VERİ BİLİMİ DERGİSİ
www.dergipark.gov.tr/veri

Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme

Maad M. MIJWIL[1], Emre SADIKOĞLU[2]*, Emine CENGİZ[3], Hasibe CANDAN[4]

[1]*Bağdat Koleji Ekonomi Bilimleri Üniversitesi, Bilgisayar Teknikleri Mühendisliği, Bağdat, IRAK*
[2,3]*Yalova Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Yalova, TÜRKİYE*
[4]*Bursa Teknik Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Bursa, TÜRKİYE*

Özet

Yapay zeka teknolojileri, siber güvenlik de dahil olmak üzere birçok alanı kapsamaktadır. Siber güvenliğin temel amacı; bilişim sistemlerini bilgisayar korsanları tarafından gerçekleştirilebilecek yetkisiz erişim, verilerin silinmesi/değiştirilmesi gibi şantajlara karşı korumak ve siber saldırıları önlemektir. Bu çalışma da, yapay zeka teknolojilerinin temel çerçevesi ve kavramları vurgulanarak dijital ortamda siber güvenliğin sağlanması konusunda yapay zekanın rolü ve önemi anlatılmıştır. Sanal dünyada her geçen gün daha da karmaşıklaşan siber tehditler karşısında kullanıcıların mahremiyetini ve verilerini koruyabilmek için yapay zeka yöntemlerini kullanmanın gerekli olduğu sonucuna varılmıştır.

Anahtar Kelimeler: *Siber güvenlik, Yapay zeka, Makine öğrenmesi, Endüstri 4.0, COVID-19*

Makale Bilgisi

Başvuru:
06/12/2022
Kabul:
17/12/2022

The Role and Essence of Artificial Intelligence in Cybersecurity: A Survey

Abstract

Today, artificial intelligence technologies are entering into many areas, including the area of cybersecurity, which is a branch of technology. The role of cybersecurity is to defend systems, networks and data from hacking and threats, preventing unauthorised access, tampering with, or deleting data, or blackmailing users. This article strives to determine the significance and role of artificial intelligence in achieving cybersecurity in the digital environment and seeking to preserve user data and information from the penetration and destruction of systems by highlighting the essential dimensions and concepts of artificial intelligence techniques. In this article, the authors decided to confirm the role of artificial intelligence in conducting cybersecurity for users of social networking sites. This article concluded that it is necessary to think about artificial intelligence techniques in employing them to protect the privacy and data of individuals and users across various digital platforms and in all areas.

Keywords: *Artificial Intelligence, Cybersecurity, Fourth industrial revolution, Intrusion, COVID-19*

* İletişim e-posta: emre.sadikoglu@yalova.edu.tr

1 Giriş

2000'li yıllarda internetin ve bilgi teknolojilerinin yaygınlaşmasından beri küreselleşme ve çağın getirdiği büyük teknolojik gelişmeler, toplumların hızlı değişimine ön ayak olmuştur. Dördüncü Sanayi Devrimi (Endüstri 4.0), bir önceki sanayi devrimine göre farklı bir dünyanın dizayn edilmesine yol açmıştır [1]. Endüstri 4.0 ile birlikte yeni 'akıllı' elektronik cihazlar hayatımızın her evresine girmiş ve dünya, hızlı bir dijitalleşme dönüşüm süreci yaşamış, yaşamaktadır. Bu devrim; Nesnelerin İnterneti, bulut bilişim, büyük veri analitiği ve yapay zekayı barındıran teknolojileri yaşantımıza entegre etmeyi amaçlar. Bireylerin ve kurumların, kurumların dijital dönüşüm karşısındaki fırsat ve zorluklarını tespit eder [2]. En kritik zorluklardan biri, tüm kurumların internet ile birlikte sıklıkla kullanımı yaygınlaşan verilerin sızma, ele geçirme, silme ve değiştirme gibi saldırılardan önceden belirlenmiş stratejilere göre korumasının gerekli hale gelmesidir. Siber güvenlik, bilgileri korumak ve hassas verilere erişimin engellenmesi için ortaya çıkmıştır [3][4]. Bilgisayar sistemlerinde, nesnelerin interneti ve kablosuz ağlara bağımlılığının artmasıyla bilgisayar korsanları tarafından gerçekleştirilen siber saldırılar da daha karmaşık hale gelmiştir. Bu durumda siber tehditleri tespit etmek ve önlemek için daha sofistike çözümlere ihtiyaç duyulmuştur. Bu nedenle yapay zeka temelli çözümlerin kullanılması kaçınılmaz hale gelmektedir. Yapay zeka ile bütünleştirilen siber güvenlik çözümleri daha etkin, başarımı yüksek koruma sağlamaktadır [5].

