1 Skor değerinin kullanılmasının en temel sebebi eşit dağılmayan veri kümelerinde hatalı bir model seçimi yapmamaktır. Ayrıca sadece yanlış negatif ya da yanlış pozitif değil, tüm hata maliyetlerini de içerecek bir ölçme metriğine ihtiyaç duyulduğu için F1 Skor çok önemlidir.

$$Doğruluk = \frac{TP+TN}{TP+FN+TN+FN} \quad (3)$$

$$Özgüllük = \frac{TN}{TN+FP} \quad (4)$$

$$Duyarlılık = \frac{TP}{TP+FN} \quad (5)$$

$$F1_{Skor} = \frac{2*Kesinlik*Duyarlılık}{Kesinlik+Duyarlılık} \quad (6)$$

5. Deneysel Sonuçlar ve Tartışmalar (Experimental Results and Discussions)

Bu çalışmada, EfficientNet, ResNet50 ve VGG-16 kullanılarak CNN modelleri, Şekil 3'te önerilen yaklaşıma göre farklı veri kümeleri için eğitilmiştir. Test verileri üzerindeki sonuçlara göre, önerilen yöntem izinsiz giriş tespitinde kabul edilebilir derecede etkili olmuştur. CNN tabanlı modeller aşağıdaki performans kriterleri ile değerlendirilmiştir: Doğruluk, Duyarlılık, F1-Skor ve Özgüllük dahil olmak üzere dört temel kriter üzerinden analiz edilmiştir.

Şekil 4, CNN algoritmaları, GWO metasezgisel algortiması ile NSL-KDD, DEFCON ve CDX, veri kümeleri için test edilmiştir. Sonuçlar aşağıdaki gibidir:

1. GWO algoritması kullanılan NSL-KDD veri seti, elde edilen sonuçlara göre EfficientNet ve ResNet50 VGG16'dan çok daha iyi performans göstermiştir, en iyi performans %86**.**2 doğruluk oranı ile EfficientNet göstermiştir.
2. GWO algoritması kullanılan DEFCON veri seti, elde edilen sonuçlara göre en iyi performansı %74,0 doğruluk oranı ile EfficientNet sağlamıştır.
3. GWO algoritması kullanan CDX veri seti, en iyi performansı %78,1 doğrulukla EfficientNet ile ilgilidir.

Şekil 5, CNN algoritmaları, MOPSO kullanarak NSL-KDD, DEFCON ve CDX, veri kümesi için çalıştırılmıştır. Sonuçların kısa özeti aşağıdadır:

1. MOPSO algoritması kullanılan NSL-KDD veri seti, elde edilen sonuçlara göre EfficientNet ve ResNet50 VGG16'dan çok daha iyi performans göstermiştir, en iyi performans %87,3 doğruluk oranı ile EfficientNet üretmiştir.
2. MOPSO algoritması kullanılan DEFCON veri seti, elde edilen sonuçlara göre VGG16 ve EfficientNet, ResNet50'den çok daha iyi performans göstermiş, en iyi performansı %62,5 doğrulukla ile VGG16 sağlamıştır.
3. MOPSO algoritması kullanan CDX veri seti, en iyi performans %41,5 doğruluk ile EfficientNet sağlamıştır.

Şekil 6, CNN algoritmaları, NSGA-II kullanarak NSL-KDD, DEFCON ve CDX, veri kümesi için test edilmiştir. Performans özetleri aşağıdaki sunulmuştur:

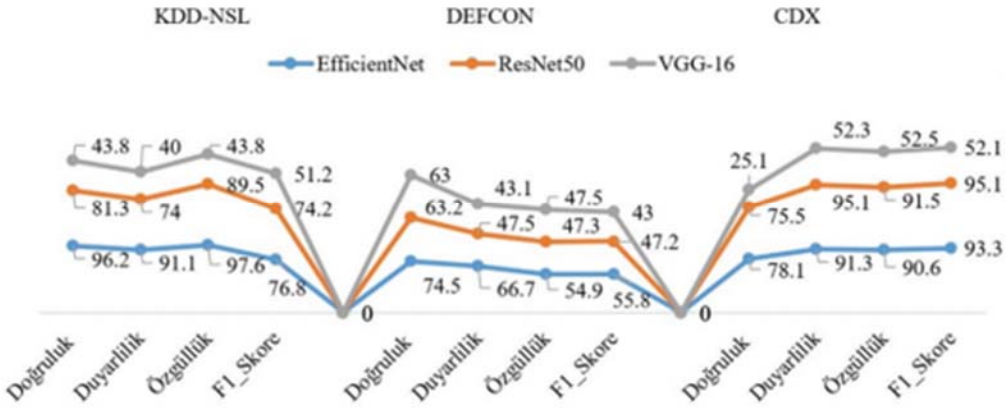
1. NSGA-II algoritması kullanılan NSL-KDD veri seti için elde edilen sonuçlara göre EfficientNet ve ResNet50 VGG16'dan çok daha iyi performans göstermiştir, en iyi performans %85.2 doğruluk oranı ile EfficientNet sağlamıştır.
2. NSGA-II algoritması kullanılan DEFCON veri seti için elde edilen sonuçlara göre EfficientNet ve VGG16, ResNet50'den çok daha iyi performans göstermiştir, en iyi performansı %67,5 doğruluk oranı ile EfficientNet sunmuştur.
3. NSGA-II algoritması kullanan CDX veri seti, en iyi performans 78,8 doğruluk oranı ile EfficientNet sağlamıştır.

Tablo 4 EfficientNet ve ResNet50'in VGG16'dan çok daha iyi performans gösterdiğini göstermektedir. EfficientNet ve ResNet50 iyi performans gösterirken, EfficientNet, farklı veri kümeleri için birçok kriterde ResNet50'den daha yüksek performans göstermiştir. Ayrıca DEFCON veri seti, NSL-KDD ve CDX ile karşılaştırıldığında zorlu bir görev gibi görünmektedir. Bunun nedeni, bu veri kümesinin içerdiği sınırlı sayıda özelliktir.

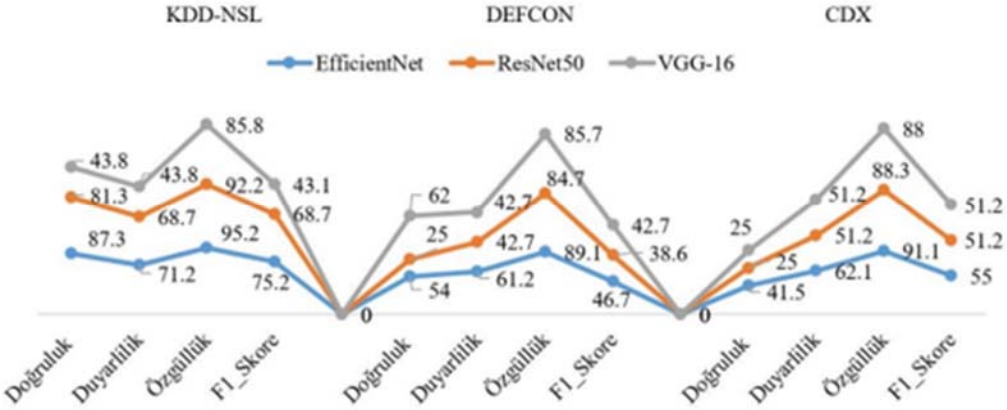
Tablo 4, farklı testlerden elde edilen tüm sonuçları içermektedir. Sonuç olarak, farklı veri kümeleri için birçok kriterde EfficientNet'in performansı ResNet50'den çok daha yüksektir.

