# Siber Güvenlik Alanında Derin Öğrenme Yöntemlerinin Kullanımı

**Muhammed Ali Koşan**[1], **Recep Benzer**[2*]

**1** Gazi University, **2** National Defense University, * Corresponding author, rbenzer@kho.edu.tr

**Özet**

Siber dünya hayatımızın bir parçası olmuşken, bu ortamda gezen bilginin değerinden kaynaklı kötücül kişilerinde hedefi olabilmektedir. Bu açıdan yapılan Siber Güvenlik çalışmaları, veri iletimindeki hız ve teknolojik altyapıların gelişiminden dolayı düşük hesap gerektiren işlemlerden büyük ve karmaşık işlem gerektiren problem çözümüne evirilmiştir. Büyük verilerin işlenerek sınıflandırma veya kümeleme gibi öğrenme yöntemlerinin kullanılması gereken problemlere Derin Öğrenme yöntemleri büyük bir bakış açısı getirmiştir. Siber Güvenliğin birçok alanında artık kullanılan Derin Öğrenme yöntemleri ile çözümü diğer Makine Öğrenmesi yöntemleri ile daha düşük başarımlara sahip iken daha yüksek başarım oranları elde edilerek problem çözümündeki kalite arttırılmaktadır. Bu çalışmada, kullanılan bazı Derin Öğrenme yöntemleri ile Siber Güvenlik içindeki kullanım alanları derleme çalışması olarak sunulmaktadır.

**Anahtar Kelimeler:** Siber güvenlik, Derin öğrenme, Yapay sinir ağları.

**Title**

Use of Deep Learning Methods in Cyber Security

**Abstract**

While the cyber world has been a part of our life, it can be the target in the evil people who are born from the value of the information that circulates in this environment. In this respect, Cyber Security studies have evolved to solve problems requiring large and complicated operations due to the speed of data transmission and the development of technological infrastructures. Deep Learning methods have given a great viewpoint to the problems that should be used in learning methods such as classification or clustering by processing large data. With Deep Learning methods, which are now used in many areas of Siberian Security, while the other machine learning methods have lower performances, higher performance rates are obtained and quality of problem solution is improved. In this study, some deep learning methods used and the usage areas in Cyber Security are presented as a compilation study.

**Keywords:** Cyber security, Deep learning, Artificial neural networks.

**Citation:** Koşan, M. A., Benzer, R. (2018, October) *Title*. Paper presented at the Fifth International Management Information Systems Conference.

**Editor:** H. Kemal İlter, Ankara Yıldırım Beyazıt University, Turkey

**Received:** August 19, 2018, **Accepted:** October 18, 2018, **Published:** November 10, 2018

**Copyright:** © 2018 IMISC Koşan, Benzer. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

IMISC 2018 PAPER

# Siber Güvenlik Alanında Derin Öğrenme Yöntemlerinin Kullanımı

Muhammed Ali KOŞAN
Bilişim Enstitüsü, Gazi Üniversitesi
makosan@gazi.edu.tr
Recep Benzer
Bilgisayar Mühendisliği, Milli Savunma Üniversitesi
rbenzer@kho.edu.tr

**Abstract**

While the cyber world has been a part of our life, it can be the target in the evil people who are born from the value of the information that circulates in this environment. In this respect, Cyber Security studies have evolved to solve problems requiring large and complicated operations due to the speed of data transmission and the development of technological infrastructures. Deep Learning methods have given a great viewpoint to the problems that should be used in learning methods such as classification or clustering by processing large data. With Deep Learning methods, which are now used in many areas of Siberian Security, while the other machine learning methods have lower performances, higher performance rates are obtained and quality of problem solution is improved. In this study, some deep learning methods used and the usage areas in Cyber Security are presented as a compilation study.