Sosyal paylaşım siteleri, dünyanın bir ucundan öbür ucuna bireyleri birbirlerine bağlayan en etkili araç olarak kabul edilirler. Etkileşim sayılarının anormal ve doğal bir şekilde artması, internet üzerinde kullanıcıların mahremiyetinin ihlal edilmesi sonucunu doğurmaktadır. Konu artık Facebook veya Twitter ile sınırlı kalmayıp kullanıcı ve müşterilerin verilerini barındıran birçok platforma yayılmıştır. Bu nedenle kullanıcı veya müşterilerin gizliliğini güvence altına alan ve elektronik ortamda güvenliklerini sağlayan stratejilerin düşünülmesi zorunlu hale gelmiştir. Yapay zeka, dijital ortamın kullanımı ve kullanıcılar için siber güvenliğin sağlanmasında, verilerin ve bilgilerin yetkisiz kişilerce kötüye kullanımının engellenmesinde hayati bir rol oynamaktadır. Günümüzde pek çok kişi siber güvenliği sağlamada ve verileri korumada yapay zeka tekniklerinin kapsamı ve becerisi hakkında bir takım şüphelere sahiptir. Bu makale çalışması, yapay zekanın siber güvenlikteki rolü ve önemini; siber güvenliği sağlamanın ve sosyal paylaşım sitelerinde kullanıcı mahremiyetini korumanın ne ölçüde mümkün olduğunu vurgulamaktadır.

Çalışma beş bölümden oluşmaktadır. Bölüm 2, yapay zekaya ve neden gerekli olduğuna genel bir bakış sunmaktadır. Bölüm 3, siber güvenlik hakkında öz bilgiler vermektedir. Bölüm 4, yapay zekanın topluma hizmeti ve COVID-19 pandemisiyle mücadeleye katkılarından bahsetmektedir. Bölüm 5'te, yapay zekanın siber güvenliği sağlama ve kullanıcı verilerini korumadaki rolü tartışılmaktadır. Son olarak Bölüm 6'da ise bu araştırmanın sonuçları açıklanmaktadır.

2 Yapay Zeka

Yapay zeka, bilgisayar biliminin dallarından biridir ve modern çağda teknoloji ve elektronik endüstrisinin temel taşlarından biridir [6-9]. Yapay zeka, dijital makinelerin ve bilgisayarların düşünme veya geçmiş tecrübelerden öğrenme, karar verme veya bilişsel süreçler gerektiren işlemler için insanlar davranışlarını simüle eden ve insanı andıran belirli görevleri yerine getirme yeteneği olarak tanımlanabilir [10][11]. Ayrıca yapay zeka, öğrenme ve anlama açısından insan gibi davranan sistemler elde etmeyi amaçlar. Bu sistemler kullanıcılarına eğitim, rehberlik, etkileşim vb. çeşitli hizmetler sunar. Yapay zekanın en dikkat çekici dalları makine öğrenmesi ve derin öğrenmedir (Şekil 1).

Yapay zeka, insan kapasitesini artırmak ve daha yüksek doğrulukla karar vermesine yardımcı olmak için insan benzeri robotlar üretmeyi amaçlamaktadır [12][13]. Yapay zeka, müşterilerle çevrimiçi iletişim kurmak veya satranç vb. oyunları oynamak gibi bir zamanlar insan gerektiren karmaşık görevleri yerine getiren uygulamalar için kapsayıcı bir terim haline gelmiştir. Yapay zekanın, insan benzeri karar vermeyi hedefleyen alanı olan makine öğrenmesi, veriye dayalı olarak öğrenmeye veya performansı arttıran sistemler oluşturmaya yoğunlaşmıştır [14-16]. Tüm makine öğrenmesi işleri yapay zeka kapsamında olsa da tüm yapay zeka işlerinin makine öğrenmesi kapsamına girmediğini bilmek önemlidir. Yapay zeka üç bölüme ayrılır [17]:

- **Yapay dar zeka:** Yapay zekanın bu türü, sürücüsüz (otonom) araçlar, görüntü ve konuşma tanıma yazılımı, araç plaka tanıma yazılımı veya akıllı cihazlarda satranç ve tavla

gibi sınırlı ve net görevleri yerine getirebilir. Bu tür, Xbox ve PlayStation oyunlarında yaygın olarak kullanılmaktadır. Ayrıca yapay zekanın bu türü en yaygın olanlardan biridir ve son yıllarda kullanılmaktadır.

- **Yapay genel zeka:** Makineyi kendi başına düşünebilir ve planlayabilir hale getirmeye ve insan düşünmesini gerçekleştirmeye odaklandığından, düşünme açısından insan yeteneğine benzer bir yetenekle çalışır. Yine de bu türün gerçek örnekleri yoktur. Şimdiye kadar var olan tek şey, gerçekleştirmek için çok çaba gerektiren bilimsel araştırma çalışmalarıdır. Yapay sinir ağları tekniği, düşünme ve planlama sürecinde insan beyninde bulunana benzer sinir ağları ürettiği için bir yapay genel zeka sistemidir.
- **Yapay süper zeka:** Bu tür, birçok uygulamada insan zekasının seviyesini aşabilir ve bilgi gerektiren görevlerde uzman bir kişinin yaptığından daha faydalı işler yapabilir. Bu tür, birçok karakteristik özellik gerektirir; Bunlar öğrenme, planlama, otomatik iletişim kurma ve yargıda bulunma gibi yeteneklerdir. Ancak günümüzde var olmayan ve uygulanması çok zor olan teorik bir terim olarak kabul edilmektedir. Bu tür, siborg (siber organizma) dünyasında uzak bir gelecekte gerçekleştirilecektir.