5.1. Karşılaştırma Çalışması (Comparison Study)

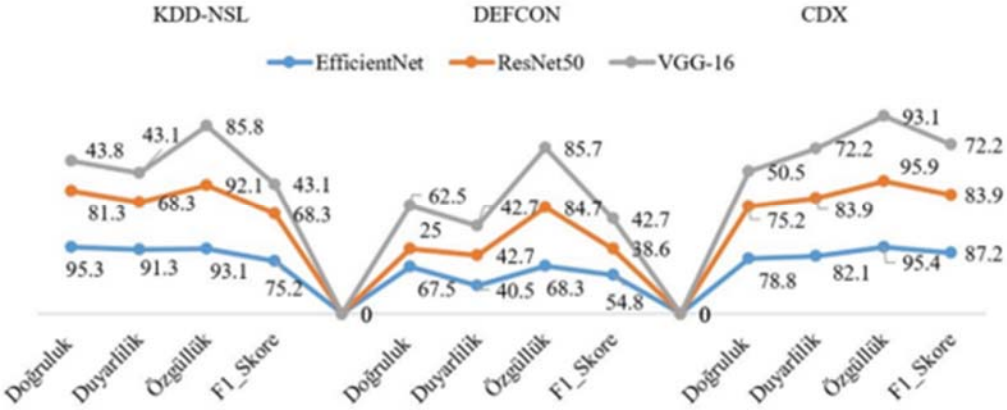
Çalışma [27]'te yazarlar, özellikleri resimlere dönüştürerek saldırı tespiti için CNN tabanlı bir yöntem önerilmektedir. CNN mimarisi ve



Şekil 4. CNN algoritmaları, GWO kullanarak NSL-KDD, DEFCON ve CDX, veri kümesi için test sonuçları
(CNN algorithms test results for NSL-KDD, DEFCON and CDX dataset using GWO)



Şekil 5. CNN algoritmaları, MOPSO kullanarak NSL-KDD, DEFCON ve CDX, veri kümesi için test sonuçları
(CNN algorithms test results for NSL-KDD, DEFCON and CDX dataset using MOPSO)



Şekil 6. CNN algoritmaları, NSGA-II kullanarak NSL-KDD, DEFCON ve CDX veri kümesi için test sonuçları
(CNN algorithms test results for NSL-KDD, DEFCON and CDX dataset using NSGA-II)

Tablo 1. Karar Ağacına göre NSL-KDD için ön eğitim sonuçları (Pre-training results for NSL-KDD by Decision Tree)

Metasezgisel algoritma	Özellik sayısı	Özellik Seçimi	Özellik Seçimi (%)
GWO	41	[2, 4, 22,11, 34, 37, 39]	17,1
MOPSO	41	[1, 2, 5, 10, 11, 16, 20, 21, 29, 34, 37]	26,8
NSGA-II	41	[2, 3, 4, 11, 16, 28]	14,6

NSL-KDD veri seti için ResNet50 kullanarak %79,2 doğruluk elde edilmiştir. Ancak, bu çalışmada önerilen modelde GWO tarafından seçilen ek özelliklerle yaklaşım zenginleştirilmiştir. Sonuç olarak %81,3 doğruluk elde edilmiştir. Çalışma [28] 'da CNN'leri kullanan, eğitim ve test için NSL-KDD veri setini kullanan bir izinsiz giriş tespit sistemi sunulmuştur. Yazarlar, veri kümesindeki sınıf dengesizliği

Tablo 2. Karar Ağacına göre CDX için ön eğitim sonuçları (Pre-training results for CDX by Decision Tree)

Metasezgisel algoritma	Özellik sayısı	Özellik Seçimi	Özellik Seçimi (%)
GWO	41	[1, 6, 8, 15, 21, …]	24,3
MOPSO	41	[1, 5, 8, 34, 42, 45, …]	10,3
NSGA-II	41	[0, 1, 6, 7, 10, 14, …]	39,1

Tablo 3. Karar Ağacına göre DEFCON için ön eğitim sonuçları (Pre-training results for DEFCON by Decision Tree)

Metasezgisel algoritma	Özellik sayısı	Özellik Seçimi	Özellik Seçimi (%)
GWO	41	[1,6,9]	30
MOPSO	41	[6,8]	20
NSGA-II	41	[2,9]	20

Tablo 4. Farklı veri kümeleri, CNN mimarisi ve meta-sezgisel algoritmalar için yapılan testlerin sonuçlar (The results of tests for different datasets, CNN architecture and meta-heuristics alohorithms)