**Keywords** Cyber Security, Deep Learning, Artificial Neural Networks

**Özet**

Siber dünya hayatımızın bir parçası olmuşken, bu ortamda gezen bilginin değerinden kaynaklı kötücül kişilerinde hedefi olabilmektedir. Bu açıdan yapılan Siber Güvenlik çalışmaları, veri iletimindeki hız ve teknolojik altyapıların gelişiminden dolayı düşük hesap gerektiren işlemlerden büyük ve karmaşık işlem gerektiren problem çözümüne evirilmiştir. Büyük verilerin işlenerek sınıflandırma veya kümeleme gibi öğrenme yöntemlerinin kullanılması gereken problemlere Derin Öğrenme yöntemleri büyük bir bakış açısı getirmiştir. Siber Güvenliğin birçok alanında artık kullanılan Derin Öğrenme yöntemleri ile çözümü diğer Makine Öğrenmesi yöntemleri ile daha düşük başarımlara sahip iken daha yüksek başarım oranları elde edilerek problem çözümündeki kalite arttırılmaktadır. Bu çalışmada, kullanılan bazı Derin Öğrenme yöntemleri ile Siber Güvenlik içindeki kullanım alanları derleme çalışması olarak sunulmaktadır.

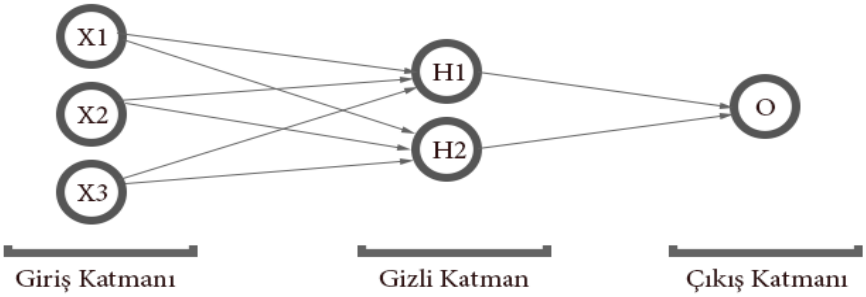
**Anahtar Kelimeler:** Siber Güvenlik, Derin Öğrenme, Yapay Sinir Ağları

## 1. *GİRİŞ*

Gelişen dünyada yaşanılan problemlere çözüm ürettikçe, yaşam standartlarının gelişimi ile birlikte problemlerde büyümekte ve karmaşıklaşmaktadır. Karmaşık problemlerin çözümü, teknoloji yardımı olmadan uzun sürmekte hatta çoğu zaman imkansız olmaktadır. Teknolojinin sunduğu olanaklar gelişmiş CPU'lara dayalı hesaplama ile başlayan serüven ile birçok problemin çözümüne olanak sağlamıştır. Çözüm için kullanılan alanlardan biri Makine Öğrenmesidir. Makine Öğrenmesi ile Yapay Sinir Ağları, Genetik Algoritma ve Destek Vektör Makineleri gibi birçok algoritma farklı uygulama biçimleri ile kullanılmaktadır. Temel olarak Makine Öğrenmesi, elde bulunan veya rastgele oluşturulan veriler ile öğrenim işlemini tamamlayan ve sonraki durumlarda tahmin ve karar verebilme yetisini kullanan yöntemlerden oluşmaktadır [1]. Veriler büyüdükçe, yöntemlerin işlem kalitesi ve süresi artmaktadır. Zamanın değerli olduğu bir devirde, zamansal kazanım sağlamak ve devasa veriler ile işlem yapmayı kolaylaştırmak için Büyük Veri alanı doğmuştur. Bununla birlikte Derin Öğrenme; var olan yöntemlerin geliştirilmesi ile ortaya çıkmış ve yeni yöntemlerin tasarlanmasıyla gelişip büyüyerek ayırt edici bir çalışma alanı olarak günümüze gelmiştir. Derin Öğrenme alanı, ses, resim, video, ağ trafiği ve kullanıcı etkileşimleri gibi devasa verileri tanıma, gruplama ve karar verme gibi amaçlarla kullanılmaktadır. Örnek olarak, Google her gün 20,000 TB civarında veri işlemekte ve aynı şekilde Flicker'da 3.6 TB veri oluşturulmaktadır [2].
Sürekli çalışan en küçük ağlarda dahi, anlık olarak birçok veri akışı oluşmaktadır. Bu veri akışını işlemek için Büyük Veri yöntemleri kullanılmakla birlikte, bu verilerden anlamlı sonuçlar çıkarmak için genel olarak Derin Öğrenme yöntemleri kullanılmaktadır. Bu çalışmada, Derin Öğrenme yöntemlerinin Siber Güvenlik alanında kullanımına yönelik araştırma ve değerlendirmeler yapılmıştır.