Şekil 1. Yapay zeka, makine öğrenmesi ve derin öğrenme arasındaki farkın kronolojik olarak açıklanması [18]

3 Siber Güvenlik

Genel olarak siber güvenlik, sistemlerin, ağların, programların ve web sitelerinin saldırılara ve izinsiz girişlere, yetkisiz kişilerin girişine ve elektronik saldırılara karşı bir kalkandır [19-21]. Elektronik saldırılar genellikle değiştirmek, yok etmek, şantaj yapmak, verileri çalmak, manipüle etmek ve kamuya açık yayınlamak amacıyla hassas bilgilere erişmeye çalışır. Siber güvenlik kavramı, kurum içi veya dışı sunucularda depolanan dahili veya harici ağlar üzerinden dolaşan veri ve bilgilerin güvenliğini sağlamayı ve onları bilgisayar korsanlığı ve çalınmaya karşı korumayı da içerdiği için bilgi güvenliğinden çok daha geniştir. Bugün dünya her zamankinden ve her şeyden daha fazla teknolojiye tutunuyor; sonuç olarak siber güvenlik, genellikle birden çok koruma katmanından ve yetkisiz erişimin önlenmesinden ve güvenli alıcılara veri aktarımından oluşan belirli bir yaklaşımı benimser. Genellikle kullanıcılar sistemlerini, programlarını ve verilerini siber saldırılara karşı korumayı ve siber saldırılara karşı etkili bir savunma oluşturmak için kullanıcıların ve teknolojilerin iş birliği yapması gereken kötü amaçlı programlarla mücadele etmeyi tercih eder. Diğer bir deyişle, yalnızca bilgi ve gizliliği korumak için bir siber sistem benimsemek mümkün değildir. Bu nedenle mahremiyet ve verileri korumak için kullanıcı, teknoloji ve siber güvenlik girişimlerini yoğunlaştırmak hayati bir önem taşımaktadır. Son yirmi yılda, birbirimizle iletişim kurduğumuz araçlar, Facebook, Twitter, YouTube ve Tiktok gibi yeni ve etkili dijital platformların ortaya çıkmasıyla kökten değişmiş olup bilgi keşfi ve kullanımında sosyal medya etkili ve giderek daha önemli bir hale gelmiştir. Ayrıca sosyal medya, resmi kaynaklardan tek yönlü bilgi aktarımının yanı sıra, bir kişi veya grup tarafından yapılan ve pasif alıcı oldukları

kadar artık aktif bilgi üreticisi de olan internet kullanıcılarının bilgileri aktarmadaki etkin yeteneğini ortaya koymuştur. Sosyal paylaşım siteleri, küresel internet üzerinden birçok kullanıcıya hizmet veren ve onlar aracılığıyla ortak ilgi alanlarını paylaşan milyonlarca insanla iletişim kurulabilen sitelerdir [22]. Bu siteler, kullanıcıların çizim ve fotoğraf paylaşımı, video alışverişi, blog oluşturma, mesaj gönderme ve anlık sohbetler kurabilmelerine olanak tanır. Buna ek olarak bu siteler, özellikle bireysel kişisel olayların tanıtımı ile ilgili olarak gelenekselden biçim, teknoloji ve özellik bakımından farklı olan yeni etkileşimli araçların sonucu olarak ortaya çıkmıştır.

4 Yapay Zeka Uygulamaları

Son zamanlarda hayatımızın önemli ve vazgeçilmez bir parçası haline gelen yapay zekaya birçok alanda güvenilmektedir [23]. Yapay zeka, özel bireylerin tüm ihtiyaçlarını karşılayabilme yeteneğine sahiptir. Örnek olarak, görme engellileri desteklemek için çalışan yapay zekaya dayalı cihazlar, Microsoft'un görme engellilere etrafındakileri anlatan uygulamaları bulunmakta ve böylece görme engelli bireyler, görme duyusunun eksikliğini hissetmiyor [24]. Metinleri sesli okuyan, insanları ve duyguları tanımlayan bu uygulamalar makine öğrenmesine dayalı 3 boyutlu teknikleri kullanırlar. Aslında yapay zeka, COVID-19 pandemisinin ortaya çıkmasından bu yana pratikte çok popüler hale geldi ve birçok doktorun hasta verilerini analiz etmesine ve virüs ile enfeksiyon oranını belirlemesine yardımcı oldu [25-27]. Yapay zeka, aile içi şiddet mağdurlarına yardım etme işine girmiş ve aile içi şiddete maruz kalmış bireylerle birçok görüşme yapılarak bu tür şiddetle karşılaştıklarında daha faydalı yardım almalarına yardımcı olmuştur [28]. Bu görüşmeler, kadınların en çok öldürüldüğü ülkelerden biri olduğu için Güney Afrika'da yapıldı ve şiddetin önlenmesi konusunda onlara yardımcı olmak için yapay zeka teknikleri kullanıldı. Bu teknikler, doğrudan ve basit bir şekilde yardım alabilecekleri yerleri belirlerken marjinal grupların haklarını ve kendilerine sunulan destek seçeneklerini bilmelerine katkıda bulunduğu için aile içi şiddete karşı güvenli bir ortam sağlar. Bu teknoloji, sanki karşısında bir insanla veya arkadaşıyla konuşuyormuş gibi tanımlanabilir. Yapay zeka teknikleri, kişilere hizmet eden, sağlıklı karar vermelerine ve birçoğu ölümle sonuçlanan aile içi şiddetten korunmalarına yardımcı olan eksiksiz ve mükemmel bir elektronik ortam sağlar. Yani sosyal hizmette önemli bir role sahiptir. Kısacası yapay zeka, dünyayı afetlerden kurtarmaya, çocukların ihtiyaçlarını karşılamaya, mülteci ve yurdundan edilen kişileri korumaya ve insan haklarını destekleme yeteneğine sahip olmaya çalışmaktadır [29][30].

