Yapay Zeka Odaklı Siber Risk ve Güvenlik Yönetimi

***

Artificial Intelligence Focused Cyber Risk and Security Management

DOI:10.33461/uybisbbd.972206

Ahmet EFE[1]

Öz

Makale Bilgileri

Makale Türü: Derleme Makalesi

Geliş Tarihi: 16.07.2021

Kabul Tarihi: 05.09.2021

Yapay zekayı (YZ) ve makine öğrenimini siber güvenlik için silahlandırmak hala erken aşamalarda olsa da büyük ölçekli firmalar ve kuruluşlar, güvenlik sistemlerini ve uygulamalarını korumak için YZ ve makine öğrenimini içeren özerk savunma yeteneklerini geliştirmeye çalışmaktadırlar. Bunun yanı sıra, siber saldırganlar da yetenek ve araçlarını sürekli geliştirirken yeni güvenlik açıklarını ortaya çıkarmak ve yasa dışı amaçlarına ulaşmak için sağladığı avantajlardan dolayı otonom YZ algoritmalarını kullanmaya başlamışlardır. Bu nedenle kendi kendisine öğrenen, zafiyetleri otomatik olarak tarayarak hangi tekniklerle suiistimal yapılmasının ve güvenlik duvarlarının etkisiz hale getirilebileceğinin nasıl olanaklı olduğunu raporlayan ve/veya doğrudan saldırıya geçebilen otonom saldırı araçları büyük bir risk olarak çok sofistike hale gelmiştir. Buna karşın dinamik BT ortamındaki riskleri ve kontrol zafiyetlerini otomatik olarak algılayarak ve bunların olasılık ve etki derecelerini raporlayarak risk yönetiminin de daha etkili olarak güvenlik ve savunma hizmetine destek sağlamasında da YZ kritik roller oynayabilmektedir. Dolayısıyla YZ ile risk yönetimi daha etkin hale gelebilirken YZ üzerinden maruz kalınan riskler de daha sofistike hale gelmiştir. Bu çalışma, YZ' nin siber suç ve siber güvenlikteki rolünü, bu alandaki risklerin YZ üzerinden yönetilebilirliğini literatür ve sektörel raporların incelenmesi yoluyla araştırmaktadır. Çalışmada, YZ tabanlı risk ve tehditlerin ne kadar ciddi olduğu yanı sıra, bir kuruluşun YZ destekli gelişmiş kalıcı tehditlere (APT) karşı güvenlik duruşunu ve risk iştahını iyileştirmeye nasıl yardımcı olunabileceği teknik olarak ortaya konulmaktadır.

Anahtar kelimeler: *yapay zekâ, risk yönetimi, BT riskleri, risk otomasyonu, akıllı YBS.*

Abstract

Article Info

Paper Type: Review Paper

Received: 16.07.2021

Accepted: 05.09.2021

While arming AI and machine learning for cybersecurity is still in its early stages, large-scale firms and organizations continuously develop autonomous defense capabilities that include AI and machine learning to protect their security systems and applications. In addition, intelligent cyber attackers have started to use independent AI algorithms, continuously developing their capabilities due to the advantages of automatically uncovering new security vulnerabilities for achieving their illegal goals. For this reason, attack tools that learn by themselves, automatically scan vulnerabilities, discover proper techniques to exploit and disable firewalls and attack directly have become very sophisticated. On the other hand, AI can play a critical role in risk management and providing more effective and agile service by automatically detecting risks and control vulnerabilities in the dynamic IT environment and reporting their probability and impact degrees. Therefore, while risk management can become more effective with AI, the risks exposed through AI have also become more sophisticated. This study investigates from literature and sectoral reports the role of AI in cybercrime and cybersecurity and the manageability of risks in the cyber area through AI algorithms. The study explores how serious the AI-based dangers and threats are and how they can help improve an organization's security posture and risk appetite against AI-powered advanced persistent threats (APT).

Keywords*: artificial intelligence, risk management, IT risks, risk automation, smart MIS.*

Atıf/ to Cite (APA): Efe, A. (2021). Yapay Zeka Odaklı Siber Risk ve Güvenlik Yönetimi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 5(2), 144-165

[1] Dr. CISA, CRISC, PMP, COBIT-F, İç Denetçi, Ankara Kalkınma Ajansı, aefe@ankaraka.org.tr

1. GİRİŞ

Yapay zekâ (YZ), düşünme, öğrenme ve tahmin etme gibi sadece insan süreçleri olarak kabul edilen sınırları genişleten ve bunları ağa bağlı makinelere yerleştiren "*bilişsel yenilikçi bir teknoloji*" olarak belirginleşmektedir. YZ, günümüz toplumunun giderek daha büyük bir parçası haline gelmektedir. Mevcut YZ teknolojisi Yapay Dar Zekâ (ANI) olarak sınıflandırılabilir ve tek bir görevi etkin bir şekilde gerçekleştirebilir. Bununla birlikte, ANI, insan zekasını aşabileceği önerilen teorik Yapay Genel Zekâ ile karşılaştırıldığında nispeten zayıf kalmaktadır. YZ teknikleri, finansal risk yönetimine ve siber risk değerlendirmelerine yaklaşımları dönüştürmektedir. Riski anlamak ve kontrol etmekle ilgili bir bankanın bir müşteriye ne kadar borç vermesi gerektiğine karar vermekten, finansal piyasa tüccarlarına pozisyon riski hakkında uyarı sinyalleri sağlamaya, dolandırıcılık ve uyumluluğun iyileştirilmesi ve model riskinin azaltılmasından müşteriyi ve içeriden bilgileri tespit etmeye kadar pek çok konu ve kritik karar süreçleri, YZ güdümlü çözümlerin gelişmesiyle birlikte daha etkin ve verimli hale gelebileceği gibi bir takım ciddi riskleri de bünyesinde barındıracaktır.

Siber güvenlik, bilgisayar sistemlerini kötü niyetli saldırılara ve bilgisayar korsanlarının istismarlarına karşı korumaya adanmış bir bilgisayar bilimi dalı olarak bilinmektedir. Türkiye'nin "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" içerisinde siber güvenlik kavramı için yapılan tanımlamaya göre ise, "bilişim sistemlerinin birleşerek oluşturduğu ve siber ortam olarak kavramsallaşan ortamı, saldırıları tespit etmek suretiyle kayıplardan korumaya, saldırının tespiti halinde gerekli teknik desteği devreye sokmaya ve saldırı öncesi konuma geri döndürmeye odaklı stratejiler bütününe verilen addır" (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013-2014: 9' dan aktaran: Aldemir, 2020).

YZ, siber güvenlik kapsamında sistemlere izinsiz ve kötü niyetli girişleri tespit etmek için bir ağdaki anormal olayları izlemek için uygulanmakta olan bu alanda zaten çok önemli bir rol oynamaktadır. YZ'nin algoritmalarla nasıl çalıştığını, öğrendiğini, barındırdığı ve yönettiği riskleri ve siber güvenlikteki uygulamaları içeren konular bu makalede tartışılmaktadır. Bunun için öncelikle Araştırma problemi, metot ve Literatür taraması yapılarak araştırmanın kapsamı ve motivasyonu ortaya konulmaktadır. Ardından YZ ve makine öğrenimi çağında siber risk konusu ele alınarak siber risklerin YZ ortamında nasıl yönetilebildiği üzerinde değerlendirmeler yapılmaktadır. Daha sonra kötü adamlar ve iyi adamların makine öğreniminden yararlanma şekilleri üzerinde durularak YZ'nin bu anlamdaki yapıcı ve bozucu potansiyel nitelikleri üzerinde durulmaktadır. Ardından risk yönetimi ve siber risk incelenmekte, YZ'yi siber güvenliğe uygulama konusu kapsamında güvenlik risk yönetimi için kompleks ve algoritmik makine öğreniminin sınırları irdelenerek muhtemel çözümler geliştirilmeye çalışılmaktadır.

2. ARAŞTIRMA PROBLEMİ, METOT VE LİTERATÜR TARAMASI

İnsan gibi düşünme ve sanatsal faaliyetler, bu alanda en büyük engel olarak ortaya çıkmıştır. YZ'nin en başarılı çalışma alanlarından birisi uzman sistemlerdir. Çünkü bilgi insandan alınarak doğru bir şekilde kurgulanır ise uzman sistem insanın verdiği gibi kararlar verebilmektedir (Yıldız, 2021). İnsanlar gibi olması için düşünsel ve davranışsal olarak modellemelerin yapılması gerekir. Davranışsal takibi YZ ile gerçekleştirmek, müşteri tabanını daha iyi anlamak isteyen işletmeler veya vatandaşların ihtiyaç, beklenti ve eğilimlerini tespit etmek isteyen kamu kurumları için çok büyük bir yarar sağlayacaktır[1].

Risk yönetiminde YZ, şirket veya kuruluşların mevzuat ve stratejilerle uyumluluğunu sağlamak için düzenleyici değişikliklerle politikaları, prosedürleri ve kontrolleri birleştirmek ve iyileştirmek için de kullanılabilir. Ancak bu tür sistemler, ihtiyaç duyulan zaman ve gerek duyulan şekilde risk

[1] Bu hususta geliştirilmiş örnek bir ürün için bkz: https://luthresearch.com/digital-measurement/technology/zq-intelligence/

yöneticilerine doğru risk verilerini sağlayacak şekilde ayarlanabilmektedir. Ayrıca YZ teknolojisi birçok alan ve sektöre fayda sağlarken, uygulanması bir takım yeni etik zorluklar da meydana getirmiştir. Bu zorluklar arasında, istihdam alanlarında bazı meslek grupları için temel bir tehdit olabileceği gibi, YZ programlarına insan tarafından yerleştirilebilecek yanlılık, kasıtlı/hatalı yanlış algoritmalar, daha gelişmiş ve daha az gelişmiş YZ'nin etik ikilemlere nasıl tepki vereceği ve teknolojiyi siber güvenlik gibi bir alanda uygulamanın olası etik sorunları yer almaktadır. Nöral ağlar ve derin öğrenme teknikleriyle algoritmalarını iyileştirebilecek olan süper YZ bu anlamda çeşitli riskler barındırmaktadır. Bunun dışında, Tesla ve SpaceX CEO'su Elon Musk, iddia ettiği gibi YZ'nin "*insan uygarlığının varlığı için temel bir risk*" olduğu iddia edilmektedir. YZ'nin olumsuz görünen niteliklerini azaltmak ve yönetilebilir hale getirebilmek için daha güçlü düzenleyici gözetim mekanizmaları ile daha sorumlu araştırmalar için yaptığı baskının bir parçası olarak, bir bütün olarak topluma fayda sağlayacak dost YZ'yi teşvik etmeyi ve geliştirmeyi amaçlayan kâr amacı gütmeyen bir YZ araştırma şirketi olan OpenAI'yi kurmuştur (Tung, 2017). Bu kapsamda sorulan önemli sorular şu şekilde belirlenmiştir:

- *YZ yaygınlaşarak demokratikleştirildiğinde hangi riskleri yönetmemiz gerekecek?*
- *Şirketler ve kamu kurumları YZ' yi gerçekte ne için kullanacak?*
- *Risk yöneticileri kendi insan önyargılarını YZ' ye yansıtacak mı?*
- *Böylesine önemli bir teknoloji kurumsal süreçleri ve yetkinlikleri nasıl değiştirebilir?*
- *YZ riskleri nasıl düzenlenmelidir?*

Siber risk analitiğindeki mevcut boşluklar tanımlayıcı, öngörücü ve kuralcı veri analitiği alanındadır (Barker ve diğerleri 2017). YZ algoritmalarının incelenmesi YZ bağlantılı ve oldukça karmaşık BT sistemlerinin mevcut siber risk analitiği için etkisiz kalabilmektedir. Çünkü bunlar yüksek oranlarda yanlış negatifler (tespit edilememe) ve yanlış pozitifler (yanlış uyarılar) sunabilmektedirler (Malhotra 2018).