## 2. *DERİN ÖĞRENME VE YÖNTEMLERİ*

Makine Öğrenmesi, elde edilen anlamlı bilgiler topluluğunu bir yöntemi eğitmek amacı ile kullanmak ve bu eğitilen modelin sonraki durumlarda en doğru şekilde çözüm üretmesini sağlamakla ilgilenmektedir. Yapay Sinir Ağları (YSA) ise Makine Öğrenmesinin bir alt çalışma alanıdır. YSA, beyindeki nöronları temel alan düğümler ve düğümler arası ağlardan oluşmaktadır. Şekil 1'de örnek bir girdi, gizli katman ve çıktı katmanından oluşan örnek bir YSA modeli sunulmaktadır. 3 giriş alanından oluşan (Xi) ve 2 nörona sahip bir gizli katman (Hi) ile birlikte 1 çıkış alanına (O) sahip bir modeldir.




Şekil 1. Örnek bir YSA modeli

Birçok farklı yöntemi bulunmakla birlikte verinin git gide büyümesi ve işlem hacmine duyulan ihtiyaçtan dolayı Derin Öğrenme alt çalışma alanını kendi bünyesinden ortaya çıkarmıştır. Birçok yöntem olmakla birlikte, en çok Derin İleri Beslemeli Ağlar (Deep Feedforward Networks – DFN), Sınırlı Boltzmann Makineleri (Restricted Boltzmann Machines – RBM), Derin Otomatik Kodlayıcılar (Deep Auto-Encoders – DAE), Konvolüsyonel Sinir Ağları (Convolution Neural Networks – CNN). Tekrarlayan Sinir Ağları (Recurrent Neural Networks – RNN), Derin İnanç Ağları (Deef Belief Networks – DBN) yöntemleri kullanılmakta ve temel özellikleri Tablo 1'de sunulmaktadır. [1-3]

Tablo 1. Bazı Derin Öğrenme Yöntemleri ve Temel Özellikleri

| ***Yöntem*** | **Temel Özellikleri** |
|---|---|
| *DFN* | • Denetimli öğrenme<br>• Normal YSA ile farkları: Katman, Girdi ve Nöron sayıları<br>• Eğitim normal ileri besleme ve geri yayılımlı YSA ile aynı |
| *RBM* | • Denetimsiz öğrenme<br>• Yönsüz bağlantılar içerir<br>• Boltzmann Makinelerinden farklı olarak aynı katmandaki nöronlar birbiri ile bağlı değildir<br>• Bir gizli bir görünür katmandan oluşur<br>• Olasılık dağılımına göre çalışır |
| *DAE* | • Denetimsiz öğrenme<br>• Diğer adı Diabolo Ağıdır<br>• Veri kümesin boyut indirgeyerek kodlama yapmaya yarar<br>• Sıkıştırılmış veriler ile öğrenme de denilebilir |
| *CNN* | • Denetimli öğrenme<br>• Çok katmanlı algılayıcıların (Multi Layer Perceptron – MLP) bir türüdür<br>• İki ana katmandan oluşur<br>  ○ Özellik çıkartımı<br>  ▪ Konvolüsyon ve altörnekleme<br>  ▪ Maksimum havuzlama<br>  ○ Sınıflandırma: Normal MLP ağlarındaki gibi ilerler |
| *RNN* | • Denetimli ve denetimsiz öğrenme<br>• Her nöronun çıktısı tekrarlı olarak tutulmaktadır<br>• Tekrarlı tutulan çıktılar yeni girdiler ile işlenmek amacıyla kullanılır |

| | |
|---|---|
| | • Ardışık girdilerin önceki girdilere bağlı işlenmesinde genel olarak kullanılmaktadır |
| *DBN* | • Eğitim türüne bağlı olarak iki aşamadan oluşur<br>  ○ Denetimli öğrenme<br>  ○ Denetimsiz öğrenme<br>• İşlem süreci temelinde iki bölüm<br>  ○ İlk bölüm yönsüz bir RBM ağı veya DAE ağından oluşmaktadır (Denetimsiz)<br>  ○ Sonraki bölüm ise doğrusal inanç ağlarından oluşur (Denetimli) |