Yapay zeka, birçok ülkede hükümetlerin COVID-19 pandemisinin yayılımının azaltmasına yardımcı oldu; Örneğin Güney Kore, ülkedeki sağlık durumunu kontrol etmek, enfekte olmuş kişileri izlemek ve virüsün nereye yayıldığını bilmek için yapay zeka tekniklerine başvurmuş [31][32], enfekte olmuş kişilerin arttığı bölgelerin sağlık yetkililerine bildirilmesi ve nerede bulunduklarının belirlenmesi için makine öğrenmesi temelli uygulamalar geliştirmiştir. Ayrıca radarlar aracılığıyla yol boyunca insan ve araç akışının izlenmesine yardımcı olmak için modern araçlardan yararlanılmış ve bu da gerekli tıbbi önlemlerin alınmasına katkıda bulunmuştur. İş dünyasına gelince, yapay zeka 2019 yılından bu yana dünyanın içinden geçtiği zorlu ekonomik şartların gölgesinde operasyonel verimliliği sürdürmek için şirket ve kuruluşlara ticari avantajlar sağladı [33]. Yapay zekanın COVID-19 ile mücadelede kullanılması birçok soruyu gündeme getirdi, mahremiyet ve kişisel özgürlük ihlalleri oluşturmayacak şekilde kullanımını sağlaya küresel protokollerin olmaması ve düzenlemeye yönelik belirli standartların veya kuralların yokluğunda verilerin kullanılması gibi [34]. Doğru kullanıldığında yapay zeka, kaçınılmaz bir şekilde değerli olacak ve birçok alanda hükümetleri destekleyecektir, fakat yanlış kullanılması durumunda sonuçları felaket olabilir.

Pandemi salgınından bu yana dünya çapında kamu ve özel sektör, yapay zekayı COVID-19 virüsüyle mücadele için yeterli araçlardan biri olarak kullandı. Sağlık sektöründe yapay zeka, sağlık çalışanları ve doktorlar tarafından göğüs röntgeni ile hastaların teşhis edilmesinde, pratik aşıların geliştirilmesinde kullanılmaktadır [35]. Çoğu hükümet fiziksel mesafe önlemlerini aldı ve vatandaşlarından mümkün olduğunca evde kalmalarını ve sadece gerçekten gerekli olduğunda dışarı çıkmalarını istedi. Ayrıca hükümetler, vatandaşlarını ihtiyaçlarını giderebilmeleri için yapay zeka destekli mobil uygulamaları kullanmaya zorladı. Ayrıca o dönemde yapay zeka, ulusların işgücünün ekonomik faaliyetini ve üretkenliğini sürdürürken aynı zamanda yeterli düzeyde sağlık, eğitim ve yaşam yolunun korunmasına yardımcı olan diğer hizmetleri sağlamayı başardı. COVID-19

pandemisi deneyimi, robotların bu pandemi krizi gibi insanlar için güvenli olmadığı düşünülen durumlarda krizlerle başa çıkabilmek için gerekli görevleri yerine getirebilme yeteneğine sahip olduğunu kanıtlamıştır. Bu robotlar, sokaklarda dolaşırken insanları virüse maruz kalmaktan başarıyla korudu [36], dünya çapında birçok şehre bölge sakinlerini fiziksel mesafeyi korumaya ve güvenlik önlemlerini almaya çağırdı. Başka bir deyişle, pandemi ile mücadelede yapay zekanın fiilen kullanıldığı birçok alan vardır ve şu üç uygulamayı içermektedir:

- Sağlık kaynakları yönetimi,
- Hizmet ve araştırma yönetimi,
- İlaç ve aşıların geliştirilmesi.

Enfekte olan veya hastalık belirtileri gösteren kişileri uzaktan veya başka bir şekilde belirlemek için yapay zeka kullanılabilir. Neyse ki yapay zeka, sağlık çalışanları için her hastanın durumu hakkında tam raporlar vermeleri adına güvenli bir ortam sağladı. Ek olarak veri bilimi ve yapay zeka sistemleri, hastaları tanımlayıp teşhis ederek ve ayrıca hasta bilgilerini otomatik olarak güncelleyerek sağlık yönetimini ilerletmek için kullanılabilir. Ayrıca biyoinformatikte yapay zekanın kullanılması birkaç ay boyunca aşı ve ilaç geliştirmek üzere yapılan deneyler için gereken süreyi kısaltır.