Bulut seviyesinde dağıtılmış saldırı tespiti, nesnelerin interneti (IoT) için merkezi bir buluttan daha ölçeklenebilir hale gelmiştir (Diro ve Chilamkurti, 2018). Bu, YZ işlemesinin buluttan uca doğru kaydığı ve YZ iş akışının taşındığı ve verilerin cihazla sınırlandırıldığı birleşik öğrenme ve blok zinciri tabanlı dağıtık YZ mimarisini gerektirmektedir (Porambage ve diğerleri 2019). Bu nedenle, hesaplayıcı ve tanımlayıcı, öngörücü ve kuralcı risk analitiği üzerine ortaya çıkan ana soruları ele almak için YZ uygulamalarının mutlaka analiz edilmesi gerekir. Risk analitiğine YZ'yi entegre ederek, bilişsel veri analitiği için yeni bir yaklaşım geliştirilebileceği ve fiziksel, dijital ve sosyal boyutlarında daha güçlü bir sistem esnekliği oluşturulabileceği düşünülmektedir. Bu yaklaşım, sistemlerin uyum sağlamasını ve tehlikeye düştüğünde güvenli ve emniyetli bir şekilde işlemeye devam etmesini sağlamak için, tavizlerin nasıl ve ne zaman gerçekleştiğini anlamaya odaklanmayı gerektirmektedir.

Bu alanda YZ'nin karşılıklı olarak nasıl birbiriyle savaşabildiğini gösterebilmesi açısından bir örnek olarak, İleri Savunma Araştırma Projeleri Ajansı (DARPA), tarafından düzenlenmiş olan dünyanın en büyük hacker sözleşmelerinden biri olan DEFCON 2016'da ilk olarak YZ ile "*Cyber Grand Challenge*" yarışması gösterilebilir. Yedi takım, YZ bilgisayar makinelerinin "Bayrağı Ele Geçir" (CTF)[2] oyununun 96 raundunda bir nevi savaşarak yarışmıştı. Bu tarihi bir yarışmaydı, çünkü makineler ilk kez yarışma sırasında insan müdahalesi olmaksızın birbirlerini ele geçirmeye hazırlanırken aynı zamanda kendilerini diğer makinelerden gelen saldırılara karşı savunmak durumunda bırakılmışlardı. Herhangi bir CTF yarışması gibi, bu makinelere hatalar ve güvenlik açıklarıyla dolu yeni kodlar geliştirerek ve makinelerin yalnızca nasıl yama yapılacağını değil, aynı zamanda diğer sistemlere nasıl saldırılacağını da bulması gerekiyordu. Dünya ilk kez, siber güvenlik alanının yalnızca güvenlik saldırılarını iyileştirmek ve bunlara karşı savunma sağlamak için değil,

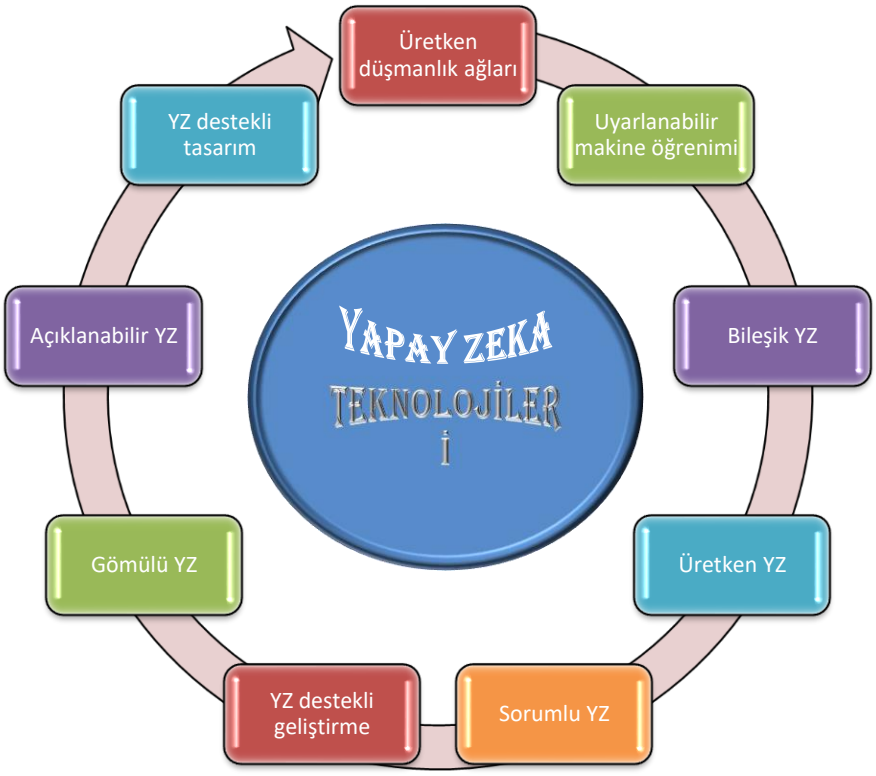
[2] Makinelerin yarışı ile ilgili detaylar için bkz: https://defcon.org/html/defcon-24/dc-24-ctf.html

aynı zamanda kötü bir şekilde kullanıldığında, savunmasız kişilere saldırgan bir şekilde otonom saldırılar gerçekleştirmek için YZ' den nasıl yararlanabileceğine tanık olunmuştu. CTF rekabeti, bilgi işlem gereksinimlerinin ve finansal zorlukların artık otonom güvenlik saldırılarına engel teşkil etmediğini kanıtlamıştır. (Thomson ve Vidas, 2018). Bu durum, kötü niyetli bir tehdit aktörünün, dünya çapındaki şirketlerin ve kamu sektörü kurumlarının siber güvenlik duruşunu tehdit ederek, çok az insan müdahalesi ile saldırılar gerçekleştirebilen sistemler kurmasının mümkün olduğunu da göstermiştir. O zamandan beri siber güvenlik uzmanları, siber suçlarla mücadelede YZ'yi ve makine öğrenimini en iyi şekilde nasıl kullanacaklarını anlamak için çalışmaktadırlar. En az saldırganlar kadar yetkin olmak gerektiği için artık YZ, riske maruz kalmanın belirlenmesinden, ölçülmesine, tahmin edilmesine, etkilerinin değerlendirilmesine ve karşı önlemler alınması aşamalarına kadar risk yönetimi sürecinin çeşitli aşamalarında kurumlara yardımcı olabilmektedir (Sanford ve Moosa 2015).

Bugün çoğu banka ve kredi birliği YZ kullanmaya başlamıştır. Narrative Science ve National Business Research Institute tarafından yürütülen bir ankette, katılan finansal hizmetler yöneticilerinin %32'sinin tahmine dayalı analitik, önemli riskler için otomatik uyarma, öneri motorları, ses tanıma, yardım masası ve yanıt gibi YZ teknolojilerini kullandığı tespit edilmiştir. Bu analize göre YZ, bankalar tarafından tekrarlayan karmaşık süreçlerde ve veri analizinde kullanılmaktadır. Örneğin, JPMorgan Chase teknolojisine yatırım yaparak yakın zamanda "*yasal belgeleri analiz etmek ve önemli veri noktalarını ve kritik bilgileri çıkarmak*" için tasarlanmış bir "Sözleşme İstihbaratı" (COiN) platformunu tanıtmıştır. Bu YZ teknolojisi, binlerce ticari anlaşmanın saniyeler içinde analiz edilmesini sağlamaktadır. Şu anda sektör genelinde benimsenen en görünür YZ biçimi, finansal kurumların ön bürolarında aktif olarak kullanılan sohbet robotlarıdır. Robot teknolojileri ülkemizde üretim tesislerinde montaj gibi tekrarlı işlemlerin yapılmasında yaygın olarak kullanılsa da endüstriyel üretim tesislerinde YZ'ye sahip sosyal asistan robotlar henüz kullanılmamaktadır (Baloğlu ve diğ., 2020).

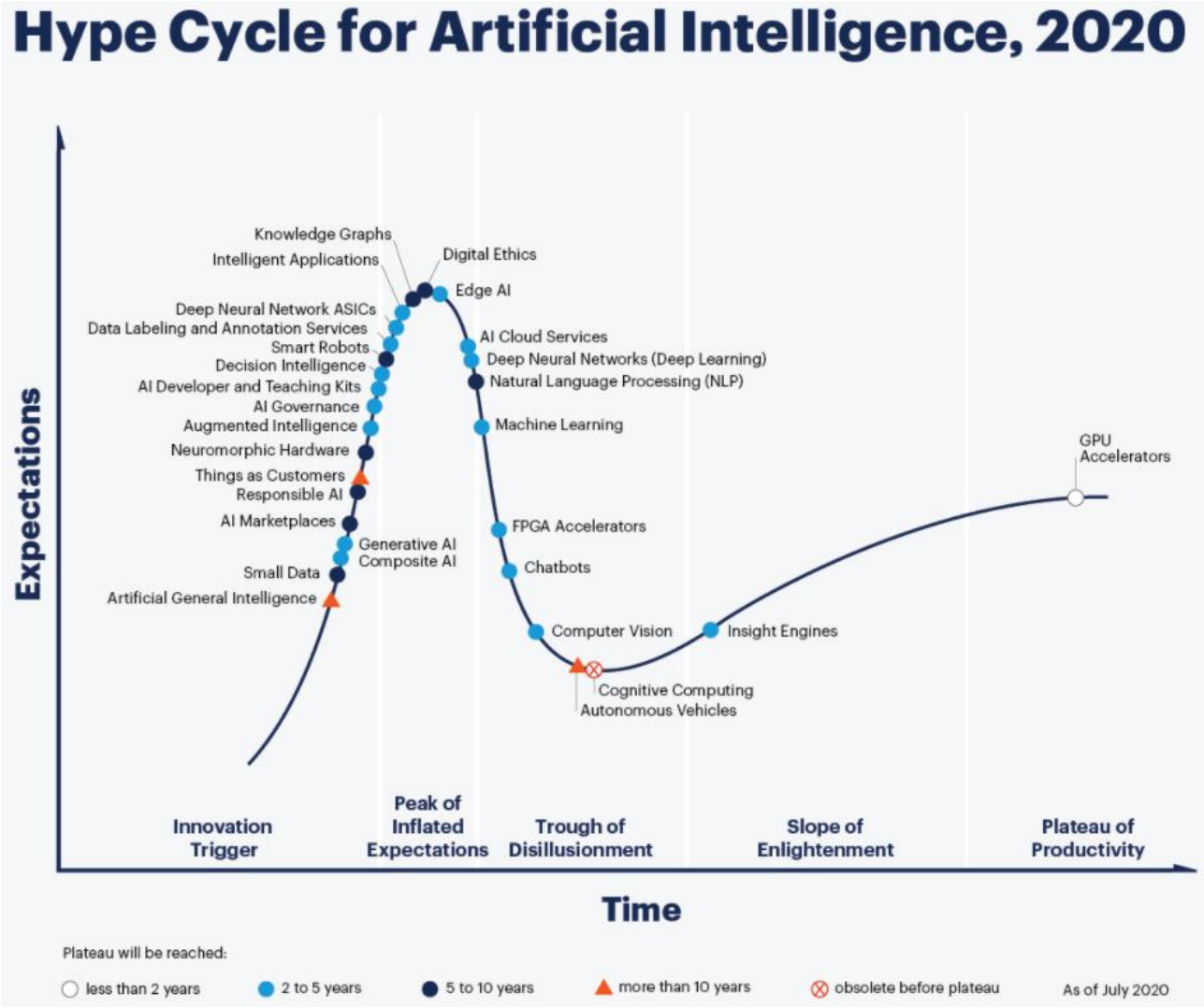
Bank of Amerika, şirketin 45 milyondan fazla müşterisine finansal rehberlik sağlamak için "*tahmin, analitik ve bilişsel mesajlaşma*" kullanan akıllı sanal asistanı için YZ teknolojisini benimsemiştir. YZ'nin bankacılıktaki bir başka uygulaması da dolandırıcılık tespiti ve ortadan kaldırılmasıdır (Archer, 2021a). Başka bir örnek olarak CitiBank, hizmetlerini geliştirmek ve ön planda kalmak için teknoloji şirketleriyle ortaklık kurmaktadır. Stratejik yatırımlarından biri, çevrimiçi ve yüz yüze bankacılık da dahil olmak üzere ticaretin tüm yollarında *"büyük verileri*" ve potansiyel olarak dolandırıcılık faaliyetlerini değerlendirmek için "*makine tabanlı öğrenmeyi"* kullanan lider bir küresel veri bilimi kuruluşu olan Feedzai'dir. Bununla birlikte, tahminler, sahtekarlık saldırıları nedeniyle tüccarların ortalama kaybının yıllık gelirlerinin %1,5'i olduğunu gösterdiğinden, muhtemelen YZ'nin finansal hizmetler sektöründeki en önemli uygulaması risk yönetimidir (Archer, 2021b).