## 3. *SİBER GÜVENLİK VE ÇALIŞMA ALANLARI*

Siber Güvenlik, dijital saldırılardan ağları, sistemleri ve yazılımları korumak olarak tanımlanabilir. Günümüzde hayatımızın hemen her alanına teknoloji hükmetmektedir. Dijital dünyada sunulan veya alınan hizmetlere birçok saldırı yapılmaktadır. Bu hizmetler, kişisel bilgiler, devlet bilgileri, ar-ge dökümanları, finansal kayıtlar gibi verileri barındırıyor ise, yapılan saldırılardan kaynaklı verilen zararın boyutları daha büyük noktalara ulaşmaktadır. Bilinen en iyi örneklerden biri StuxNet virüsü olarak bilinen bir kötücül yazılım ile İran Nükleer programına yapılan ve programı geriye götüren saldırıdır. Bunun dışında, WannaCry adı ile bilinen fidye yazılımından dolayı birçok kurum ve kuruluş verilerini kaybetme eşiğine gelmiştir. Bu bilgilerin kurtarılması için kötücül yazılımı programlayan kişilerin hesaplarına yatan paralar ile verilerin kurtarılması sağlanmıştır. Bu bağlamda fidye yazılımları ile kötücül kişiler büyük miktarlarda para toplamışlardır. Bir diğer siber saldırı ise Mirai botnet olarak bilinen zombi ağı yardımı ile yapılan Dağıtık Servis Dışı Bırakma (DDoS) saldırısıdır. Yapılan saldırı ile Reddit, Twitter, Amazon, Netflix ve BBC gibi çok bilinen ve kullanılan web sitelerine erişim engellenmiştir. Bu noktada, bir web hizmetinin sunduğu hizmetler üzerinden saatlik kazandığı para ve müşterilerine karşı güvenilirlik düzeyi açısından düşünmek gerekir. Bir şirket için bu tür durumlar büyük zarar olarak görülmektedir. Son olarak Carbanak saldırısından bahsedecek olursak, neredeyse 30 ülkede bulunan finans kuruluşlarına yapılan saldırı olarak bilinmektedir. Yüzden fazla finans kuruluşunu etkileyen saldırıda kaynaklar arası farklılıklara göre 100 milyon ile 1 milyar dolar arası kayıp yaşanmıştır [4]. Carbanak saldırısı, 2013 yılından 2018 yılına kadar sürmüştür.

Bahsedilen ve bahsedilmeyen birçok gerçek saldırı olaylarına bakıldığından siber saldırıların verdiği zarar ve siber güvenliğin önemi açıkça görülmektedir. Geniş bir alanı içinde barındıran siber dünya, farklı alt alanları barındırmaktadır.

## 4. *DERİN ÖĞRENMENİN SİBER GÜVENLİK ALANINDA KULLANIMI*

Siber güvenlik alanında problemlerin çözümü problemin türü, içerdiği veri boyutu, problemin hassasiyeti, çözümdeki karar toleransı gibi bazı parametrelere göre çeşitli yöntemler kullanılarak halledilmektedir. Verinin büyük olduğu ve karmaşık işlemler gerektirdiği noktalarda paralel işleme dayalı Derin Öğrenme yöntemleri kullanılmaktadır. Bu bölümde Siber Güvenlik alanında Derin

Öğrenme yöntemleri kullanılarak yapılan çalışmalar incelenmiş ve bu incelenen çalışmalar kategorik olarak alt başlıklar ile sunulmuştur. Fakat çoğu çalışma birden fazla kategori ile tanımlanabilir.

### 4.1. Bilgi Güvenliği

Derin öğrenme ağları sadece yerel tabanlı değil aynı zamanda sunucu tabanlı sistemler olarak da tasarlanabilmektedir. Böylesi sistemlerde verinin bütünlüğü, gizliliğini ve güvenilir iletimini sağlamak önem arz etmektedir. Bu noktada yapılan çalışmada tasarlanan model iki aşamadan oluşmaktadır. İlk aşama yerel ortamda verilerin sunucuya iletildiği alanın şifrelenmesinden oluşur. Sonraki aşama ise bu verilerin sunucuya gönderilerek, sunucuya gelen şifreli verilerin işlenmesidir. İki aşamalı sistemde görsellerden karakter tanıma üzerine bir işlem yapıldığında karakterler şifrelenerek iletildiğinde sunucu ile yerel sistem arasındaki herhangi bir ortadaki adam saldırısı ile elde edilen veri anlamsız bir veri akışı olarak görülmektedir. Böylelikle bilginin güvenli bir şekilde iletimi sağlanabilir. [5]

Derin öğrenmedeki bilgi güvenliği dışında, diğer alanların tamamında çözülen problemler bilgi güvenliği temelindedir.