5 Siber Güvenlikte Yapay Zeka

Yapay zeka, teknoloji dünyasındaki herkesin geleceği olduğu için geniş bir deneyci ve destekçi kitlesi için giderek yaygınlaşan bir kavram haline geliyor. Aslında Google ve telefonlarımızdaki uygulamalar, işlerimizi gerçekleştirmek için özellikle yapay zekaya güvendiğinden yapay zeka milyonlarca insan tarafından günlük olarak kullanılmaktadır. Ayrıca yapay zeka, birçok programcıyı, uygulama geliştirme aşamasında yapay zekayı kullanmaya zorlayan özelliklere sahiptir. Sonuç olarak bilgisayar insandan daha hızlı öğrenir. Böylece çözümlere erişmede, belirli bir sorunun çözümünü bulmada insan hızını aşan muazzam bir hıza ulaşabilir. Yapay zeka, siber güvenlik alanında önemli ve etkili bir rol oynamaktadır [37][38]. Bireylerin artık tehditleri kendilerinin tanımlamasına ve savunma mekanizmaları oluşturmasına gerek yoktur. Yapay zeka ile donatılmış bir bilgisayar, tehditleri kötü amaçlı yazılımları ayırt etme ve bunları önleme, bilgisayar sistemine erişmeme ve kullanıcıların verilerini görmeme konusunda çözüm üretme yeteneğine sahiptir. Örneğin siber güvenlikte yapay zekanın uygulandığı ve günümüzde hemen herkesin kişisel cep telefonlarında dahi kullandığı biyometrik kimlik doğrulama uygulamaları geliştirilmektedir. Bu uygulamalar, iris tanıma, parmak izi tanıma veya yüz tanıma gibi farklı özelliklerle kimlik tespiti yapabilmektedir [39]. Bu özelliklerin arka planında konvolüsyonel yapay sinir ağları (CNN) [40], derin öğrenme veya tekrarlanan yapay sinir ağları (RNN) [41] gibi yapay zeka teknikleri kullanılmaktadır. Böylece kişinin gerçek mi yoksa sahte mi olduğuna yapay zeka yöntemi karar vermektedir. Yapay zeka ayrıca kullanılan internet ağı üzerindeki veri alışverişini izleyerek anormal durumları bulanık sinir ağları (FNN) [42], çok varlıklı Bayes Ağları (MEBN) [43] gibi yöntemlerle tespit edebilmektedir [44]. Bunun örneklerinden olan DeepArmour [45], saldırgan ataklara karşı geliştirilmiş bir savunma sistemidir ve olası saldırıları başarılı bir şekilde tespit ettiğini kanıtlamıştır. Siber güvenlikte yapay zekanın kullanılması ile sisteme herhangi bir saldırı olma ihtimalinde bunun önüne geçilebilmesi de sağlanmaktadır. Son yıllarda büyüyen ve siber güvenlikte yapay zeka kullanan birçok girişim (start-up) ortaya çıktı. Şekil 2 Türkiye kaynaklı öne çıkan yerli siber güvenlik girişimleri olan Secpoint, StrixEye, Forestall, Kondukto, Picus, Brandefense ve ATARLabs'ın logolarını göstermektedir. Aslında yapay zeka, siber suçluların sisteme sızmalarına yardımcı olan kötü amaçlı yazılımlar aracılığıyla tehdidi büyümeden önce bile tahmin edebilir. Ancak yapay zekada da bir tehdit var, çünkü suçluların da saldırı için güçlü yapay zeka kullanması mantıksız değildir. Bir yanda virüs tarayıcıları, güvenlik duvarları ve siber güvenlik kalkanları ile diğer yanda siber suçlular arasındaki savaş, gerçek bir kedi-fare oyunudur. Güvenlik, suç tarafındaki gelişmeleri takip eder: bu, sürekli tekrarlanan bir eylemdir. Siber güvenlik görevlileri risklerin nerede olduğunu tahmin etmeye ve bunlara karşılık vermeye çalışsa da, virüslerdeki, zararlı kod yerleştirmelerindeki ve benzeri tehditlerdeki artışlara cevap vermek gibi daha çok kavram vardır. Yapay zeka, ciddi bir yol oluşturduğunda bile bunu yapmaya devam edebilecek güzel fırsatı var. Oyun tamamen aynı kalabilir ancak inanılmaz derecede zeki iki bilgisayar, daha yüksek bir seviyede birbirini alt etmeye çalışır: biri savunma yaparken, diğeri saldırmaktadır. Yapay zeka da bazen kendi başına bir tehdit olarak görülüyor. Çünkü aynı zamanda kötüye kullanılabiliyor ve hatta kendi iradesini

geliştirebiliyor. Şu anda yapay zeka en basit haliyle geleceğin melodisidir.

Şekil 2. Türk siber güvenlik teknolojisi girişimleri

Birçok ülke sistemlerini korumak ve elektronik saldırılara karşı yenilikçi ve etkili savunma mekanizmaları oluşturmak için sistemlere, mevzuata ve teknolojik yatırım yapmaya çalıştığından yapay zeka teknolojisinin oluşturduğu siber tehditlerin artmasıyla siber güvenlik alanı, hükümetler için bir öncelik haline geldi. Ne yazık ki yapay zeka teknikleri hemen hızlı çalışmıyor. Çünkü daha fazla veri bu tekniklerin gelişmesini sağladığından öğrenmede ve eğitim üzerinden geliştirilmeleri gerekir. Genellikle bu zaman alır, bu teknikler bazı geliştiricileri ve ağları bozmaya çalışan yanlış pozitif (false positive) değerlere yol açar. Bulut ortamlarını korumak için yapay zeka teknikleri de giderek daha fazla kullanılmaktadır [46]. Siber güvenlik ekipleri, müşteri verilerini uygun şekilde oluştururken ve korurken bulut ortamlarını güvenli hale getirmek için bu teknikleri uygulamak ve öğrenmek için çaba sarf etmek zorundadır. Şu anda birincil görev, güvenli olması ve müşteriler arasında yetkisiz kişilerin girişine gerek kalmadan veri aktarımı yapabilmesi gereken bulut güvenlik platformları ve makine öğrenmesi araçlarının geliştirilmesi, her türlü saldırı, bilgisayar korsanlığı, veri hırsızlığı ve aldatma yöntemlerinin tahmin edilebilmesidir. Buna göre yapay zeka tekniklerine olan ilgi, sistemlerin kalıcılığını arttırmakta ve tahminlerin siber güvenlik alanına entegre edilmesi gerekmektedir. Ayrıca kullanıcı verileri değiştirilirken veya silinirken kanun dışı olan her şeyin tahminini sağlamak için bu teknikler profesyonel olarak öğretilmelidir. Siber güvenlik uzmanları, sistemlere giren yetkisiz kişileri tespit edebilmek için tüm trafik verilerini yoğun bir şekilde toplamaya ve bu veriler üzerinde makine öğrenmesi yöntemlerini eğitmeye çalışır. Yapay zekanın siber güvenlik alanında kullanılması, uzmanların doğru zamanda daha doğru kararları vermelerine yardımcı olacaktır. Bu nedenle önümüzdeki yıllarda siber güvenlik alanında makine öğrenmesi temelli çözümlerin artacağını ön görmekteyiz.