YZ uygun bir risk azaltma stratejisinin seçilmesine ve risk değişimini veya transferini kolaylaştırabilecek araçları bulmaya da yardımcı olabilmektedir. Bu nedenle, kredi kartı sahtekarlıkları gibi harici kayıpları önlemeye çalışmakla başlayan operasyonel risk yönetimi için YZ tekniklerinin kullanımı, artık kapsamlı veri yığınlarının analizi ve tekrarlayan süreçlerin performansının yanı sıra büyük veri kümelerinin derin incelenmesini gerektiren kara para aklamanın tespiti gibi yeni alanlara doğru bir genişleme göstermektedir. En son Gartner'ın Hype Cycle 2020'de yer alan 30 yeni teknolojiden dokuzunun, YZ ile önemli ölçüde ilgili olduğu tespit edilmiştir. Dolayısıyla YZ algoritmalarının gelişmesi ve uygulamalarda olumlu sonuç verdiğinin görülmesiyle birlikte farklı alanlara sürekli genişleme gösterdiği söylenebilir. Bu da YZ'nin risk yönetimine yardımcı olmasının yanı sıra YZ uygulamalarından kaynaklanan çeşitli risklerin de dikkate alınmasını gerekli kılmaktadır.



Şekil 1. Bilinen YZ alt teknolojileri

Şekil 1.'den de anlaşıldığı üzere, YZ ile ilgili çok hızlı gelişen ve giderek kompleks hale gelen bir kavram seti mevcuttur. Bunlar üzerinde literatürde pek çok çalışma olup, bunların nasıl anlaşılması gerektiği, riskleri ve yeni yorumları üzerinde sürekli tartışmalar yapılmakta ve öneriler geliştirilmektedir. Tabi bu kavramsallaştırma çalışmaları farklı alanlarla ilişkili bir şekilde Şekil 2'den de anlaşıldığı üzere bazen disiplinler arası boyutta artmakta bazen de farklı kavram ve yeni paradigmalara yerlerini bırakmaktadırlar. Gartner Hype Cycle önümüzdeki on yılı kapsamaktadır. Ancak teknolojiler trendleri inişteyken ilerledikten sonra neyin gerçekçi ve yaygın olarak benimsendiği görülecektir. Grafikte YZ bileşenleri ile ilgili beklentilerin trend olarak zamanla nasıl yükselip indiğini göstermektedir.



Şekil 2. YZ ile ilgili alt teknoloji alanlarının zamanla beklentilere göre iniş çıkışları

Kaynak: (Goasduff, 2020)'den alınmıştır.

Konuyla ilgili daha güçlü, dönüştürücü ve etkili bir anlayış oluşturmak için gereken YZ gerçek zamanlı ve hızlı veri analitiği yoluyla üstünlüğü sağlama konusuna odaklanmak gerekir. Literatürde YZ ile ilgili kavramsal ve teknik risklerle birlikte teknik ve modellemeler de yoğun bir şekilde işlenmiştir. Doğal dil işleme, doğal dilde oluşturulmuş metinler üzerinde otomatik olarak gerçekleştirilen metin ayrıştırma, metin sınıflandırma, bilgi çıkarımı, duygu analizi gibi birçok önemli konuyu bünyesinde barındırmaktadır ve uygulama alanları da gün geçtikçe artmaktadır (Küçük ve Arıcı, 2018). Mevcut Saldırı Tespit Sistemlerinin (IDS) çoğunluğu YZ algoritmalarına dayanmakta ve bu kapsamda CNN (Convolutional Neural Network) + LSTM (Long Short Term Memory), diğer Derin Öğrenme (ML'nin alt kümeleri) modellerinden daha iyi performans göstermektedir (Roopak ve diğ., 2019). Derin Sinir Ağı (DNN), ağ tabanlı ve ana bilgisayar tabanlı saldırı tespit sistemlerini (NBID ve HBID) toplamak için dağıtılmış derin öğrenme ile uygulanabilmektedir (Vinayakumar ve diğerleri 2019). Yazılım Tanımlı Ağ Teknolojileri (SDN), Makine Öğrenimi (ML) ve derin öğrenme (DL) ile entegre edildiğinde ağ güvenliğini tespit ve izlemede etkili olabilmektedir (Sultana ve diğerleri 2019). SDN ve Ağ İşlevlerini Sanallaştırma (NFV) ile ilgili ana risk endişesi, tek bir hata noktası oluşturan merkezileştirilmiş yapılardır (Gebremariam ve diğerleri 2019). Bunu çözmek için, SDN tabanlı bulut IoT ağlarında NIDS sistemi için Edge-IDS, Fog-IDS ve Cloud-IDS şeklinde üç katmanlı düğüm yöntemi de önerilmektedir (Nguyen ve diğerleri 2019). Saldırı vektörleri biliniyorsa, tekrarlayan bir sinir ağına (RNN) eklenen çift yönlü uzun kısa süreli bellek (LSTM) birimleri ile saldırı türüne göre %99,99'a kadar doğruluk elde edilebileceği gösterilmiştir (Berman ve diğerleri

2019). Bununla birlikte, MLP'nin (yapay sinir ağı türü- YSA) en az doğru derin öğrenme modeli olduğu bulunmuştur (Roopak ve diğerleri 2019). İstatistiksel önlemler veya bilgisayar eşikleri kullanan Ağ Tabanlı Saldırı Tespit Sistemleri (NIDS), bilgisayar mimarisinin ilk günlerinden beri güvenlik araştırmalarıyla ilişkilendirilmiştir (Vinayakumar ve diğerleri 2019). Benzer şekilde, bir Siyam Ağı Sınıflandırma Çerçevesi (SNCF), risk tahminindeki dengesizliği hafifletebilir ve diğer algoritmalarla karşılaştırıldığında daha güvenilir sonuçlar sunabilmektedir (Sun ve diğerleri 2019). Bulut ortamları, dinamik bir sanal ağ aracılığıyla uzaktan erişilebilen ve kontrol edilebilen sanal IoT nesnelerine neden olan IoT cihaz sanallaştırmasını etkinleştirebilmektedir (Ullah ve diğerleri 2019). Bir güç yükü tahmini optimizasyon algoritması ile genelleştirilmiş regresyon sinir ağına dayandırılabilmektedir (Hu ve ark. 2017). Bu tür YZ algoritmalarının geliştirilmesiyle ilgili en büyük endişe, 5G dağıtımının gerçek zamanlı istihbarat ve güvenliği IoT, IoE ve hatta IoNT arasında ayırabilmesidir (Al-Turjman 2020). Dolayısıyla, zekâ ve biliş teknikleri uygulama alanları ve mimari açısından farklılık gösterecektir. Olası sorunlardan biri, makine öğrenimi platformlarının (TensorFlow, Gaia, Petuum, Apache Spark ve GraphLab gibi) çevrimdışı veri analizi için tasarlanması ve eğitim verilerinin veri analizi için makineler oluşturmak üzere çevrimdışı olarak toplanması, bölümlere ayrılması ve öğrenilmesidir (Cui ve diğerleri 2019). Benzer şekilde, IoT sis hesaplamasında lojistik regresyon ve çok kriterli karar verme, kaynak tahsisi için kullanılabilmektedir (Bashir ve diğerleri 2019).

İzinsiz giriş tespit ve önleme sistemleri (IDS / IPS) ve erişim kontrolü gibi geleneksel siber güvenlik mekanizmaları, bu siber saldırı kategorisini tespit etme, önleme ve engelleme yeteneğine sahip değildir, çünkü sıfırıncı gün tehditleri bilinmeyen bir yanlış davranış sergilerler. Güvenlik sistemlerinin imzalarının veri tabanında bunlar henüz tanımlanamamıştır. Son zamanlarda, sistemleri bu sıfırıncı gün saldırılarından korumak için YZ'ye dayalı yeni bir siber güvenlik mekanizmaları çağı geliştirme aşamasındadır. Siber güvenlik bağlamında, makine öğrenimi teknolojileri, otomatik olarak farklı saldırı patentleri oluşturmak ve dolayısıyla gelecekteki saldırganların yanlış davranışlarını doğru bir şekilde tahmin etmek amacıyla farklı bilgi kaynaklarından gelen büyük miktarda heterojen veriyi yönetmek için kullanılır. Siber savunma bağlamında karar verme sorunlarını (yani, şüpheli cihaz bir saldırgandır ya da değildir) ve saldırı tahminini çözmek için oyun teorik yaklaşımları kullanılmıştır. Karar verme konularında, siber güvenlik oyunu, şüpheli kişileri sınıflandırmak için güvenlik ajanlarının optimal karar vermesini belirlemek amacıyla IDS ve IPS gibi güvenlik aracıları ve saldırganlar gibi rakipleri arasındaki etkileşimi incelemek için kullanılır (Sedjelmaci ve diğ., 2020). Sıfır gün saldırılarının ortaya çıkmasını önlemek, makine öğrenimi ve oyun teorisi dahil olmak üzere farklı YZ sistemleri arasında iş birliğinin yanı sıra güvenlik uzmanı müdahalesini gerektirir. Aslında, karar verme sürecine insan müdahalesi, insan-makine etkileşiminin amacı yanlış pozitiflerin sayısını azaltmak olduğu için saldırı tespitinde bir iyileşmeye yol açar.

Derin Güçlendirmeli Öğrenme ve Birleşik Öğrenmenin mobil uç sistemlerle entegrasyonu, mobil işlem, önbelleğe alma ve iletişimi optimize ederken uç sistemleri daha akıllı hale getirebilir (X. Wang ve diğerleri 2019b). Derin öğrenme modelleri, DDoS saldırılarının %97,16 tespitiyle en yüksek doğruluğu kaydetmiştir ve çok katmanlı yapı, onları uç hesaplamaya çok uyarlanabilir kılmaktadır (Roopak ve diğerleri, 2019). Bu nedenle, veri yüklemede kullanıcı gizliliğini korurken performansı optimize etmek için derin öğrenme uygulanabilmektedir (Li ve diğerleri 2018). YZ uygulamaları gün geçtikçe sürekli yaygınlaşmaktadır. Risk yönetimine yardımcı olabildiği gibi kendisi de birtakım riskleri barındırabilmektedir. Gerçek zamanlı verilerle derin öğrenmenin pratikte nasıl uygulanabileceğini belirlemek için daha fazla araştırmaya ihtiyaç vardır. Muhtemelen pekiştirmeli öğrenme, denetimli/denetimsiz öğrenme ve derin pekiştirmeli öğrenme, bunun nasıl başarılabileceğine dair bazı bilgiler sağlayacaktır (Cao ve diğerleri, 2019; Radanliev ve diğerleri, 2020)

3. KÖTÜ ADAMLAR VE İYİ ADAMLARIN YAPAY ZEKA YARARLANMA ŞEKİLLERİ

Güvenlik çözümlerinin daha akıllı ilkeler ve teknolojiler kullanmaya geçişini gösteren başka bir örnek, basit oturum açma / şifre kontrolünden ses ve yüz tanımaya geçiş yapan kimlik yönetimi ve erişim kontrolüdür (IAM). Güvenlik olaylarını yorumlamak için makine öğrenimi modelleri oluştururken, YZ varlığı veri kümelerini analiz etmeli ve aşağıdaki kalıpları aramalı ve anlamalıdır.

Şekil *3.* YZ algoritma ve modelleri oluşturulduğunda sorulması gereken sorular

Bu beş sorunun yanıtlarını birleştirerek, YZ varlığı bir işlem davranışı oluşturabilir ve ardından bu davranışı geçmiş davranışlarla eşleştirebilir. Davranışlar istatistiksel olarak tutarlı değilse, bir anormallik meydana gelmiş sayılır ve güvenlik bağlamında bu, meydana gelen bir güvenlik olayını gösterebilir. Örnek olarak: Bir personel aynı iş istasyonundan her gün sabah 9'da oturum açabilir ve akşam 17'de oturumu kapatabilir ve bu saatler boyunca tüm bir yıl boyunca yalnızca dosya sunucusuna ve kelime işlemci dosyalarına erişebilir. YZ varlığı, bu modellerle meydana gelen herhangi bir faaliyetin normal davranış olarak kabul edildiği temelini kolayca belirleyebilir. Bununla birlikte, bu personel, elektronik tablo dosyalarına normalde erişmedikleri bir iş istasyonundan saat 21:00'de erişmeye başlarsa, etkinlik bir anormallik olarak kabul edilerek hemen loglanıp işaretlenecek, raporlanacak ve/veya bir karşı bir kontrol önlemi uygulanabilecektir. Bazı durumlarda, çeşitli kullanıcılar günün farklı saatlerinde oturum açabilir ve kapatabilir. İnsan yöneticinin, normal oturum açma modelini oluşturmak için her kullanıcının davranışını önceden tahmin etmesi ve bireysel olarak tanımlaması gerektiğinden, geleneksel kural tabanlı tehdit algılama teknikleri bu kadar çeşitli varyasyonlara ayak uyduramaz. Böyle bir yöntem, her kullanıcının davranışını manuel olarak tahmin etmenin pratik olmadığı geniş bir ortamda kesinlikle düşünülemez.

