Yönetim Bilişim Sistemlerinde Güncel Konular

Editör: Dr. Öğr. Üyesi Mehmet Fatih KARACA

ÖZGÜR YAYINLARI

Yönetim Bilişim Sistemlerinde Güncel Konular

Editör:
Dr. Öğr. Üyesi Mehmet Fatih KARACA

ÖZGÜR YAYINLARI

Published by
Özgür Yayın-Dağıtım Co. Ltd.
Certificate Number: 45503

15 Temmuz Mah. 148136. Sk. No: 9 Şehitkamil/Gaziantep
+90.850 260 09 97
+90.532 289 82 15
www.ozguryayınlari.com
info@ozguryayinlari.com

Yönetim Bilişim Sistemlerinde Güncel Konular

Current Topics in Management Information Systems

Editör: Dr. Öğr. Üyesi Mehmet Fatih KARACA

Language: Turkish-English
Publication Date: 2024
Cover design by Mehmet Çakır
Cover design and image licensed under CC BY-NC 4.0
Print and digital versions typeset by Çizgi Medya Co. Ltd.

ISBN (PDF): 978-975-447-941-6

DOI: https://doi.org/10.58830/ozgur.pub498

Suggested citation:
Karaca, M. F. (ed) (2024). *Yönetim Bilişim Sistemlerinde Güncel Konular.* Özgür Publications.
DOI: https://doi.org/10.58830/ozgur.pub498. License: CC-BY-NC 4.0

The full text of this book has been peer-reviewed to ensure high academic standards. For full review policies, see https://www.ozguryayinlari.com/

ÖZGÜR YAYINLARI

Önsöz

Yönetim Bilişim Sistemleri, işletmelerin karar verme süreçlerini desteklemek amacıyla bilişim teknolojileri ve yönetim uygulamalarını bir araya getiren bir alandır. Endüstri 4.0 veya teknolojik gelişmelerin gelecek trendlerine bakıldığında gerek günlük hayatta gerekse de endüstride bilişim teknolojilerinin etkisini sürdüreceğini, kullanım alanlarının genişleyebileceğini söylemek yanlış olmayacaktır.

Özellikle bilişim ve endüstriyi bir araya getiren Endüstri 4.0 ile hayatımıza yeni kavramların girdiği gözlenmiştir. Robotik sistemler, nesnelerin interneti (IoT), siber fiziksel sistemler, büyük veri ve analitiği, dijital dönüşüm gibi bu yeni kavramlar, bilişim teknolojileriyle ilişkilidir.

Yönetim Bilişim Sistemlerinde Güncel Konular başlıklı bu kitapta alanın güncel konularının bir araya getirilmesi amaçlanmıştır. 1. bölümde robotik sistemlerin özellikleri, ilgili mesleklerin geleceği ve yükseköğretimdeki robotik programlar araştırılmıştır. 2. bölümde IoT, uygulama alanları, güvenlik ve gizlilik konuları ile gelecek trendleri ele alınmıştır. 3. bölümde siber güvenlikte tehditler, koruma yöntemleri, açık kaynak yazılımlar, yapay zekâ ve trend analizleri ile güvenlik uyum yönetimi başlıkları incelenmiştir. 4. bölümde ise yönetim bilişim sistemleri perspektifinden dijital dönüşüm konusu üzerinde durulmuştur.

İçindekiler

Önsöz iii

Bölüm 1

Robotik Sistemler: Özellikleri, İlgili Mesleklerin Geleceği ve Yükseköğretimde Robotik Programlar 1

Mehmet Fatih Karaca

Bölüm 2

Nesnelerin İnterneti (IoT) 15

Ali Erbey

Bölüm 3

Siber Güvenliğin Temelleri: Tehditler, Koruma Yöntemleri, Açık Kaynak Yazılımlar, Yapay Zekâ ve Trend Analizleri ile Güvenlik Uyum Yönetimi 35

Hüseyin Parmaksız

Bölüm 4

Yönetim Bilişim Sistemleri Perspektifinden Dijital Dönüşüm: Stratejiler ve Organizasyonel Etkileri 55

Üzeyir Fidan

Bölüm 1

Robotik Sistemler: Özellikleri, İlgili Mesleklerin Geleceği ve Yükseköğretimde Robotik Programlar