6 Sonuçlar

Yapay zeka siber güvenlikte özellikle anormal durumların tespiti ve kullanıcı verilerinin gizliliği konusunda tartışılmaktadır. Saldırı tespitinde anormal durumların ve ağ trafik akışının yapay zeka ile kontrol edilmesi kullanıcılara ciddi avantajlar getirmektedir. Bu sayede sıradan bir kullanıcının haberi bile olmadan sistemine yapılan saldırılar, yapak zeka temelli uygulamalar ile önlenebilmektedir. Öte yandan kimlik doğrulama kısmında da yapay zeka, kullanıcılara büyük kolaylıklar sağlamaktadır. Bir kullanıcının her oturum için farklı şifre kullandığını düşünürsek onlarca şifreyi aklında tutması gereklidir. Ama biyometrik kimlik doğrulama yöntemleri ile şifreye gerek kalmadan sisteme giriş yapılabilmektedir. Ancak farklı bir açıdan baktığımızda ise yapay zeka aracılığı ile bir insanın yüzünün veya sesinin de kopyalanması mümkün kılındığı için büyük bir risk de gündeme gelmektedir. Araştırmacılar arasında yapay zekanın bugün ve gelecekte insanlık için yararlı mı yoksa zararlı mı olduğu konusunda ihtilaftadırlar. Siber güvenlikte yapay zeka tekniklerini kullanan ve büyüyen girişimlerin sayısı arttıkça yapay zekanın siber güvenlikte uygulanmasının potansiyel etkileri konusunda şüpheler ortaya çıkmaktadır. Yapay zeka teknikleri, kimlik doğrulama çerçevesini gerçek zamanlı olarak daha etkili hale getirilebilir ve erişim ayrıcalıkları, kullanıcının ağına ve konumuna göre değişebilir. Yapay zeka tekniklerinin nasıl çalıştığına dair yeterli bilgi ve deneyime sahip siber güvenlik şirketleri tarafından yürütülmelidir. Gelecekte, siber güvenlik verilerinde makine öğrenmesi tekniklerinin kullanımına yönelik araştırmalar ve bu tekniklerin karşılaştırılmaları ile ilgili çalışmalar hız kazanacaktır.

Kaynaklar

[1] David L. O., Nwulu N. I., Aigbavboa C. O., and depoju O. O., “Integrating fourth industrial revolution (4IR) technologies into the water,

energy & food nexus for sustainable security: A bibliometric analysis," Journal of Cleaner Production, vol63, pp:132522, August 2022. https://doi.org/10.1016/j.jclepro.2022.132522

[2] Ebekozien A. and Aigbavboa C., "COVID-19 recovery for the Nigerian construction sites: The role of the fourth industrial revolution technologies," Sustainable Cities and Society, vol.69, pp:102803, June 2021. https://doi.org/10.1016/j.scs.2021.102803

[3] Perwej Y., Abbas S. Q., Dixit J. P., Akhtar N., and Jaiswal A. K., "A Systematic Literature Review on the Cyber Security," International Journal of scientific research and management, vol. 9, no.12, pp:669-710, 2021. https://doi.org/10.18535/ijsrm/v9i12.ec04

[4] Alawida M., Omolara A. E., Abiodun O. I., and Al-Rajab M., "A deeper look into cybersecurity issues in the wake of Covid-19: A survey," Journal of King Saud University - Computer and Information Sciences, In press, August 2022. https://doi.org/10.1016/j.jksuci.2022.08.003

[5] Kuzlu M., Fair C., and Guler O., "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," Discover Internet of Things", vol. 1, no. 7, pp:1-14, February 2021. https://doi.org/10.1007/s43926-020-00001-4

[6] Aggarwal K., Mijwil M. M., Sonia, Al-Mistarehi AH., Alomari S., Gök M., Alaabdin, A. M., and Abdulrhman S. H., "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," Iraqi Journal for Computer Science and Mathematics, vol.3, no.1, pp:115-123, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[7] Tsaramirsis G., Kantaros A., Al-Darraji I., Piromalis D., Apostolopoulos C., et al., "A Modern Approach towards an Industry 4.0 Model: From Driving Technologies to Management," Journal of Sensors, vol.2022, no.5023011, pp:1-18, June 2022. https://doi.org/10.1155/2022/5023011