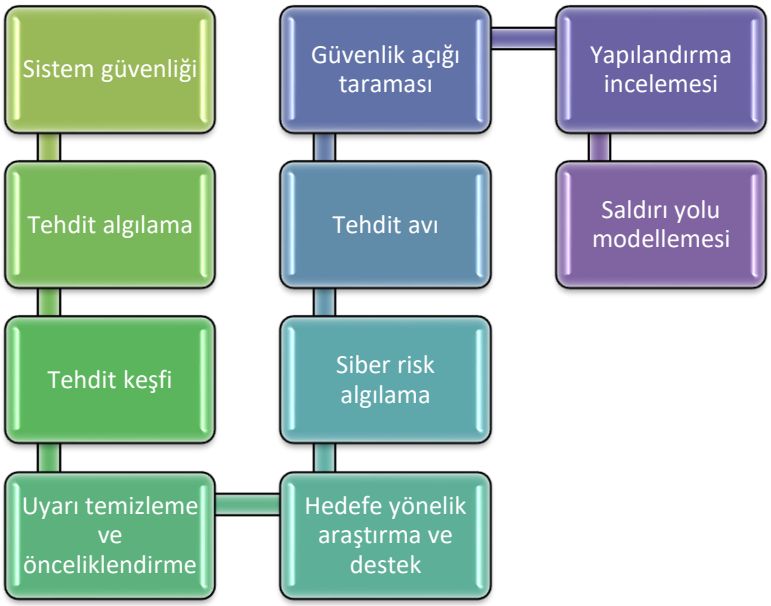
Günümüzde makine öğreniminin kullanımını savunan çoğu siber güvenlik denetimi, makine öğrenimi algoritmalarının üç genel kategorisinden birini veya tümünü kullanabilmektedir:

- *Denetimli* öğrenme, eldeki belirli görev için insan operatörleri tarafından önceden seçilmiş kümelerdeki büyük miktardaki veriler aracılığıyla davranış kalıplarını anlamak için bir YZ motorunu "eğitir". Bir YZ motoru, arabellek taşması güvenlik açıkları gibi belirli bir sınıfla ilgili kod güvenlik açıklarına sahip olduğu bilinen çok sayıda ikili uygulamadan kalıpları anlamak için "*denetimli öğrenmeyi"* kullanabilir. Bir kez eğitildikten sonra, YZ motoru, yürütülen kodun belirli belirli davranışları nasıl taklit ettiğine bakılmaksızın, bu güvenlik açığı sınıfını aramak için kullanılabilir. Bu teknikler, bir uygulamayı iyileştirmek ve güvenliğini sağlamak isteyen siber güvenlik uzmanları için yararlı görünebilir, ancak güvenlik açıklarını manuel olarak yerine hızlı bir şekilde aramak isteyen bir rakip için de yararlıdır.

- *Denetimsiz* öğrenme, bir YZ motorunun sınıflandırılmamış veya kategorize edilmemiş veri kümelerine dayalı belirli model öğrenme modelleri geliştirmesine olanak tanır. Hem bir etik güvenlik uzmanı hem de kötü niyetli bir korsan, uygun bir zaman çerçevesinde manuel olarak bulunması zor olan güvenlik açıklarını arayan otomatikleştirilmiş testler için fuzzy teknikleri geliştirmek için "*denetimsiz öğrenmeyi"* kullanabilir.

- *Takviyeli* (pekiştirilmiş) öğrenme, YZ motorunun çevre ile etkileşim yoluyla ve performansı iyileştirme veya daha iyi veri kalitesi sağlama gibi optimum eylemleri gerçekleştirme karşılığında ödüller alarak öğrenmesine yardımcı olur. Takviye öğrenme, siber güvenlik saldırısı ve savunma teknikleri için gerçekten ilginç bir alandır. "*Cyber Grand Challenge*" a katılan makinelerin tümü, rekabeti kazanmak için en iyi şans için kaynaklarını optimize etmek üzere pekiştirmeli öğrenmeyi kullanmıştır. Diğer makinelere saldırmak için bilgi işlem gücünü kullanmanın bir bedeli olduğunu ve bu maliyetin aynı bilgi işlem gücünü savunma için kullanmaktan çok daha büyük olduğunu, ödül açısından bakıldığında, zamanı kendini savunmak için harcamanın başkalarına saldırmaktan daha iyi olduğunu keşfetmişlerdi. Kuruluşlar, bu mantığı kullanarak, mevcut savunmalarını aşmaya çalışabilecek olası her saldırı kombinasyonunu incelemek ve bunlara yanıt vermek yerine, dışarıdan gelen saldırgan saldırıları durdurmak için en uygun tıkanma noktalarını aramak için makine öğrenimini kullanabilir.

Her üç makine öğrenimi yöntemi de belirli YZ yeteneklerini geliştirmek için çok uygundur ve hem saldırı hem de savunma amaçlı siber güvenlik için eşit derecede ilgilidir. Ne yazık ki, kötü niyetli aktörler tarafından kullanılmak için de çok uygundurlar. Makine öğrenimi, yeni saldırı davranışları dahil, insanların farkında olmadıkları olaylar olan "bilinmeyen bilinmeyenleri" aramada çok başarılıdır. Sonuç olarak, makine öğrenimi, sıfır gün güvenlik açığı istismarını, olağandışı ağ yanal hareketlerini ve olağan dışı saatlerde verilere erişimi tespit etmek için çok uygundur. Tüm bu faaliyetler çok sayıda meydana gelebilir ve bir insan operatörünün şüpheli güvenlik davranışını manuel olarak araştırması zaman alıcı ve yorucu olacaktır. Makine öğrenimi, öğrenmeyi hızlı bir şekilde otomatikleştirir ve çok sayıda tekrarlanan kalıpları analiz etmede ve veri noktaları arasındaki ilişkileri haritalamada mükemmeldir. Örneğin, belirli erişim ayrıcalıklarıyla belirli verilere erişen bir insan kullanıcı kimliğini bir IP adresine kolayca eşleyebilir. Verilerin ve günlüklerin katlanarak büyüdüğü bir dünyada, kalıpları manuel olarak aramak gittikçe zorlaşıyor. Makine öğrenimi, kullanım modellerinin tanımlanmasında ve kullanım modellerinin istatistiksel olarak tutarlı kalmasının sağlanmasında etkili hale gelir. Kullanım modelinin bir anormallik olduğu belirlenirse, bunun bir güvenlik sorunu olma ihtimali vardır.



Şekil 4. Siber güvenlikte YZ algoritması geliştirilen modelleme adımları

Şekilden de anlaşıldığı üzere, siber güvenlik kapsamında YZ kullanım şekilleri çok çeşitli olabilmektedir (Deloitte, 2020):

- *Sistem güvenliği:* Kontrol etkinliği Mevcut günlük verilerini izleyerek ve ardından yanlış yapılandırmayı belirleyip düzelterek güvenlik duvarları, proxy'ler ve veri kaybı önleme çözümleri gibi denenmiş ve test edilmiş araçların etkinliğini artırır ve değerlendirir.
- *Tehdit algılama:* Anormal davranış ve tehdit algılamada kullanıcı oturum açma bilgilerine, kullanıcı davranışındaki değişikliklere ve onaylanmamış değişikliklere odaklanarak anormal veri erişim etkinliklerini ve kötü amaçlı uygulama etkinliklerini tanımlamaya yardımcı olur.
- *Tehdit keşfi:* Normal davranış oluşturmak için faaliyetleri ve varlıkları izler ve dolandırıcılık, kara para aklama ve içeriden gelen tehditler gibi potansiyel riskler yaratabilecek anormallik kaynaklarını tespit eder.
- *Uyarı temizleme ve önceliklendirme:* Saldırı türü, sıklık ve önceki deneyim gibi faktörlere göre ilk triyaj düzeyini önemli ölçüde otomatikleştirmek için makine öğrenimini kullanır.
- *Hedefe yönelik araştırma ve destek:* Geçmiş analiz yoluyla yeni içgörüler elde etmek için büyük bir veri platformu kullanır, böylece mevcut ve geçmiş verilere dayalı olaylara yönelik incelemelerin hızlı ve verimli bir şekilde yapılmasına olanak tanır.
- *Siber risk algılama:* Yeni risk kategorileri, yaygın risk sinyalleri ve artan sosyal medya kullanımı gibi gelecekteki risklerin potansiyel kaynakları dahil olmak üzere, insanlar ve kural tabanlı sistemlerin tespit etmesi genellikle zor olan riskleri belirler veya tahmin eder.
- *Tehdit avlama:* Saldırı döngüsünün başlarında tehditleri etkisiz hale getirmeye yardımcı olmak için bilinen taktikleri, teknikleri, prosedürleri ve saldırı modellerini (güvenlik açığı ayrıntıları ve düzeltme bilgileriyle birlikte) içe aktararak yeni tehditleri hızla arar.
- *Güvenlik açığı taraması:* Güvenlik açıkları için uygulamaları, sistemleri ve diğer varlıkları başlatmak ve taramak, riski değerlendirmek ve yama programını önceliklendirmek için botları kullanır.
- *Yapılandırma incelemesi.* Temel sağlamlaştırmayı sağlamak ve yanlış yapılandırma olmamasını sağlamak için sistem yapılandırmalarını incelemek için botları kullanır.
- *Saldırı yolu modellemesi:* Savunmasız giriş noktalarını ve bir saldırganın erişim elde etmek için kullanabileceği olası yolu belirlemek için güvenlik verileri üzerinde tahmine dayalı analitik gerçekleştirir.

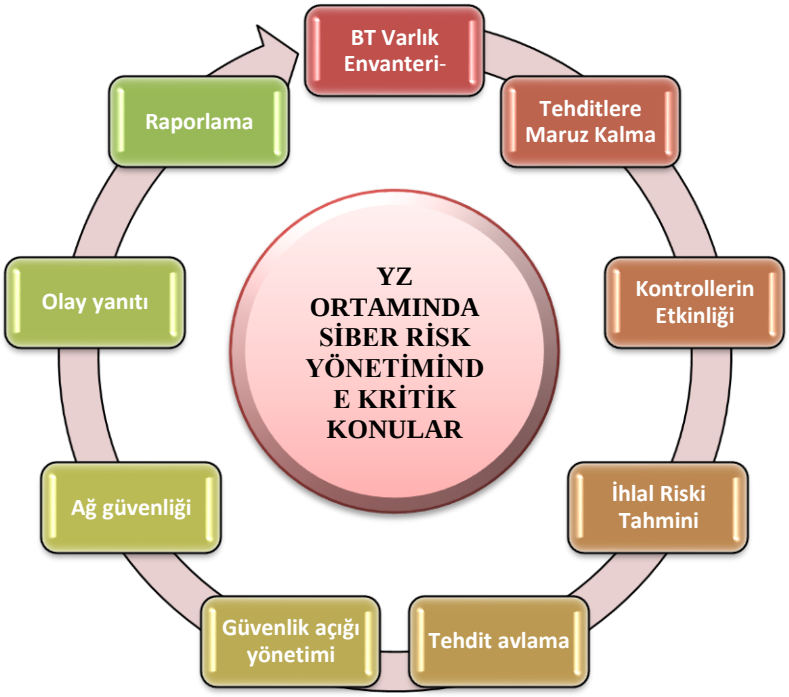
4. YAPAY ZEKAYI SİBER GÜVENLİĞE UYGULAMAK

YZ tabanlı teknolojiler, siber savunma amacıyla aktif olarak kullanılmaktadır. YZ tabanlı çözümlerin uygulanmasında zamanın geçmesi ve karmaşıklığın azalmasıyla birlikte, YZ tabanlı teknolojilerin saldırı amaçlı kullanımı dünyada görünmeye başladı. Bu saldırılar, kanserin yanlış tanımlanması için rakip makine öğrenimi kullanan tıbbi görüntülerle oynamadan, otonom araçların güvenliğini etkilemek için rakip trafik sinyallerinin oluşturulmasına kadar çeşitlilik gösterir (Yamin ve diğ, 2021).