### 4.2. Ağ Güvenliği

Siber ortamda ağlar verinin erişmek ve göndermek amacı ile kullanılmaktadır. Bir ağ ile bağlı sistemler, hem depoladıkları hem de gönderdikleri verilerin önemli olması durumunda güvenlik açısından yeterli önlemlerin alındığı yerler olmalıdır. Bir ağ ortamında ihlal durumları ağın aktifliği ve büyüklüğüne göre değişim göstermektedir. Eğer ağ büyük ve aktif ise, ağ üzerinde akan ve işlenmesi gereken veride o denli büyük olmaktadır. Böylesi büyük bir veriyi hem hızlı hem de doğru işlemek için paralel işleme ve derin öğrenme yöntemleri kullanılabilmektedir.

RNN ile ağ ihlal tespiti üzerine yapılan çalışmada, en çok kullanılan veri setlerinden olan NSL-KDD veri kümesi kullanılarak başarım oranı üzerine testler yapılmıştır. Kullanılan veri kümesi, Eğitim, Test ve Test21 alt veri kümelerinden oluşmaktadır. İkili (binary) ve kategorik olmak üzere iki tür veri tipi olarak sunulmaktadır. Farklı düğüm ve öğrenme oranları ile yapılan testlerde, 80 gizli katman düğümü ve 0.1 öğrenme oranı ile %99.81 eğitim veri kümesi doğruluğu gözlemlenmiştir. Diğer sınıflandırma yöntemleri ile karşılaştırıldığında öğrenme doğruluğu yüksek ve performans düşük olarak sunulmaktadır. Performansın da arttırılması için grafik işlemcileri kullanılarak paralel işlemler yardımı ile hızlı sınıflandırma yapılabilmektedir. [6]

### 4.3. Kötücül Yazılım Tespiti

Derin öğrenmede kötücül yazılım tespiti siber güvenlik ve derin öğrenme çatısı altında en çok çalışılan konulardan biridir. Kötücül yazılımların özellikleri ve birçok kötücül/iyicil yazılımın bulunmasından dolayı veri kümelerinin birçok parametreden ve örnekten oluşması derin öğrenmeyi bu noktada cazip kılmaktadır. Dört farklı kötücül yazılım ailesinden 5647 örneği barındıran

çalışmada, derin öğrenmenin CNN yöntemi kullanılarak geliştirilen model ile kötücül yazılım tespiti çalışması yapılmıştır. Veri kümesinde bulunan uygulamalar gen dizileri çıkartılarak ağa eğitim amacı ile verilmiştir. Ağa eğitim için verilen veri kümesinin işlenmesi sonrası test işlemlerinde, en bilinen yöntemlerden biri olarak sunulan Destek Vektör Makineleri (Support Vector Machine – SVM) ile önerilen Derin Öğrenme modeli kıyaslanmış ve önerilen modelin daha iyi tespit oranına sahip olduğu (SVM: %94.7, Önerilen Model: %98) gözlemlenmiştir. [7]

### 4.4. Yetkilendirme Güvenliği

Derin Öğrenme yöntemlerinin Siber Güvenlik alanında kullanıldığı bir diğer alan ise Yetkilendirme Güvenliğidir. Yetkilendirme alanında; biyolojik özellikler, PIN, şifre ve davranış tabanlı yetkilendirmeler gibi yöntemler üzerinde çalışılmaktadır. Klavye dinamiklerine göre derin öğrenme yöntemi ile kullanıcı tanımlama üzerine yapılan bir çalışmada, RNN'den türeyen Uzun-Kısa Vadeli Hafıza Ağları (Long-Short Term Memory – LSTM) ve Kapılı Tekrarlayan Birim (Gated Recurrent Unit – GRU) yöntemleri farklı katman sayıları ile test edilmiştir. En iyi hata oranları 2 ve 3 katmanlı LSTM ağlarında gözlemlenmiştir. 2 hücreli LSTM ağında elde edilen hata oranı 0.1 civarındadır. Böylelikle yetkilendirme temelinde başarım oranı yüksek işlemler yapılabilmektedir. [8]