[8] Saura J. R., Ribeiro-Soriano D., and Palacios-Marqués D., "Setting B2B digital marketing in artificial intelligence-based CRMs: A review and directions for future research," Industrial Marketing Management, vol.98, pp: 161-178, October 2021. https://doi.org/10.1016/j.indmarman.2021.08.006

[9] Mijwil M. M., Aggarwal K., Doshi R., Hiran K. K., and Gök M., "The Distinction between R-CNN and Fast R-CNN in Image Analysis: A Performance Comparisont," Asian Journal of Applied Sciences, vol.10, no.5, pp:429-437, Novmber 2022. https://doi.org/10.24203/ajas.v10i5.7064

[10] Rammo F. M. and Al-Hamdani M. N., "Detecting The Speaker Language Using CNN Deep Learning Algorithm," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, pp: 43–52, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.005

[11] Murad N. M., Rejeb L., and Said L. B., "The Use of DCNN for Road Path Detection and Segmentation," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp: 119-127, June 2022. https://doi.org/10.52866/ijcsm.2022.02.01.013

[12] Korteling J. E., Boer-Visschedijk G. C. V., Blankendaal R. A. M., Boonekamp R. C., and Eikelboom A. R., "Human- versus Artificial Intelligence," Frontiers in Artificial Intelligence, vol.4, no.622364, pp:1-13, March 2021. https://doi.org/10.3389/frai.2021.622364

[13] Zhang Y., Geng P., Sivaparthipan C. B., and Muthu B. A.,"Big data and artificial intelligence based early risk warning system of fire hazard for smart cities," Sustainable Energy Technologies and Assessments, vol.45, pp:100986, June 2021. https://doi.org/10.1016/j.seta.2020.100986

[14] Qamar R., Bajao N., Suwarno I., and Jokhio F. A., "Survey on Generative Adversarial Behavior in Artificial Neural Tasks," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 2, pp: 83–94, March 2022. https://doi.org/10.52866/ijcsm.2022.02.01.009

[15] Mijwil, M. M., and Shukur B. S., "A Scoping Review of Machine Learning Techniques and Their Utilisation in Predicting Heart Diseases," Ibn AL-Haitham Journal For Pure and Applied Sciences, vol. 35, no.3, pp: 175-189, July 2022. https://doi.org/10.30526/35.3.2813

[16] Li Y., Xia J., Zhang S., Yan J., Ai X., and Dai K., "An efficient intrusion detection system based on support vector machines and gradually feature removal method," Expert Systems with Applications, vol.39, no.1, pp:424-430, January 2012. https://doi.org/10.1016/j.eswa.2011.07.032

[17] Meskó, B., Hetényi, G. & Győrffy, Z. Will artificial intelligence solve the human resource crisis in healthcare?. BMC Health Serv Res 18, 545 (2018). https://doi.org/10.1186/s12913-018-3359-4

[18] Blog website, The significant difference between AI, ML and Deep Learning, USoft, https://www.usoft.com/blog/difference-between-ai-ml-and-deep-learning

[19] Ramadan R. A., Aboshosha B. W., Alshudukhi J. S., Alzahrani A. J., El-Sayed A., and Dessouky M. M., "Cybersecurity and Countermeasures at the Time of Pandemic," Journal of Advanced Transportation, vol.2021, no.6627264, pp:1-19,