Günümüzün sürekli gelişen siber saldırıları ve cihazların yaygınlaşmasıyla birlikte makine öğrenimi ve YZ, tehdit algılamayı otomatikleştiren ve geleneksel yazılım odaklı yaklaşımlardan daha verimli yanıt veren "kötü adamlara ayak uydurmak" için kullanılabilir. Aynı zamanda, siber güvenlik bazı benzersiz zorlukları da beraberinde getirir:

- Geniş bir saldırı yüzeyi
- Kuruluş başına 10'lu veya 100'lü binlerce cihaz
- Yüzlerce saldırı vektörü
- Nitelikli güvenlik profesyonellerinin sayısındaki büyük eksiklikler
- İnsan ölçeğindeki bir sorunun ötesine geçen veri yığınları

Kendi kendine öğrenen, YZ tabanlı bir siber güvenlik duruş yönetim sistemi, bu zorlukların çoğunu çözebilmelidir. Teknolojiler, kurumsal bilgi sistemlerinizden sürekli ve bağımsız olarak veri toplamak için kendi kendine öğrenen bir sistemi uygun şekilde eğitmek için mevcuttur. Bu veriler daha sonra analiz edilir ve kurumsal saldırı yüzeyiyle ilgili milyonlarca ila milyarlarca sinyal arasında modellerin korelasyonunu gerçekleştirmek için kullanılır. Sonuç, aşağıdakiler dahil olmak üzere çeşitli siber güvenlik kategorilerinde insan ekiplerini besleyen yeni zekâ seviyeleridir:



Şekil 5 Yapay zekâ ortamında siber risk yönetiminde dikkat edilmesi gereken kritik hususlar

- **BT Varlık Envanteri-** Yukarıda, günümüzdeki sorunun çoğunun, saldırı yüzeyini açan IoT'nin yaygınlaşması olduğu belirtilmiştir; YZ, hiçbir insan güvenlik uzmanının makul bir şekilde bunu yapmasının beklenemeyeceği yerlerde, aygıt yazılımı güncellemelerinde ve güvenlik yamalarında gezinmek için filizlenen cihaz okyanusunu yönetmeye yardımcı olur. Bilgi sistemlerine herhangi bir erişimle tüm cihazların, kullanıcıların ve uygulamaların eksiksiz

ve doğru bir envanterini elde etme işidir. İş kritikliğinin sınıflandırılması ve ölçülmesi de envanterde büyük rol oynar.

- **Tehditlere Maruz Kalma**- YZ aracılığıyla, bir güvenlik sisteminin hem küresel hem de sektöre özgü tehditler hakkında sık sık güncellenmesi ve bunların yerel potansiyellerine göre önceliklendirilmesi artık mümkündür. Bilgisayar korsanları da herkes gibi eğilimleri takip edeceğinden dolayı bilgisayar korsanlarının modası düzenli olarak değişebilir. YZ tabanlı siber güvenlik sistemleri, yalnızca kuruluşunuza saldırmak için nelerin kullanılabileceğine değil, aynı zamanda kuruluşunuza saldırmak için kullanılabileceklere dayalı olarak kritik önceliklendirme kararlarının alınmasına yardımcı olmak için küresel ve sektöre özgü tehditler hakkında güncel bilgiler sağlayabilir.

- **Kontrollerin Etkinliği**- güçlü bir güvenlik duruşu sağlamak için kullandığınız çeşitli güvenlik araçlarının ve güvenlik süreçlerinin etkisini anlamak önemlidir. YZ, infosec programınızın nerede güçlü olduğunu ve nerede boşlukları olduğunu anlamanıza yardımcı olabilir.

- **İhlal Riski Tahmini**- BT varlık envanteri, tehdide maruz kalma ve kontrol etkinliğini hesaba katan YZ tabanlı sistemler, zayıflık alanlarına yönelik kaynak ve araç tahsisi için plan yapabilmeniz için ihlal edilme olasılığınızın en yüksek olduğu yer ve nasıl olacağını tahmin edebilir. YZ analizinden elde edilen kuralcı içgörüler, kuruluşunuzun siber dayanıklılığını en etkili şekilde iyileştirmek için kontrolleri ve süreçleri yapılandırmanıza ve geliştirmenize yardımcı olabilir.

- **Tehdit avlama.** YZ ile tehditler maliyetli hale gelmeden önce tespit edilebilir. Güvenlik sistemi, özel bir hizmet reddi saldırısı (DDoS) saldırısını kritik hale gelmeden çok önce algılamak için potansiyel olarak eğitilebilir. Birçok siber güvenlik sağlayıcısı tarafından sunulan ortak bir özellik. Tepkisel olmaktan çok proaktif bir yaklaşım olan otomatik tehdit taramasını ifade eder: Sistem, bilinen izinsiz girişler için uç noktaları izlemekten fazlasını yapabilmektedir. Yalnızca bilinen kalıpları değil, aynı zamanda olası endişe verici tanıdık olmayan kalıpları da tespit etmek için trafiği aktif olarak analiz edebilmektedir. İlk yaklaşım-imza tabanlı algılama- bir şekilde etkilidir ve bilinen tehditlerin %90'ını ortadan kaldırabilir. Ancak YZ, ağ trafiği verilerini analiz ederek ve her türden kalıpları arayarak çok daha iyisini yapabilir, böylece beklenmeyenleri tespit edebilir. Ancak bu, şaşırtıcı olmayan bir şekilde, tehdit olabilecek, ancak tehdit oluşturmayan şeylerin tespit seliyle sonuçlanacak ve boşa zaman harcanmasına neden olacaktır. Pek çok satıcı, bu durumda, hibrit bir yaklaşım benimsemektedir: rutin şeyler için imza tabanlı algılama, geri kalanı için YZ tabanlı model analizi gibi.

- **Güvenlik açığı yönetimi.** Büyük ve karmaşık ağlarda, insan profesyonellerin güvenlikteki olası boşlukları test etmesi de aynı şekilde çok zordur; Ancak YZ bunu halledebilmektedir. Ağ güvenlik açığının yönetimi giderek zorlaşmaktadır. 2019'da bir önceki yıla göre %18artışla 20.000'den fazla yeni güvenlik açığı bildirilmiştir. Birçok satıcı, bu güvenlik açığını azaltmak için araçlar ve özellikler sunabilmektedir. Bu, herhangi bir siber güvenlik sağlayıcı platformunu değerlendirirken aranacak bir özelliktir.

- **Ağ güvenliği.** Siber güvenlikte YZ, bir sistemin büyüdükçe öğrenmesini, her başarı ve başarısızlıkta, kendi kendini ayarlamanın giderek daha verimli ve etkili olmasını mümkün kılabilir. Sıradan bir endişe gibi görünse de kurallar veya politikalar ağ üzerinden zamanında dağıtılmadığı veya tüm cihazlara ürün yazılımı güncellemeleri veya yamaları uygulanmadığı için kaç saldırının başarılı olduğunu düşünmek endişe vericidir. Pek çok siber güvenlik tedarikçisi artık YZ'ye dayalı politika ve güncelleme yönetimi sunmakta ve gösterişsiz de olsa etkili bir değerlendirme yapabilmektedir.

- **Olay yanıtı**- YZ, saldırının ayrıntılı bağlamını ve sonraki çalışma için etkisini sağlayabildiğinden insan ekibi neyin yanlış gittiğini ve siber güvenliğin nasıl

geliştirilebileceğini anlayabilir. YZ destekli sistemler, güvenlik açıklarını azaltmak ve gelecekteki sorunları önlemek için güvenlik uyarılarına hızlı yanıt vermek ve güvenlik uyarılarına hızlı yanıt vermek için önceliklendirme ve yanıt için iyileştirilmiş bağlam sağlayabilir.

- **Raporlama**- YZ, savunma başarısızlıklarının temel nedenlerini ortaya çıkarmaya yardımcı olabilir ve yalnızca politika ve yönetim yerine hem altyapıyı hem de dağıtımı iyileştirmeyi kolaylaştırabilir. Bu, çeşitli infosec programlarının etkisini anlamak ve ilgili bilgileri, son kullanıcılar, güvenlik operasyonları, CISO, denetçiler, CIO, CEO ve yönetim kurulu dahil olmak üzere tüm ilgili paydaşlara raporlamak için, kuruluş genelindeki yönetmenler paydaşların katılımını sağlamak açısından büyük önemi haizdir.

5. YAPAY ZEKA TABANLI SİBER RİSK YÖNETİM ARAÇLARI

Google: Gmail, e-postaları filtrelemek için makine öğrenimi tekniklerini kullanmaktadır. Günümüzde, neredeyse tüm hizmetlerinde, özellikle derin öğrenme yoluyla, algoritmaların eğitilirken ve gelişirken daha bağımsız ayarlamalar ve öz düzenleme yapmalarına olanak tanıyan makine öğrenimi uygulamaları vardır. Google, neredeyse tüm hizmetlerinde, özellikle derin öğrenme olarak bilinen ve algoritmaların eğitilirken ve geliştikçe daha bağımsız ayarlamalar ve öz düzenleme yapmalarına olanak tanıyan bir ML tekniği aracılığıyla makine öğrenimi için uygulamalar bulmuştur. Artık derin öğrenme sayesinde, ne kadar çok veri varsa o kadar iyi demektir. Play Store'da şiddet içeren görüntüleri önlenebiliyor, yorumları taranabiliyor, kimlik avı ve kötü amaçlı yazılımları tespit edilebilmektedir. Bu dolandırıcılık ödemelerini tespit etmek için kullanılabilmekte ve ayrıca bulutu korumak ve güvenliği ihlal edilmiş bilgisayarları tespit etmek için kullanılmaktadır (Newman, 2018)

IBM / Watson: Günümüzde bir güvenlik operasyon merkezinde gerçekleşen birçok iş rutin veya tekrarlayıcıdır. Peki ya bunların bir kısmını makine öğrenimini kullanarak otomatikleştirildiğinde nasıl olacaktır? (Newman, 2018) Watson, IBM'in yapay zekanın benimsenmesinin maliyetlerini ve engellerini azaltırken sonuçları ve yapay zekanın sorumlu kullanımını optimize etmek için tasarlanmış, akıllı hazır araçlar, uygulamalar ve çözümler portföyü olarak bilinmektedir. IBM'deki ekip, bu sorulara cevap olarak makine öğrenimine dayalı "*bilgi birleştirme*" görevleri ve tehdit tespiti için Watson bilişsel öğrenme platformuna giderek daha fazla güvenmektedir (Barrett, 2016).

Juniper Networks: Ağ oluşturma topluluğu, günümüz ağlarının sürdürülemez ekonomisini ele almak için yıkıcı fikirlere ihtiyaç duymaktadır. Juniper, ekonomik olarak uygulanabilir bir "Otonom Ağ Yönetimi" olarak cevap vermeye çalışmaktadır. Juniper WootCloud'un motoru, ağdaki cihazları ve radyo frekansı spektrumunu algılamak için YZ ve makine öğrenimi (ML) kullanmaktadır. HyperContext oluşturmak için fiziksel, mantıksal, operasyonel ve konumsal temas noktalarından cihaz bağlamını derleyebilmekte ve erişim kontrolü ve güvenlik politikaları için gerçeğin kaynağı olarak hizmet eden değerli bilgiler ve doğru risk ve tehdit değerlendirmeleri sağlayabilmektedir. YZ, makine öğrenimi ve amaca yönelik ağ iletişimindeki gelişmeler bizi otomasyonun yerini özerkliğe bıraktığı bir eşiğe getirmiştir (Madrid, 2020).

Balbix BreachControl platformu, sürekli ve gerçek zamanlı risk tahminleri, risk tabanlı güvenlik açığı yönetimi ve ihlallerin proaktif kontrolünü sağlamak için YZ destekli gözlemler ve analizler kullanmaktadır. Platform, siber güvenlik ekiplerinin güçlü bir güvenlik duruşu sağlamak için yapmaları gereken birçok işte daha verimli ve daha etkili olmasına yardımcı olmaktadır. Sistemleri yamalı tutmaktan fidye yazılımlarını önlemeye kadar pek çok şey YZ ile yapılabilmektedir (Bablix, 2021).

bioHAIFCS, siber güvenlik için biyo-ilhamlı bir hibrit YZ çerçevesidir. Bu çerçeve, kritik ağ uygulamalarının, yani askeri bilgi sistemlerinin, uygulamaların ve ağların korunmasına uygun, zamanında ve biyo-ilhamlı makine öğrenimi yöntemlerini birleştirmektedir. Daha spesifik olarak, pasif güvenlik önlemleri kullanarak; kötü amaçlı yazılım tespiti için gelişen hesaplamalı zekâ sistemi

(ECISMD); ve SQL enjeksiyon (ePSSQLI) saldırılarından evrimsel önleme sistemi sağlamaktadır (Demertzis ve Illiadis, 2015).