### 4.5. Siber Fiziksel Alan Güvenliği

Siber ortamların donanımsal ve iletim altyapıları da siber ortama yapılan dijital saldırılar gibi fiziksel saldırılara maruz kalabilmektedir. Bunun yanında, kritik öneme sahip alanların korunması da teknolojik donanımlar kullanılarak tespit ve değerlendirme yöntemleri ile sağlanabilmektedir. Korunması gereken fiziksel bir alandaki anormal hareketliliği tespit etmek amacı ile yapılan bir çalışmada CNN yöntemi kullanılarak video işleme ve değerlendirme yöntemi uygulanmıştır. CNN'in GoogleNet ve AlexNet yöntemleri ile birlikte QuadraticSVM yöntemi 4 farklı nesne türünü (arka plan, çanta, geyik ve insan) tespit etmek üzerine test edilmiştir. CNN yöntemleri SVM'e göre daha yüksek başarım oranlarına sahip olurken, QuadraticSVM özellikle insan tespitinde düşük oranlarda başarım göstermiştir. Bu bakımdan video işleme ve bunun siber fiziksel alan güvenliğine uygulaması düşünüldüğünde büyük ve akıcı verilerin işlenmesinde Derin Öğrenme yöntemleri ile daha iyi sonuçlar elde edilebilmektedir. [9]

### 4.6. Spam Tespiti

E-posta, sosyal medya ve bilgi paylaşım sitelerindeki en büyük problemlerden biri spam girdilerin tespitidir. E-posta sağlayıcılarda kullanıcılara gelen maillerin hangilerinin gereksiz ve zararlı girdiği olduğunu her daim bilebilme imkanı bulunmamaktadır. Aynı şekilde, sosyal medya da bir konu veya etikette taranan gündem paylaşımlarını doğru değerlendirmek için spam olan girdilerin temizlenmesi gerekir. Twitter üzerine yapılan bir çalışmada DFN kullanılarak spam aktivitelerinin tespitine yönelik testler yapılmıştır. Sürekli akış ve rastgele olarak elde edilen twitter

paylaşımlarından 4 farklı veri kümesi oluşturulmuştur. Elde edilen veri kümelerinden öznitelik çıkartım yöntemleri kullanılarak paylaşımları tanımlayan vektörler oluşturulmuştur. Sonrasında, derin öğrenme yöntemi uygulanarak spam tespitine yönelik testler yapılmıştır. Uygulamada hem sınıflandırıcı yöntemlerin kıyaslanması hem de sözdizimine dayalı yöntemler kıyaslanmıştır. Yapılan kıyaslamalarda, uygulanan Derin Öğrenme yönteminin tüm yöntemler ile kıyaslanarak hesaplanan başarı ölçütleri değerlendirildiğinde en başarılı yöntem olduğu gözlemlenmiştir. [10]

### 4.7. Donanım Güvenliği

Siber ortamda kişilerin ortam ile etkileşimini sağlayacak donanımsal aygıtlarda güvenlik açısından düşünülmesi gereken bir noktadır. Hayatımızın bir parçası olan bilgisayarlar dışında internetteki uygulamalardan endüstri de bulunan sanayi donanımlarına kadar birçok yerde işlemciler, bellekler ve hatta internet erişimi bulunmaktadır. Taşıtlar da artık akıllı donanımlar ile birlikte internet ve ağ erişime sahip olarak sunulmaktadır. Yapılan bir çalışmada, bir ağa bağlı araçlara yapılan saldırıların tespitine yönelik bazı Derin Öğrenme yöntemleri ile diğer bazı Makine Öğrenmesi yöntemleri kıyaslanmıştır. Komut enjeksiyonu, servis dışı bırakma (DoS), kötücül yazılım (CPU'yu etkileyen), kötücül yazılım (neti etkileyen) saldırı türleri temelinde 7 farklı makine öğrenmesi yöntemi arasında en başarılı ortalama doğruluk oranı RNN yöntemi ile elde edilmiştir. Bu başarım oranı, değerlendirilmesi gereken verinin boyutu ve karmaşıklığı ile Derin Öğrenme yöntemlerinin bu tarz problemlerin çözümü amacıyla geliştirilmesinden kaynaklandığı düşünülebilir. [11]