Metasezgisel algoritma	CNN Mimarisi	Doğruluk [NSL-KDD, DEFCON,CDX]	Duyarlılık [NSL-KDD, DEFCON,CDX]	Özgüllük [NSL-KDD, DEFCON,CDX]	F1_Skore [NSL-KDD, DEFCON,CDX]
GWO	EfficientNet	[96.2,74.5,78.1]	[91.1,66.7,91.3]	[98.6,54.9,90.6]	[76.8,55.8,93.3]
	ResNet50	[81.3,63.2,75.5]	[74.0,47.5,95.1]	[89.5,47.3,91.5]	[74.2,47.2,95.2]
	VGG-16	[43.8,63.0,25.1]	[40.0,43.1,52.3]	[43.8,47.5,52.5]	[51.2,43.0,52.1]
MOPSO	EfficientNet	[87.3,54.0,41.5]	[71.2,61.2,62,1]	[95.2,89.1,91.1]	[75.2,46.7,55.0]
	ResNet50	[81.3, 25.0,25.0]	[68.7,42.7, 51.2]	[92.2,84.7,88.3]	[68.7,38.6,51.2]
	VGG-16	[43.8, 62.5,25.0]	[43.8,42.7,51.2]	[85.8,85.7,88.0]	[43.1,42.7,51.2]
NSGA-II	EfficientNet	[95.3,67.5,78.8]	[91.3,40.5,82.1]	[93.1,68.3,95.4]	[75.2, 54.8,87.2]
	ResNet50	[81.3, 25.0,75.2]	[68.3,42.7,83.9]	[92.1,84.7,95.9]	[68.32,38.6,83.9]
	VGG-16	[43.8,62.5,50.5]	[43.1,42.7,72.2]	[85.8,85.7,93.1]	[43.1,42.7,72.2]

sorununu ele almak için, ön eğitim sürecini optimize etmek ve en etkili eğitim verileri yeniden örnekleme ağırlıklarını elde etmek için "Meyve Sineği Optimizasyonu" (Fruit Fly Optimization Algorithm-FOA) algoritmasını kullanmışlardır. NSL-KDD için bu makaleden elde edilen sonuçlar, EfficientNet dahil CNN mimarisinde de önerdiğimiz yaklaşımdan daha düşük olan %95,6'lık bir doğruluk ortaya koymaktadır. Sonuç olarak %96,2 doğruluk elde edilmiştir. Çalışma [29] 'de bir SDN ortamında akış tabanlı anormallik tespiti için derin bir öğrenme yaklaşımı uygulanmıştır. Saldırı tespit sistemi için Derin Sinir Ağı (DNN) modeli oluşturulmuş ve model NSLKDD Veri Kümesi ile eğitilmiştir. DNN yaklaşımı ile NSL-KDD veri setinin sınıflandırmasını yaptıklarında %75,75 doğruluk elde ettiklerini gözlemlemişlerdir. Bu sonuç bu çalışmada ulaşılan doğruluktan daha düşüktür. Çalışma [30] 'de yazarlar, izinsiz giriş tespiti için birkaç aşamalı bir derin öğrenme yaklaşımı ileli sürmüşlerdir. Bu araştırmada hem KDD 99, hem de NSL-KDD veri setleri için sınıflandırıcılar kullanılmıştır. Veri seti sonuçlarına göre 1-NN ve SVM mimarisi ve KDD 99 veri seti için %65,83 ve %64,05, 1-NN ve SVM mimarisi ve NSL-KDD veri seti için %53,84 ve %56,609 doğruluk elde edilmiştir. Önerilen yöntemin performansı KNN ve SVM algoritmalarından çok daha iyidir. Çalışma [14] 'de genetik algoritma kullanılarak KDD99 veri setinde özellik seçimi yapılmış ve seçilen özellikler kullanılarak anomali belirlemede optimal bir özellik alt kümesi elde edilmeye çalışılmıştır. En iyi sonuçlar, bu makalenin sonuçlarından çok daha iyi olan %97 ile J48 sınıflandırıcılı NSGAII algoritması kullanılarak elde edilmiştir. Ancak NSL-KDD, KDD'99 veri setinin genişletilmiş versiyonudur. İlgili veri seti izinsiz giriş tespit yöntemlerinin karşılaştırmasına yardımcı olan etkili bir kıyaslama veri setidir.