Mehmet Fatih Karaca[1]

Özet

Robotik sistemler programlanabilen, belirli görevleri otonom veya yarı otonom olarak yerine getirebilen, mekanik, elektronik ve yazılımdan oluşan, otomasyon ve yapay zekâ unsurlarını bir araya getiren sistemlerdir. Yalnızca üretim süreçlerinde değil; hayatın birçok alanında kullanılır hale gelen robotik sistemler, endüstriyel üretimden sağlık hizmetlerine, tarımdan uzay araştırmalarına kadar oldukça geniş uygulama alanlarına sahiptir. Bu çalışmada robotik sistemlerin genel tanıtımı, robotik sistemler mesleğinin mevcut ve gelecekteki olası durumları ile yükseköğretim kurumlarındaki lisans ve ön lisans düzeyindeki robotik programlarının incelenmesi gerçekleştirilmiştir. Ayıca, robotik sistemlerin genel özellikleri, bileşenleri, kullanım alanları, avantajları ve gelişmeler ele alınmıştır.

1. Giriş

İhtiyaç ve gereksinimlerin artmasına karşın kaynakların azalması, farklı üretim teknolojilerinin kullanılmasını gerekli hale getirmiş; teknolojinin hızlı gelişmesiyle beraber kas gücüne dayalı üretim faaliyetleri yerini makineleşmeye bırakmıştır. Bunun neticesinde de daha önceleri insan eliyle yapılan işlemler bugün robotlarla gerçekleştirilir olmuştur.

Endüstri 4.0 üretim ve imalat süreçlerinde dijitalleşme, otomasyon ve veri alışverişini temel alan sanayi devrimidir. Endüstri 4.0 ile bilişim teknolojileri ile endüstrinin bir araya getirilmesi amaçlanmış olsa da esasında bu devrimin altında yatan motivasyon az işçiyle kaliteli ürün elde etme ve insanın beden gücünden değil; beyin gücünden faydalanma isteğidir. Endüstri 4.0

1 Dr. Öğr. Üyesi, Tokat Gaziosmanpaşa Üniversitesi, Erbaa Sosyal ve Beşeri Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, ORCID: 0000-0002-7612-1437, mehmetfatih.karaca@gop.edu.tr

https://doi.org/10.58830/ozgur.pub498.c2089

ile verimli, hatasız, yenilikçi ve düşük maliyetli ürünlerin üretilebilmesi sağlanmış; akıllı fabrika kavramı ortaya çıkmıştır. Akıllı fabrika, üretimde dijital teknolojilerin kullanıldığı, sürecin dijital teknolojilerle entegre edildiği, üretimde yer alan tüm cihaz, makine ve ekipmanların birbirlerine bağlanarak haberleşebildiği bir üretim modelidir. Bunu tesis etmenin yolu da üretimde robotik sistemlere yer vermektir.

Robot sistemleri, üretim görevlerini yerine getirmek ve üretim verimliliğini optimize etmek amacıyla kullanılmaktadır. Günümüzde ise yalnızca üretim süreçlerinde değil; hayatın birçok alanında robotik sistemleri görmek mümkündür.

Robotik sistemler teknoloji ve mühendislik disiplinlerinin birleşimiyle ortaya çıkan, günümüz üretim süreçlerinde otomasyon ve yapay zekâ unsurlarını bir araya getirerek yenilikçi çözümler olarak ortaya çıkan önemli bir konu halini almıştır. Bu sürecin basit makinelerle başladığı; günümüzde ise karmaşık algoritmalar, sensörler ve aktüatörler kullanılarak yüksek düzeyde otonomi ve etkileşim yeteneğine sahip robotların geliştirilmesiyle devam ettiği görülmektedir.

Robotik sistemler, endüstriyel üretimden sağlık hizmetlerine, tarımdan uzay araştırmalarına kadar oldukça geniş uygulama alanlarına sahiptir. Bu sistemlerin sağladığı avantajlar, verimliliğin artırılması ve maliyetlerin düşürülmesi gibi ekonomik faydaların ötesinde insan yaşam kalitesini iyileştirmesine de katkılar sağlamaktadır.