Siber Güvenlik Araç Kiti (CyberSecTK), siber güvenlikle ilgili verilerin ön işlemesi ve özellik çıkarımı için bir Python kitaplığıdır. Bu kütüphanenin amacı, siber güvenlik ve makine öğrenimi teknikleri arasındaki boşluğu kapatmaktdır. Araç takımı temel olarak bir dizi program modülü, veri seti ve ayrıca siber güvenlik araştırmalarını destekleyen öğreticilerden oluşmaktadır. CyberSecTK, siber uzmanların sıfırdan temel bir makine öğrenimi hattı uygulamasına yardımcı olarak çalışmaktadır (Calix ve diğ., 2020).

Vectra'dan Cognito bulut, veri merkezi, IoT ve kurumsal ağlardaki saldırıları algılayan ve bunlara yanıt veren bir YZ aracıdır. Vectra Cognito platformunu kullanmanın faydalarından bazıları, otomatik tehdit algılama, tehdit avcılarını güçlendirme, tüm dağıtımda görünürlük sağlama ve benzerini içermaktedir (Vectra, 2021).

DefPloreX, büyük ölçekli e-suç süreci kapsamında adli tıp için bir makine öğrenimi araç takımı olarak bilinmektedir. Milyonlarca tahrif edilmiş web sayfasını verimli bir şekilde analiz etmek için açık kaynak kitaplıklarına dayanan esnek bir algoritma kullanmaktadır. DefPloreX veya Defacement eXplorer, yapılandırılmamış verileri anlamlı üst düzey açıklamalara dönüştürmek için makine öğrenimi ve veri görselleştirme tekniklerinin bir kombinasyonunu kullanır. DefPloreX'in en ilginç yönlerinden biri, benzer tahrif edilmiş sayfaları otomatik olarak kümeler halinde gruplandırması ve web olaylarını kampanyalar halinde düzenlemesidir (Balduzzi ve Maggi, 2017)

IBM QRadar Danışmanı, kullanıcılara olay ve risk analizi, önceliklendirme ve yanıt konularında yardımcı olmak için IBM kognitif YZ'sını kullanmakta ve güvenlik operasyonları ekiplerinin çeşitli ihtiyaçlarını karşılamak üzere kurgulanmıştır. Araç, olayları araştırmak için harcanan süreyi günler ve haftalardan dakikalara veya saatlere indirmeye yardımcı olabilmektedir. Rutin SOC görevlerini otomatikleştirme, araştırmalar arasında ortak noktaları bulma ve analistlere eyleme dönüştürülebilir sistematik geri bildirim sağlama gibi nitelikleri haizdir (IBM, 2021).

StringSifter, kötü amaçlı yazılım analiziyle alakalarına göre dizeleri otomatik olarak sıralayan bir makine öğrenme aracıdır. Strings programından aşağı akış yönünde oturmak için inşa edilmiştir. Bu, girdi olarak dizelerin bir listesini aldığı ve kötü amaçlı yazılım analiziyle alakalarına göre sıralanan çıktılarla aynı dizeleri sunduğu anlamına gelmektedir (Stigsifter, 2020).

Sophos'un Intercept X aracı hem bilinen hem de daha önce hiç görülmemiş tehditlere karşı koruma sağlamak için uç nokta güvenliğini reaktif bir yaklaşımdan tahmine dayalı bir yaklaşıma değiştirerek çalışan derin öğrenme sinir ağı ile entegre edilmiş bir siber güvenlik aracıdır. Sophos Intercept X, yalnızca tek bir birincil güvenlik tekniğine güvenmek yerine, uç nokta korumasına yönelik kapsamlı bir derinlemesine savunma yaklaşımı kullanır. Bu aracın özellikleri arasında, diğerlerinin yanı sıra veri yürütme önleme, yığın ekseni, yığın püskürtme tahsisi zorlama yer almaktadır (Intercept, 2020).

Symantec'ten hedefli saldırı analizi (TAA), Symantec tarafından yeni saldırı tekniklerine otomatik olarak uyum sağlayan bulut tabanlı analitikler, sürekli olarak sağlanan saldırı tespitleri ve devam eden yeni saldırı analizlerinin eklenmesi ve daha fazlası gibi çeşitli faydalar sağlamak için geliştirilmiştir. Ayrıca, her müşterinin ortamına göre özelleştirilmiş YZ güdümlü ve insan analiziyle birlikte birden fazla saldırı algılama olayıyla Gelişmiş Tehdit Koruması müşterilerine fayda sağlayabilmektedir (Symantech, 2018).

6. GÜVENLİK RİSK YÖNETİMİ İÇİN KOMPLEKS YAPAY ZEKA SINIRLARI

YZ Makine öğrenmesi yöntemleri kullanılarak devamlı olarak izlenmesi gereken sistemler otomatik hale getirilebilir ama bu sistemin kesinlikle güvenli çalıştığı anlamına gelmemektedir. Zira daha önceden kullanılmamış bir yöntem bulan saldırganlar bir sistem açığından faydalanıp çeşitli zararlara sebebiyet verebilir. Sistemler bu yüzden devamlı olarak geliştirilmeli, güncel teknoloji

haberleri de takip edilip kullanılan sistemler de güncellenmelidir (Takaoğlu ve Özer,2019). Dolayısıyla, makine öğrenimi hiçbir zaman bir olaya bağlamsallaştırma sağlayamaz, ancak olağan dışı kalıpları hızlı bir şekilde insan operatörün dikkatine sunabilir.

Makinelerin "*öğrenmesi*" ve "*eğitilmesi*" için gerekli doğru veri analiz yöntemlerinin uygulanması için verinin hazırlanması ve ayıklanması biraz zaman aldığından dolayı makine öğrenimi kontrolleri, temel davranışı anlamak için modeller geliştirirken kullanımın ilk birkaç haftasında etkisiz olabilir. Genel olarak gelişmiş ülkeler ve özellikle YZ ve siber yeteneklerde önde gelen ülkeler, vatandaşları için güvenlik sağlamak için kontrol mekanizmalarını oluşturmada açık bir başlangıç noktasına sahiptirler. Ancak bu karşılaştırmalı avantajı sürdürmek, çok sayıda kaynaktan önemli ve sürekli bir taahhüt gerektirir. İhtiyaç duyulan şey, ille de bol miktarda bulunmayan ileri görüşlü kurumsal stratejik planlamanın sürdürülmesidir. Açıklık ve güvenlik arasında doğru dengeyi kurmak, sistemlerin sağlamlığını resmi olarak doğrulamak için teknik önlemleri iyileştirmek ve daha önce daha az YZ ile aşılanmış bir dünyada geliştirilen politika çerçevelerinin yeni dünyaya adapte olmasını sağlamak için çok daha fazla çalışma yapılmalıdır. Sistemler eğitile eğitile zamanla daha iyi hale gelebilmektedir. Ancak ilk günlerde doğru yöntem ve uygulama için biraz sabırlı olmak çok önemlidir. Kötü niyetli saldırganlar bildiğiniz her şeyi bilir ve aynı araçlara sahiptirler. Bu durumda üç özel riskten söz edilebilmektedir:

- *Birincisi*, akıllı makinelerin genellikle tasarımcının herhangi bir niyetinden değil, sistemi eğitmek için sağlanan verilerden kaynaklanan gizli önyargıları vardır. Örneğin, bir sistem, geçmişte insan işe alım görevlileri tarafından verilen kararların veri setini kullanarak bir mülakat için hangi işe başvuranların kabul edeceğini öğrenirse, yanlışlıkla ırk, cinsiyet, etnik veya diğer önyargıları sürdürmeyi öğrenebilir. Dahası, bu önyargılar açık bir kural olarak görünmeyebilir, daha çok dikkate alınan binlerce faktör arasındaki ince etkileşimlere gömülü olabilir.
- *İkinci* bir risk, açık mantık kuralları üzerine inşa edilmiş geleneksel sistemlerin aksine, sinir ağlarının gerçek gerçeklerden ziyade istatistiksel gerçeklerle ilgilenmesidir. Bu, özellikle eğitim verilerinde temsil edilmeyen durumlarda, bir sistemin her durumda çalışacağını tam bir kesinlikle kanıtlamayı imkânsız değilse de zorlaştırabilir. Doğrulanabilirdik eksikliği, görev açısından kritik uygulamalarda (bir nükleer santralin kontrol edilmesi gibi) veya ölüm kalım kararları söz konusu olduğunda bir endişe olabilir.
- *Üçüncü* bir risk, makine öğrenimi sistemleri hata yaptığında, sorunun kesin doğasını teşhis etmek ve düzeltmek zor olabilir. Çözüm setine yol açan şey hayal edilemeyecek kadar karmaşık olabilir ve sistemin eğitildiği koşullar değişirse çözüm optimal olmaktan uzak olabilir. Tüm bunlar göz önüne alındığında, uygun kriter mükemmellik arayışı değil, mevcut en iyi alternatiftir.

Risk yöneticileri, bilinmeyen bilinmeyenleri risk hesaplamalarına entegre etmeye adapte olabilmektedirler. Ancak bu, riskin türetildiği konuda sağlam bir temele sahip olduklarını varsayımı altında geçerli bir önermedir. Örneğin, siber risk geliştikçe, daha fazla risk yöneticisi siber riskin gerçekte ne olduğuna daha fazla aşina olma fırsatına sahip olduklarından sigortacılar bu riskleri ele almak için yeni sigorta ürünleri geliştirmek için zaman bulmuştur. Sektörün ne kadar yeni olduğu göz önüne alındığında, çoğu risk yöneticisi ve karar vericinin YZ ve makine öğreniminin ne olduğu, nasıl işlediği, sektörün nasıl ilerlediği veya tüm bunların kendi YZ ve makine öğreniminden doğal olarak kaynaklanan tehditlere karşı kuruluşlarını koruma yeteneği ciddi bir şekilde değerlendirilmelidir.

Risk yöneticilerinin ve karar vericilerin, YZ ve makine öğreniminden üretilmeye devam eden tehditler hakkında daha eğitimli olmaları gerektiği açıktır. Bazı kuruluşlar, bu sistemleri dahili olarak geliştirmeyi amaçlayan kaynakları ayırmada diğerlerinden daha iyi olabilir. Ancak çok azı, bu tür tehditleri ele almak için özel olarak tasarlanmış kaynakları daha az ayırarak, kendi kuruluşlarında bu tür tehditlerin oluşturduğu tehditleri eşzamanlı olarak tahmin etme ihtiyacının farkındadırlar. Bu tehditlerin nasıl etkisiz hale getirilebileceğine dair çözümler önerirken, yönetimin potansiyel tehditlerin farkında olmasını sağlamak kritik bir önemi haizdir.

Bu alandaki büyük rekabet ve pastanın cazibesinden dolayı YZ alanı çok hızlı gelişmekte ve sık sık yepyeni modeller, algoritmalar, konseptler ve mimariler ortaya çıkmaktadır. Ayrıca, bazı ticari ürünler, uygulanan algoritmaların risklerini, avantajlarını ve dezavantajlarını, varsa çok az bir anlayışla modellemeye izin verebilecek modelleri eğitmek için 'otomatik' yollar sunmaya çalışmaktadırlar. Ayrıca, NLP ve bilgisayarla görme alanlarında, serbestçe kullanılabilen veya başka amaçlarla kullanılabilen, kamuya açık önceden eğitilmiş modellerin sayısı giderek artmaktadır. Yüksek karmaşıklık, hızla gelişen ekosistem ve satıcı veya kullanıma hazır modelleri kullanma yeteneği, genellikle kavramsal sağlamlığın değerlendirilmesini geleneksel modellerde olduğundan daha zor hale getirmektedir.

Çıktılar büyük ölçüde konu ve sistemlerle bağlı olabileceğinden, bu alanlarda YZ teknolojilerinin ne zaman kullanılacağı konusunda dikkatli bir değerlendirme yapılması gerekir. Teknolojinin teorik olarak bir görevi yerine getirebilmesi, o görev için mutlaka uygulanması gerektiği anlamına gelmez. YZ' nin belirli bir sorun için uygulanıp uygulanmaması, bir görevi yerine getirmek için teknolojinin teknik kapasitesinin ötesine geçen ticari, düzenleyici ve müşteri kabulü konularını kapsayan daha geniş bir iş sorusudur.