## 5. *SONUÇ*

Derin öğrenme yöntemleri ilk gündeme geldiği yıllarda özellikle görüntü ve video işleme amacı ile kullanılmıştır. İki ve üç boyutlu medya verileri üzerinde yapılan testlerde yüksek başarımlar elde edildikten sonra farklı büyük verilerde de kullanımı yaygınlaşmıştır. Siber güvenlik alanında depolanan, iletilen verilerin çokluğu ve işlem gücü gereksinimin fazla olduğu dikkate alındığında Derin Öğrenmenin uygulanabileceği alanlardan biri de Siber Güvenlik alanıdır. Bu bağlamda incelenen ve değerlendirilen çalışmalara bakıldığında, Derin Öğrenme yöntemlerinin Siber Güvenlik alanındaki problemlere uygulanması için bazı noktalara dikkat edilmesi gerekmektedir. Bu bağlamda, probleme ait elde edilecek veri kümesinin denetimli mi yoksa denetimsiz yöntemlere mi uygun olduğu, önceki bilginin sonraki bilgiyi etkileyip etkilemediği ve etkiliyorsa bunun düzeyi, problemin çözümünde performansın etkisi, örneklerin tek boyutlumu yoksa çok boyutlumu olduğu gibi temel sorunların cevabını bulmak gerekmektedir. Bunun dışında, yapılan çalışmalar diğer yöntemler ile kıyaslandığında genel olarak yüksek başarım göstermişlerdir. Ama bu avantajı değerlendirilirken CPU ile yapılan işlemlerde karmaşık işlemlerden kaynaklı performansı diğer yöntemlere kıyasla biraz daha düşük olduğu sunulmaktadır. Bu problemi ise, GPU üzerinde yapılacak paralelleştirme işlemleri ile aşabilmekte olduğumuzu görmekteyiz. Siber güvenlik alanında birçok probleme Derin Öğrenme yöntemleri ile çözüm bulmaya çalışan araştırmacıların

daha el değmemiş problemlere de bir süre var olan ve geliştirilecek olan Derin Öğrenme yöntemleri ile çözüm bulmaya devam edecekleri düşünülmektedir.

## *KAYNAKLAR*


[1] W. B. Liu, Z. D. Wang, X. H. Liu, N. Y. Zengb, Y. R. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing,* vol. 234, pp. 11-26, Apr 2017.

[2] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "A survey on deep learning for big data," *Information Fusion,* vol. 42, pp. 146-157, 2018.

[3] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks,* vol. 61, pp. 85-117, Jan 2015.

[4] (2018, 08 May). *Leader of Hacking Group Who Stole $1 Billion From Banks Arrested In Spain*. Available: https://thehackernews.com/2018/03/carbanak-russian-hacker.html

[5] H. Dong, C. Wu, Z. Wei, and Y. K. Guo, "Dropping Activation Outputs With Localized First-Layer Deep Network for Enhancing User Privacy and Data Security," *Ieee Transactions on Information Forensics and Security,* vol. 13, pp. 662-670, Mar 2018.

[6] C. L. Yin, Y. F. Zhu, J. L. Fei, and X. Z. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *Ieee Access,* vol. 5, pp. 21954-21961, 2017.

[7] X. Meng, Z. Shan, F. D. Liu, B. L. Zhao, J. Han, J. Wang*, et al.*, *MCSMGS: Malware Classification Model Based on Deep Learning*. New York: Ieee, 2017.

[8] P. Kobojek and K. Saeed, "Application of recurrent neural networks for user verification based on keystroke dynamics," *Journal of Telecommunications and Information Technology,* p. 80, 2016.

[9] J. J. Stubbs, G. C. Birch, B. L. Woo, and C. G. Kouhestani, "Physical Security Assessment with Convolutional Neural Network Transfer Learning," in *2017 International Carnahan Conference on Security Technology*, A. Morales, R. Vera-Rodriguez, R. Lazzeretti, J. Fierrez, and J. OrtegaGarcia, Eds., ed New York: Ieee, 2017.

[10] T. M. Wu, S. Wen, S. G. Liu, J. Zhang, Y. Xiang, M. Alrubaian*, et al.*, "Detecting spamming activities in twitter based on deep-learning technique," *Concurrency and Computation-Practice & Experience,* vol. 29, p. 11, Oct 2017.

[11] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," *Ieee Access,* vol. 6, pp. 3491-3508, 2018.