6. Sonuçlar (Conclusions)

Bu çalışmada, izinsiz giriş tespiti uygulamasında farklı veri kümelerindeki en önemli özellikleri seçmek için üçüncü kararla birleştirilmiş metasezgisel tabanlı bir özellik seçme yöntemi önerilmiştir. Bu özellikler ResNet50, VGG16 ve EfficientNet dahil olmak üzere Evrişimli Derin Sinir Ağ modelleri ile kullanılmıştır. Önerilen öznitelik seçim yöntemi, güçlü girdi özniteliklerinin elde edilmesine ve CNN modelinin doğruluğunu yükseltmeye imkan vermiştir. Deneysel sonuçlarımız, önerilen özellik seçim yöntemi, CNN kombinasyonunun bazı veri kümelerinde ve CNN mimarilerinde verimli olabileceğini göstermiştir. Genel olarak bulgularımız, önerilen yöntemin ağ trafiğindeki izinsiz girişleri etkili bir şekilde belirleme ve sınıflandırma potansiyeline sahip olduğunu göstermektedir.

Gelecekteki araştırmalar kapsamında, önerilen yöntemin diğer alanlarda uygulanabilirliği araştırılacak ve özellik seçimi için diğer metasezgisel algoritmaların adaptasyonu üzerinde çalışılacaktır. Ek olarak, önerilen yöntem, izinsiz giriş tespit sistemlerinin performansını daha da iyileştirmek için diğer makine öğrenimi algoritmalarını ve farklı derin öğrenme mimarilerini içerecek şekilde genişletilecektir.

Teşekkür (Acknowledgement)

Yazarlar çalışmanın gelişimini olumlu yönde etkileyen yorumları için editör ve inceleyicilere teşekkür eder.

Kaynaklar (References)

1. Liao H.-J., C.-H. Lin R., Lin Y.-C., and Tung K.-Y., ntrusion detection system: A comprehensive review, Journal of Network and Computer Applications, 36 (1), 16–24, 2013.
2. Gümüşbaş D., Yıldırım T., Genovese A., and Scotti F., A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems, IEEE Systems Journal, 15 (2), 1717–1731, 2020.
3. Agrawal P., Abutarboush H. F., Ganesh T., and A. Mohamed W., Metaheuristic algorithms on feature selection: A survey of one decade of research, Ieee Access, 9, 26766–26791, 2021.
4. Kim J., Kim H., Shim M., and Choi E., CNN-based network intrusion detection against denial-of-service attacks, Electronics, 9 (6), 916, 2020.
5. Dandıl E., Yıldırım M.S., Selvi A.O., Uzun S., Automated liver segmentation using Mask R-CNN on computed tomography scans,