February 2021. https://doi.org/10.1155/2021/6627264
[20] Adamu U. and Awan I., "Ransomware Prediction Using Supervised Learning Algorithms," In Proceedings of International Conference on Future Internet of Things and Cloud, 26-28 August 2019, pp:1-6, Istanbul, Turkey. https://doi.org/10.1109/FiCloud.2019.00016
[21] Ahsan M., Nygard K. E., Gomes R., Chowdhury M., Rifat N., and Connolly J. F., "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review," Journal of Cybersecurity and Privacy, vol.2, no.3, pp:1-29, July 2022. https://doi.org/10.3390/jcp2030027
[22] Eghtesadi M. and Florea A., "Facebook, Instagram, Reddit and TikTok: a proposal for health authorities to integrate popular social media platforms in contingency planning amid a global pandemic outbreak," Canadian Journal of Public Health, vol. 111, pp:389-391, June 2020. https://doi.org/10.17269/s41997-020-00343-0
[23] Bohr, A., and Memarzadeh, K., "The rise of artificial intelligence in healthcare applications". In Artificial Intelligence in healthcare, pp: 25-60. Academic Press, 2020. https://doi.org/10.1016/B978-0-12-818438-7.00002-2
[24] Jordan Novet, 2017, Microsoft has a new app that tells the visually impaired what's in front of them. CNBC [online]. 18 July 2017. [Accessed;13 December 2022]. Available from: https://www.cnbc.com/2017/07/12/microsoft-launches-seeing-ai-app-for-ios.html
[25] Mijwil, M. M. and Al-Zubaidi, E. A., "Medical Image Classification for Coronavirus Disease (COVID-19) Using Convolutional Neural Networks," Iraqi Journal of Science, vol.62, no.8, pp: 2740-2747, August 2021. https://doi.org/10.24996/ijs.2021.62.8.27
[26] Mijwil, M. M., "Implementation of Machine Learning Techniques for the Classification of Lung X-Ray Images Used to Detect COVID-19 in Humans," Iraqi Journal of Science, vol.62, no.6., pp: 2099-2109, July 2021. https://doi.org/10.24996/ijs.2021.62.6.35
[27] Mijwil M. M., Aggarwal K., Doshi R., Hiran K. K., Sundaravadivazhagan B. "Deep Learning Techniques for COVID-19 Detection Based on Chest X-ray and CT-scan Images: A Short Review and Future Perspective," Asian Journal of Applied Sciences, vol.10, no.3, pp:224-231, July 2022. https://doi.org/10.24203/ajas.v10i3.6998
[28] Nasare, R., Shende, A., Aparajit, R., Kadukar, S., Khachane, P., & Gaurkar, M. "Women Security Safety System using Artificial Intelligence", International Journal for Research in Applied Science & Engineering Technology, vol. 8, February 2020, http://doi.org/10.22214/ijraset.2020.2088
[29] Dwivedi Y. K., Hughes D. L., Coombs C., Constantiou I., Duan Y., et al., "Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life," International Journal of Information Management, vol.55, pp:102211, December 2020. https://doi.org/10.1016/j.ijinfomgt.2020.102211
[30] Ahmed S., Abbood Z. A., Farhan H. M., Yasen B. T., Ahmed M. R., Duru A. D., "Speaker Identification Model Based on Deep Neural Networks," Iraqi Journal For Computer Science and Mathematics, vol. 3, no. 1, p:108–114, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.012
[31] Mijwil, M. M., Al-Mistarehi, AH., and Aggarwal K., "The Effectiveness of Utilising Modern Artificial Intelligence Techniques and Initiatives to Combat COVID-19 in South Korea: A Narrative Review," Asian Journal of Applied Sciences, vol.9, no.5, pp:343-352, November 2021. https://doi.org/10.24203/ajas.v9i5.6753
[32] Palaniappan A., Dave U., and Gosine B., "Comparing South Korea and Italy's healthcare systems and initiatives to combat COVID-19," Revista Panamericana de Salud Pública, vol.44, pp:1-5, April 2020. https://doi.org/10.26633/RPSP.2020.53
[33] Pal, R. "Applications Of Artificial Intelligence in Company Management, E-Commerce, And Finance: A Review", International Journal of Multidisciplinary Educational Research, vol.11, February: 2022. http://ijmer.in.doi./2022/11.02.39
[34] Mijwil, M. M., Abttan R. A., and Alkhazraji A., "Artificial intelligence for COVID-19: A Short Article," Asian Journal of Pharmacy, Nursing and Medical Sciences, vol.10, no.1, pp:1-6, May 2022. https://doi.org/10.24203/ajpnms.v10i1.6961
[35] Ilyas, M., Rehman, H., & Naït-Ali, A., "Detection of covid-19 from chest x-ray images using artificial intelligence: An early review", arXiv preprint arXiv:2004.05436, 2020.
[36] Yi, J., Zhang, H., Mao, J., Chen, Y., Zhong, H., & Wang, Y., "Review on the COVID-19 pandemic prevention and control system based on AI", Engineering Applications of Artificial Intelligence, 105184, 2022. https://doi.org/10.1016/j.engappai.2022.105184
[37] Abbas N. N., Ahmed T., Shah S. H. U., Omar M., and Park H. W., "Investigating the applications of artificial intelligence in cyber security,"

Scientometrics, vol. 121, pp:1189–1211, September 2019. https://doi.org/10.1007/s11192-019-03222-9

[38] Chandrasekhar A. M. and Raghuveer K., "Confederation of FCM clustering, ANN and SVM techniques to implement hybrid NIDS using corrected KDD cup 99 dataset," In Proceedings of International Conference on Communication and Signal Processing, 03-05 April 2014, pp:1-6, Melmaruvathur, India. https://doi.org/10.1109/ICCSP.2014.6949927

[39] Sudiro, Sunny Arief, and Saepul Lukman. "Minutiae matching algorithm using artificial neural network for fingerprint recognition." 2015 3rd international conference on artificial intelligence, modelling and simulation (AIMS). IEEE, 2015.

[40] Ding, Changxing, and Dacheng Tao. "Trunk-branch ensemble convolutional neural networks for video-based face recognition." IEEE transactions on pattern analysis and machine intelligence 40.4 (2017): 1002-1014.

[41] Amberkar, Aditya, et al. "Speech recognition using recurrent neural networks." 2018 international conference on current trends towards converging technologies (ICCTCT). IEEE, 2018.

[42] Li, Cheng, and Xing Ming Li. "Cyber performance situation awareness on fuzzy correlation analysis." 2017 3rd IEEE international conference on computer and communications (ICCC). IEEE, 2017.

[43] Park, Cheol Young, et al. "A process for human-aided multi-entity bayesian networks learning in predictive situation awareness." 2016 19th international conference on information fusion (FUSION). IEEE, 2016.

[44] Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." Journal of Network and Computer Applications 60 (2016): 19-31.

[45] Ji, Yuede, Benjamin Bowman, and H. Howie Huang. "Securing malware cognitive systems against adversarial attacks." 2019 IEEE international conference on cognitive computing (ICCC). IEEE, 2019.

[46] Girish, L., and Sridhar KN Rao. "Anomaly detection in cloud environment using artificial intelligence techniques." Computing (2021): 1-14. https://doi.org/10.1007/s00607-021-00941-x