YZ, ses-görüntü tanımlama, sınıflandırma, algılama problemlerini çözme, yüksek boyutlu verileri anlamlandırma ve aynı zamanda yaptığımız şeylerin nispeten dar dilimlerini oluşturan görevleri gerçekleştirme konusunda mükemmel, genellikle insanüstü bir kapasiteye sahiptir. Bu nedenle, YZ modelleri, çeşitli karar verme süreçlerinin birden çok bileşeni için harika çözümler sunabilir. Ancak şu anda sahip olamayacakları yetenekleri sergilemeleri beklenmemelidir. Çalışmasının hızı ve doğruluğu nedeniyle, bir YZ modeline veya herhangi bir hesaplama aracına çok fazla güven atfetme konusunda doğal bir insan eğilimi vardır. Sonuç olarak, kuruluşların teknolojinin risklerini anlamak ve ele almak için yeterince hazır olduklarından emin olmaları gerekir. Bir kuruluşun hazırlık durumunun değerlendirilmesine yönelik pratik bir yaklaşım, aşağıdaki soruların yanıtlanmasını içermektedir (PwC, 2020):

- Seçilen model veya teknolojinin nasıl çalıştığını ve göreceli avantaj ve dezavantajlarının neler olduğunu açıklayabiliyorlar mı?
- Hem model sahipleri hem de üst düzey yönetim, teknolojinin riskleri ve sınırlamalarının farkında mı?
- Bu teknolojiyle ilgili deneyim düzeyleri nedir?
- Eldeki vaka için seçilen teknolojinin uygulanması için sağlam endüstriyi ve akademik kanıtları gördüler mi?
- Model oluşturmanın hangi bölümünü kontrol ediyorlar?
- Modelin üzerinde eğitildiği veriler üzerinde kontrolleri var mı ve eğitim verilerinin hedef kitleyi temsil ettiğinden eminler mi?
- Model kullanımı bağlamını göz önünde bulundurarak, ek karmaşıklığın ve azalan yorumlanabilmenin göreli maliyetini performanstaki potansiyel kazanıma karşı değerlendirdiler mi?
- Yönetim, bu değerlendirmenin sonucundan daha geniş bir iş anlamında memnun mu (yalnızca model teknik performans derecesi değil)?

7. SONUÇ

Yapay zeka (YZ) teknolojilerindeki son gelişmeler özellikle inovasyon ve otomasyonda muazzam büyümeye neden olmuştur. Tehdit aktörleri, saldırı sürecinde YZ tabanlı siber saldırı adı verilen YZ odaklı tekniklerin uygulanmasına özellikle vurgu yaparak saldırı stratejilerini sürekli olarak değiştirmekte ve geliştirmektedir. Bu YZ teknolojileri önemli faydalar sağlasa da kötü amaçla da kullanılabilirler. Örneğin DeepLocker gibi iyi huylu taşıyıcı uygulamalarında yüksek düzeyde hedeflenmiş ve kaçamak saldırılarla YZ' nin zararlı amaçlar için kasıtlı olarak kullanıldığını göstermiştir (Kaloudi ve Li, 2020). Ancak YZ, BT güvenlik uzmanları tarafından iyi siber güvenlik

uygulamalarını güçlendirmek ve kötü amaçlı etkinlikleri sürekli olarak kovalamak yerine saldırı alanını daraltmak için kullanılabilir. Aynı zamanda, devlet destekli saldırganlar, kriminal siber çeteler ve ideolojik hackerler, kurumsal siber savunma duvarlarını aşmak ve tespit edilmekten kaçınmak için aynı YZ tekniklerini kullanabilir. Burada "*YZ / siber güvenlik bilmecesi*" yatmaktadır (Ganti, 2018). YZ olgunlaşıp siber güvenlik alanına giderek daha fazla girdikçe, şirketlerin bu heyecan verici yeni teknolojinin olası dezavantajlarına karşı önlem alması gerekecektir:

- Bilgisayar korsanları, savunmaları aşmak ve tespit edilmekten kaçınmak için yapısını değiştiren mutasyona uğramış kötü amaçlı yazılımlar geliştirmek için YZ'yi kullanabilmektedir.
- YZ, siber saldırılara karşı korunmaya yardımcı olabilmektedir. Ancak bilgisayar korsanları eğitim verdikleri verileri ve aradıkları uyarı bayraklarını hedefleyerek güvenlik algoritmalarını engelleyebilme riskini her halükârda dikkate almak gerekir (Giles, 2018).
- Risk değerlendirmesinde YZ, bir müşterinin özelliklerini ve kapasitesini hesaba katmak için bulabileceği hem finansal hem de finansal olmayan her veriyi kullanarak hızlı ve doğru bir risk değerlendirmesi sağlayabilir. YZ destekli risk yönetimi çözümleri, Avrupa ve ABD sektör düzenleyicileri tarafından gerekli görülen model risk yönetimi (geriye dönük test ve model doğrulama) ve stres testi için de kullanılabilmektedir (Archer, 2021).
- YZ sistemleri, muazzam miktarda veri ve olay olmadan, yanlış uyarı ve hatalı tespitler sunacaktır. Bu riskleri dikkate almak ve optimizasyon için insanlar tarafından makul ölçüde kontrollerin geliştirilmesi her halükârda gereklidir.
- Veri manipülasyonu tespit edilmezse, kuruluşlar YZ sistemlerini besleyen doğru verileri kurtarmak için mücadele edecek ve potansiyel olarak feci sonuçlara yol açabilecektir (CFR, 2017).

YZ'nin siber güvenlik rolündeki belirleyici faktör- "*iyi makineler*" veya "*kötü makineler*" kazansın- hala insan zekasını belirli güvenlik ihtiyaçlarına nasıl uyguladığımızda yatmaktadır. Kuruluşlar sürekli olarak oyunlarını geliştirdiğinde ve en son teknolojileri anlamaya çalıştıklarında, YZ ve makine öğrenimi, tehditlerin bir adım önünde olmalarına ve güvenlik duruşlarını iyileştirmelerine etkili bir şekilde yardımcı olabilirler. Yukarıda yapılan değerlendirmeler sonucunda YZ ile siber güvenlik tehditlerine karşı en iyi şekilde korunmak ve ayakta kalmak için aşağıdaki önlemlerin alınmasında büyük yarar olacağı düşünülmektedir:

- *Gelecek vizyonuyla bakmak:*

"Türkiye Ulusal Yapay Zeka Strateji Belgesi" nde (2021-2025) de ifade edildiği üzere YZ, siber güvenlik ekiplerinin bilginin sınırlarını zorlayan, hayatı zenginleştiren ve siber güvenliği parçalarının toplamından daha büyük görünecek şekilde yönlendiren güçlü insan-makine ortaklıkları oluşturması bir zorunluluk haline gelecektir. Belirli davranışlar sergileyen güvenlik saldırılarını tespit etmek için dar ve kuralcı bir şekilde kullanıldığında, YZ motorları hem saygın şirketler hem de saldırganlar tarafından güvenlik faaliyetlerini gerçekleştirmek için son derece uygun olmaya devam edecektir. YZ, güvenlik açısından riski belirleyebilir ve önceliklendirebilir, bir ağdaki herhangi bir kötü amaçlı yazılımı anında tespit edebilir, olay yanıtına rehberlik edebilir ve başlamadan önce izinsiz girişleri tespit edebilir. Bu YZ tabanlı güçlü yeni siber teknolojilerin geleceğini şekillendirmeye yardımcı olmak için ekosisteminizle iş birliği yapmak ve hatta gerekirse treni kaçırmamak için sektörel öncülük ve değişimde abilik de yapmakta yarar vardır.

- *Ekipleri sürekli eğitmek:*

Siber alanda YZ teknolojileri ve analitiği ile ilişkili iş fırsatlarını anlamak ve değerli bir katkıda bulunulduğundan emin olmak için kurumsal süreçleri çalıştırmak ve sistematik bir yaklaşım sergilenmesi gerekir. Özellikle BT güvenliğinde çalışan personelin yanı sıra denetim (müfettiş, kontrolör, denetçi vb.) görevlileri, operasyonlarda çalışanlar, sistemlere mantıksal veya fiziksel erişimi olanlar ve vatandaşları gerektiği ve yeteri kadar eğitime tabi tutmakta büyük yarar vardır.

Bazen bir temizlik görevlisi veya yardımcı personelin zafiyeti bile devasa güvenlik mekanizmalarını etkisiz hale getirmek için tek başına yeterli olabilmektedir.

- *Risk ve tehdit ortamını sürekli değerlendirmek:*

Kötü amaçlı faaliyetler farklı şekillerde meydana gelebilir. Bu, belirli saldırı davranışını aramak için korelasyon kurallarını kullanan geleneksel güvenlik bilgileri ve olay yönetimi (SIEM) araçlarının genellikle başarısız olacağı anlamına gelir. Bu nedenle, modern güvenlik operasyon merkezleri, SIEM, kötü amaçlı yazılımdan koruma ve güvenlik duvarları gibi kural tabanlı kontrollerin kullanımını, uç nokta koruma platformları ve kullanıcı ve varlık davranış analitiği (UEBA) gibi makine öğrenimi özellikli kontrollerle desteklemelidir. Yeni teknolojilerin etkisini anlayarak uygun risk yönetimi yanıtları geliştirmek için tehdit vektörlerini, olasılık ve etkilerini iyice incelemek gerekir.

- *Hesap verebilirlik modelini yeniden tanımlamak*:

İşletim ortamındaki değişikliklerin risk iştahını ve gerekli kontrolleri nasıl etkileyeceğini düşünerek ardından siber ekibin rollerini ve sorumluluklarını buna göre ayarlamak gerekir. Herhangi bir ihlal, sızma veya suiistimal olması durumunda kimlerin ne derece sorumlu tutulacakları ve kimlerin ne tür cezalara maruz kalabilecekleri konusu son derece net olarak belirlenmeli ve ilgili personel tarafından bilinmelidir.

- *Kontrol çerçevenizi mantıklı hale getirmek:*

Maliyet tasarrufu ve süreçlerin verimliliğini sağlamak için gereksiz kontrol katmanlarını azaltmak ve önceden daha fazla önleyici ve otomatikleştirilmiş yetenekler oluşturmak için yeni sistemler, teknolojiler ve kontrol çerçeveleri için riske duyarlı tasarımı teşvik etmek gerekir. Bunun için rol tabanlı ve ihtiyaca göre yetkilendirme şart tutulmalı ve erişim politika ve kontrolleri periyodik olarak gözden geçirilmelidir.

- *Küçük başlayıp hızlı ölçeklendirmek:*

Yüksek etkiye, düşük karmaşıklığa, hazır verilere ve yetersiz mevcut yeteneklerle muhtemel fırsatları belirleyerek YZ teknolojilerini ve analitiği siber güvenliğe uygulamak için pratik bir strateji geliştirmek gerekir. Neticede bir 10 yıl sonra YZ ile her türlü süreç ve çalışan bir şekilde aşina olacaktır. Bu nedenle şimdiden en ufaktan başlayarak imkanlar ölçüsünde hazırlıklara başlamak gerekir.

- *Siber yetenek stratejini yeniden düşünmek:*

Yetenekli siber profesyonellerin siber güvenlik çabalarınıza öncülük etmesini sağlamak için adımlar atarak gerekirse danışmanlık ve rehberlik de sağlayarak İK yetenek stratejisini güncellemek gerekir.