Journal of the Faculty of Engineering and Architecture of Gazi University, 37 (1), 29-46, 2022.
6. Aymaz S., A new hybrid approach for multi-focus image fusion using CNN and SVM methods, Journal of the Faculty of Engineering and Architecture of Gazi University, 39 (2), 1123-1136, 2024.
7. Saidi R., Bouaguel W., and Essoussi N., Hybrid feature selection method based on the genetic algorithm and pearson correlation coefficient, Machine learning paradigms: theory and application, 3–24, 2019.
8. Alzaqebah M. et al., Hybrid feature selection method based on particle swarm optimization and adaptive local search method, International Journal of Electrical and Computer Engineering, 113, 2414, 2021.
9. Hasan H. and Tahir N. M., Feature selection of breast cancer based on principal component analysis, 6th International Colloquium on Signal Processing & its Applications, 1–4, 2010.
10. Fang L. et al., Feature selection method based on mutual information and class separability for dimension reduction in multidimensional time series for clinical data, Biomedical Signal Processing and Control, 21, 82–89, 2015.
11. Dincalp U., Güzel M. S., Sevine O., Bostanci E., and Askerzade I., Anomaly based distributed denial of service attack detection and prevention with machine learning, 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–4, 2018.
12. Vijayanand R., Devaraj D., and Kannapiran B., Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection, Computers & Security, 77, 304–314, 2018.
13. Bakour K., G. S. Daş, and Ünver H. M., 'An intrusion detection system based on a hybrid Tabu-genetic algorithm',International Conference on Computer Science and Engineering (UBMK), 215–220, 2017.
14. Uysal E. İ., Demircioğlu G., Kale G., Bostanci E., Güzel M. S., and Mohammed S. N., 'Network Anomaly Detection System using Genetic Algorithm, Feature Selection and Classification', 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–5, 2019.
15. Jasim A. D. and others, A survey of intrusion detection using deep learning in internet of things, Iraqi Journal for Computer Science and Mathematics, 3 (1), 83–93, 2022.
16. Ahmad Z., Shahid Khan A., Wai Shiang C., Abdullah J., and Ahmad F., Network intrusion detection system: A systematic study of machine learning and deep learning approaches, Transactions on Emerging Telecommunications Technologies, 32 (1), 4150, 2021.
17. Rafique M. Ali F., M., Qureshi A. S., Khan A., and Mirza A. M., Malware classification using deep learning based feature extraction and wrapper based feature selection technique, arXiv preprint arXiv:1910. 10958, 2019.
18. Devi E. M. and Devi R. C. x, Feature selection in intrusion detection grey wolf optimizer, Asian Journal of Research in Social Sciences and Humanities, 7 (3), 671–682, 2017.
19. Wang Z. Li, W., Yan Y., and Li Z., 'PS--ABC: A hybrid algorithm based on particle swarm and artificial bee colony for high-dimensional optimization problems', Expert Systems with Applications, 42, 22, 8881–8895, 2015.
20. Protić D. D., 'Review of KDD Cup '99, NSL-KDD and Kyoto 2006+ datasets', Vojnotehnički glasnik/Military Technical Courier, 66 (3), 580–596, 2018.
21. Sharafaldin I., Lashkari A.H., Ghorbani A. A., Toward generating a new intrusion detection dataset and intrusion traffic characterization, ICISSp. 1, 108–116, 2018.
22. Sharafaldin I., Gharib A., Lashkari A.H., Ghorbani A. A., Towards a reliable intrusion detection benchmark dataset, Software Networking, 1, 177–200, 2018.
23. Simonyan K. and Zisserman A., Very deep convolutional networks for large-scale image recognition, arXiv preprint arXiv: 1409. 1556, 2014.
24. He K., Zhang X., Ren S., and Sun J., Deep residual learning for image recognition, in Proceedings of the IEEE conference on computer vision and pattern recognition, 770–778, 2016.
25. Tan M. and Le Q., Efficientnet: Rethinking model scaling for convolutional neural networks, in International conference on machine learning, 6105–6114, 2019.
26. Li Z., Qin Z., Huang K., Yang X., and Ye S., Intrusion detection using convolutional neural networks for representation learning, in Neural Information Processing: 24th International Conference, ICONIP 2017, Guangzhou, China, 14-18, Proceedings, Part V, 858–866, 2017.
27. Zhipeng Li,.et al., Intrusion detection using convolutional neural networks for representation learning, Neural Information Processing: 24th International Conference, ICONIP, Guangzhou, China, November 14–18, 2017.
28. Hu J., Liu C., and Cui Y., An improved CNN approach for network intrusion detection system, Int. J. Netw. Secur, 23 (4), 569–575, 2021.
29. Tang T. et al., Deep Learning Approach for Network Intrusion Detection in Software Defined Networking, The International Conference on Wireless Networks and Mobile Communications IEEE . ISBN 978-1-5090-3837-4, 2016.
30. Chowdhury M., Frederick H., Glenn K., Jiang L., Chunsheng X., and Hongyi W., A Few-shot Deep Learning Approach for Improved Intrusion Detection, IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON). New York, NY, USA: IEEE: 456-462, 2017.