KAYNAKÇA

Abegunde, J., Xiao, H., & Spring, J. (2016) A dynamic game with adaptive strategies for IEEE 802.15.4 and IoT. 2016 IEEE Trustcom/ BigDataSE/ISPA, 473–480. https://doi.org/10.1109/TrustCom. 2016.0099

Aldemir, C. & Kaya, M. (2020). Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları. Kamu Yönetimi ve Politikaları Dergisi, 1 (1), 6-27. Retrieved from https://dergipark.org.tr/tr/pub/kaypod/issue/56116/726431

Al-Turjman F (2020) Intelligence and security in big 5G-oriented IoNT: an overview. Futur Gener Comput Syst 102:357–368. https://doi.org/10.1016/j.future.2019.08.009

Anagnostopoulos, C., & Hadjiefthymiades, S. (2019) A Spatio-temporal data imputation model for supporting analytics at the edge. Digital transformation for a sustainable society in the 21st

century: 18th IFIP WG 6.11 conference on E-Business, E-Services, and E-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings, 11701, 138

Archer (2021a) Fraud Detection: How to use machine learning in fintech?, https://archer-soft.com/blog/fraud-detection-how-use-machine-learning-fintech

Archer (2021b) 6 Artificial Intelligence use cases in financial services, https://archer-soft.com/blog/6-artificial-intelligence-use-cases-financial-services

Archer, (2021c) How AI is changing the risk management? Source: https://archer-soft.com/blog/how-ai-changing-risk-management

Bablix, (2021) Balbix BreachControl, https://www.balbix.com/product-overview/

Baloglu, A, Kılıç, S, Binay, A, Tükel, D. (2020). Endüstriyel Üretim Tesisleri İçin Asistan Robot Araştırması ve Analizi. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 4 (1) , 13-27 . DOI: 10.33461/uybisbbd.620575

Balduzzi M., Maggi F., (2017) DefPloreX: A Machine-Learning Toolkit for Large-scale eCrime Forensics, Trendmicro, https://blog.trendmicro.com/trendlabs-security-intelligence/ defplorex-machine-learning-toolkit-large-scale-ecrime-forensics/

Barker K, Lambert JH, Zobel CW, Tapia AH, Ramirez-Marquez JE, Albert L, Nicholson CD, Caragea C (2017) Defining resilience analytics for interdependent cyber-physical-social networks. Sustain Resilient Infrastruct 2(2):59–67. https://doi.org/10.1080/23789689. 2017.1294859

Barrett, B. (2016) IBM's Watson Has a New Project: Fighting Cybercrime, Wired, https://www.wired.com/2016/05/ibm-watson-cybercrime/

Bashir H, Lee S, Kim KH (2019) Resource allocation through logistic regression and multicriteria decision-making method in IoT fog computing. Trans Emerg Telecommun Technol. https://doi.org/10. 1002/ett.3824

Berman D, Buczak A, Chavis J, Corbett C (2019) A survey of deep learning methods for cybersecurity. Information 10(4):122. https://doi.org/10.3390/info10040122

Blanco-Filgueira B, Garcia-Lesta D, Fernandez-Sanjurjo M, Brea VM, Lopez P (2019) Deep learning-based multiple object visual tracking on embedded system for IoT and mobile edge computing applications. IEEE Internet Things J 6(3):5423–5431. https://doi.org/10.1109/JIOT.2019. 2902141

Calix R.A., Singh S.B., Chen T., Zhang D. and Tu M., (2020) Cyber Security Tool Kit (CyberSecTK): A Python Library for Machine Learning and Cyber Security, Information 2020, 11, 100; doi:10.3390/info11020100

Cao, B., Zhang, L., Li, Y., Feng, D., & Cao, W. (2019) Intelligent offloading in multi-access edge computing: a state-of-the-art review and framework. In: IEEE communications magazine. Institute of Electrical and Electronics Engineers Inc., (vol. 57, issue 3, pp. 56– 62). https://doi.org/10.1109/MCOM.2019.1800608

CFR, (2017) The Cybersecurity Vulnerabilities to Artificial Intelligence, Net Politics, https://www.cfr.org/blog/cybersecurity-vulnerabilities-artificial-intelligence

Cui Q, Gong Z, Ni W, Hou Y, Chen X, Tao X, Zhang P (2019) Stochastic online learning for mobile edge computing: learning from changes. IEEE Commun Mag 57(3):63–69. https://doi.org/10.1109/ MCOM. 2019.1800644

Deloitte, (2020) Smart cyber: How AI can help manage cyber risk, https://www2.deloitte.com/ content/dam/Deloitte/ca/Documents/risk/ca-en-smart-cyber-pov-aoda.pdf

Demertzis K., Iliadis L. (2015) A Bio-Inspired Hybrid Artificial Intelligence Framework for Cyber Security. In: Daras N., Rassias M. (eds) Computation, Cryptography, and Network Security. Springer, Cham. https://doi.org/10.1007/978-3-319-18275-9_7

Diro AA, Chilamkurti N (2018) Distributed attack detection scheme using deep learning approach for Internet of Things. Futur Gener Comput Syst 82:761–768. https://doi.org/10.1016/ j.future.2017.08. 043

FAIR (2017) What is a cyber value-at-risk model? http://www.fairinstitute.org /blog/what-is-a-cyber-value-at-risk-model

Ganti, V. (2018). How Machine Learning and AI in Cybersecurity is Shaping IT, Biztech Magazine, https://biztechmagazine.com/article/2018/06/role-artificial-intelligence-cybersecurity

Gebremariam, A. A., Usman, M., & Qaraqe, M. (2019) Applications of artificial intelligence and machine learning in the area of SDN and NFV: a survey. 16th international multi-conference on systems, sig nals and devices, SSD 2019, 545–549. https://doi.org/10.1109/SSD. 2019.8893244

Giles, M. (2018) AI for cybersecurity is a hot new thing—and a dangerous gamble, Technology Review, https://www.technologyreview.com/2018/08/11/141087/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/

Guo Y., Cao H., Han S., Sun Y., Bai Y. (2018) Spectral-spatial hyperspectral image classification with K-nearest neighbor and guided filter. IEEE Access 6:18582–18591. https://doi.org/10.1109/ ACCESS.2018. 2820043

Hu R., Wen S., Zeng Z., Huang T. (2017) A short-term power load fore casting model based on the generalized regression neural network with decreasing step fruit fly optimization algorithm. Neurocomputing 221:24–31. https://doi.org/10.1016/j.neucom. 2016.09.027

IBM (2021) QRadar Advisor with Watson, https://www.ibm.com/in-en/products/ cognitive-security-analytics

Intercept, (2020) Stop Unknown Threats, Sophos, https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-intercept-x-dsna.pdf

Kaloudi N. & Li J., (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Comput. Surv. 53, 1, Article 20 (May 2020), 34 pages. DOI: https://doi.org/10.1145/3372823

Küçük, D, Arıcı, N . (2018). Doğal dil işlemede derin öğrenme uygulamaları üzerine bir literatür çalışması. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2 (2) , 76-86 . Retrieved from https://dergipark.org.tr/tr/pub/uybisbbd/issue/41787/443574

Li H., Ota K. & Dong M. (2018) Learning IoT in edge: deep learning for the Internet of Things with edge computing. IEEE Netw 32(1):96–101. https://doi.org/10.1109/ MNET.2018.1700202

Madrid, S., (2020) Juniper Strengthens Connected Security Portfolio with New Risk-Based Access Control Capabilities and Remote Access VPN, Juniper, https://blogs. juniper.net/en-us/security/juniper-strengthens-connected-security-portfolio-with-new-risk-based-access-control-capabilities-and-remote-access-vpn

Malhotra Y. (2018) Cognitive computing for anticipatory risk analytics in intelligence, surveillance, & reconnaissance (ISR): model risk management in artificial intelligence & machine learning (presentation slides). SSRN Electron J. https://doi.org/10.2139/ssrn.3111837

Newman, L. H., (2018) AI Can Help Cybersecurity—If It Can Fight Through the Hype, Wired, https://www.wired.com/story/ai-machine-learning-cybersecurity/

Nguyen T.G., Phan TV, Nguyen BT, So-In C, Baig ZA, Sanguanpong S (2019) SeArch: a collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks. IEEE Access 7:107678–107694. https://doi.org/10.1109/ACCESS.2019.2932438

Park D., Kim S., An Y., Jung J-Y. (2018) LiReD: a light-weight real-time fault detection system for edge computing using LSTM recurrent neural networks. Sensors 18(7):2110. https://doi.org/10.3390/s18072110

Porambage, P., Kumar, T., Liyanage, M., Partala, J., Lovén, L., Ylianttila, M., & Seppänen, T. (2019) Sec-edgeAI: AI for edge security vs. security for edge AI BrainICU-measuring brain function during intensive care view project ECG-based emotion recognition view project Sec-EdgeAI. https://www.researchgate.net/publication/330838792

PwC, (2020) Model Risk Management of AI and Machine Learning Systems, https://www.pwc.co.uk/data-analytics/documents/model-risk-management-of-ai-machine-learning-systems.pdf

Radanliev P, De Roure D, Nurse JRC, Mantilla Montalvo R, Cannady S, Santos O, Maddox L, Burnap P, Maple C (2020a) Future developments in standardization of cyber risk in the Internet of Things (IoT). SN Appl Sci 2(2):1–16. https://doi.org/10.1007/s42452-019-1931-0

Radanliev, Petar & De Roure, David & Page, Kevin & Van Kleek, Max & Santos, Omar & Maddox, la & Burnap, Pete & Anthi, Eirini & Maple, Carsten. (2020). Design a dynamic and self-adapting system, supported with artificial intelligence, machine learning, and real-time intelligence for predYun.ive cyber risk analytics in extreme environments – cyber risk in the colonization of Mars.

Roopak, M., Yun Tian, G., & Chambers, J. (2019) Deep learning models for cybersecurity in IoT networks. 2019 IEEE 9th annual computing and communication workshop and conference, CCWC 2019, 452– 457. https://doi.org/10.1109/CCWC.2019.8666588

Sanford, A., & Moosa, I. (2015). Operational risk modeling and organizational learning in structured finance operations: A Bayesian network approach. Journal of the Operational Research Society, 66(1), 86–115.

Sangaiah A.K., Medhane D.V., Han T., Hossain M.S., Muhammad G. (2019) Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics. IEEE Trans Ind Inform 15(7):4189–4196. https://doi.org/10.1109/TII.2019.2898174

Sedjelmaci H., Guenab F., Senouci S., Moustafa H., Liu J. & Han S., (2020) "Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems," in IEEE Network, vol. 34, no. 3, pp. 6-7, May/June https://doi.org/10.1109/MNET.2020.9105926 .

Stigsifter, (2020) A machine learning tool that ranks strings based on their relevance for malware analysis. Fireeye, https://github.com/fireeye/stringsifter

Sultana N., Chilamkurti N., Peng W., Alhadad R. (2019) Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Netw Appl 12(2):493–501. https://doi.org/10.1007/s12083-017-0630-0

Sun, D., Wu, Z., Wang, Y., Lu, Q., & Hu, B. (2019) Risk prediction for imbalanced data in cybersecurity: a Siamese network-based deep learning classification framework. Proceedings of the international joint conference on neural networks, 2019-July, 1–8. https://doi.org/10.1109/ IJCNN.2019.8852030

Syafrudin M, Fitriyani N, Alfian G, Rhee J (2018) An affordable, fast early warning system for edge computing in assembly line. Appl Sci 9(1):84. https://doi.org/10.3390/app9010084

Symantech, (2018) Targeted Attack Analytics, https://docs.broadcom.com/doc/targeted-attack-analytics-en

Takaoğlu, M , Özer, Ç . (2019). Saldırı Tespit Sistemlerine Makine Öğrenme Etkisi . Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 3 (1), 11-22. DOI: 10.33461/uybisbbd.558192

Thompson, M.F., Vidas, T., (2018), CGC monitor: A vetting system for the DARPA cyber grand challenge, Digital Investigation, https://doi.org/10.1016/j.diin.2018.04.016

Tung L., (2017) Elon Musk: Regulate AI now, before it's too late, ZDNET, https://www.zdnet.com/article/elon-musk-regulate-ai-now-before-its-too-late/

Ullah I, Ahmed S, Mehmood F, KimD (2019) Cloud-based IoT network virtualization for supporting dynamic connectivity among connected devices. Electronics 8(7):742. https://doi.org/10.3390/electronics8070742

Vectra, (2021) Cognito Platform-Network detection and response built on artificial intelligence https://www.vectra.ai/products/cognito-platform

Vinayakumar R, Alazab M, Soman KP, Poornachandran P, Al-Nemrat A, Venkatraman S (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

Wang J, Hu J, Min G, Zhan W, Ni Q, Georgalas N (2019a) Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning. IEEE Commun Mag 57(5): 64–69. https://doi.org/10.1109/MCOM.2019.1800971

Wang X, Han Y, Wang C, Zhao Q, Chen X, Chen M (2019b) In-edge AI: intelligent sizing mobile edge computing, caching and communication by federated learning. IEEE Netw 33(5):156–165. https://doi.org/10.1109/MNET.2019.1800286

Yamin M. M., Ullah M., Ullah H., & Katt B., (2021) Weaponized AI for cyberattacks, Journal of Information Security and Applications, Volume 57, 102722, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102722.

Yıldız, D. (2021). Bilgi Yönetiminde Kural Tabanlı Uzman Sistem Geliştirme Adımları Ve Başarı Faktörleri. Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 5 (1), 28-43. DOI: https://doi.org/10.33461/uybisbbd.913513

Yin H, Xue M, Xiao Y, Xia K, Yu G (2019) Intrusion detection classification model on an improved k-dependence Bayesian network. IEEE Access 7:157555–157563. https://doi.org/10.1109/ ACCESS. 2019.2949890

Zhang, D., Bao, W., Fang, T., Liang, W., Zhou, W., Ma, L., Gao, X., & Niu, L. (2019) Edge task allocation scheme based on data classification. Proceedings – 2019 5th international conference on big data and information analytics, BigDIA 2019, 132–138. https://doi.org/10.1109/ BigDIA.2019.8802859