Robotik sistemlerin gelişimi sadece teknolojik ilerlemelerle sınırlı değildir. Bu alanda karşılaşılan etik ve toplumsal sorunlar, robotların insan iş gücünün yerini alması, mahremiyet, güvenlik ve bağımlılık gibi konular, derinlemesine ele alınması gereken hususlardandır. Örneğin; otomasyon sistemlerinin iş gücü üzerindeki etkileri ve işsizlik riskleri, toplumda geniş yankı ve kaygı uyandırmaktadır. Ayrıca, robotların karar verme süreçlerinde şeffaflık ve hesap verebilirlikleri hem mühendislik hem de etik açısından kritik öneme sahiptir. Bu bakımdan robotik sistemlerin yalnızca teknolojik bir başarı olarak görülmemesi gerektiği; aynı zamanda toplumsal bir dönüşüme neden olacak bir araç olabilme potansiyeli barındırdığı vurgulanmalıdır.

Alan yazında robotik sistemlerin çeşitli açılardan incelendiği, çalışmalarda ağırlıklı olarak robotik sistemlerin belirli bir amaç, alan veya sektör için tasarımı ve kullanımı konularına odaklanıldığı görülmektedir.

Akbaba ve Gündoğdu (2023), telepresence robotları incelediği çalışmada günlük işlemlere uyarlanmaya çalışılan telepresence robotların yaygınlaşmaya başladığını, telepresence robotlar aracılığıyla yaşlı bireylerin iletişim

kabiliyetlerinin geliştiğini ve evde geçirdikleri zamanın kalitesinin arttığını, engelli bireylerin bakımlarını kolaylaştırdığını, evde daha uzun zaman geçirmek durumunda kalan bu bireylerin sosyalleşme süreçlerine olumlu etkilerinin olduğunu belirtmişlerdir. Sivri (2023), yaptığı araştırmada kütüphanelerdeki robotik sistemlerin kullanım örneklerini incelemiş; robotik sistemlerin kütüphanelerde birçok görevi yerine getirebileceğini, robotların görev almasıyla aranan kitaba erişimde kütüphaneciye olan ihtiyacın azalacağını, konuşma yeteneğine ulaşan robotların kullanıcıların taleplerini alarak önerilerde bulunabileceğini ifade etmiştir. Işık vd. (2021), hayvancılıkta robotik sistemlerin kullanımlarını incelemiş; tam otonom akıllı çiftlikler açısından yapay zekâ ve robotik biliminin birlikte kullanılmasının önemine değinmişlerdir. Görçün (2018), robotik sistemlerin lojistik süreçlerdeki işlevlerini incelediği çalışmasında çok uzak olmayan yakın bir gelecekte lojistik alanında robotik sistemlerin hayati ve vazgeçilmez bir konuma geleceği değerlendirmesinde bulunmuştur. Kural ve Atuğ (2010), ürolojide robotik cerrahi uygulamalarını derledikleri çalışmada 2010 yılı itibariyle robotların cerrahi teknolojiye dahil olmasının yeni bir gelişme olduğunu, ancak cerrahideki kullanım alanlarının hızla arttığını bildirmişlerdir. Özfırat (2009) çalışmasında madencilikte robotik sistemlerin kullanımını araştırmış; yeraltındaki risk barındıran bölgelerde robotik sistemlerin kullanıldığına ve madencilik alanında yeraltı üretim noktalarında operatörsüz robotik sistemlerin iş güvenliğini arttırması açısından önemli olduğuna vurgu yapmıştır. Peçe vd. (2020) araştırmasında 2 tekerlekli kendini dengeleyebilen robotik sistem tasarımı ve kontrol yöntemleri üzerine odaklanmış, tasarlanan robotik sistemin kendini dengeye getirebildiği sonucuna ulaşmıştır.

2. Çalışmanın Amacı

Bu çalışmada robotik sistemlerin genel tanıtımı, robotik sistemlerle ilgili mesleklerin geleceği ve yükseköğretim kurumlarındaki robotik programların incelenmesi gerçekleştirilmiştir. Konuyu incelemek amacıyla çalışma kapsamında aşağıdaki sorulara yanıt aranmıştır;

- Robotik sistem nedir?
  - Robotik sistemlerin bileşenleri nelerdir?
  - Robotik sistemlerin kullanım alanları nelerdir?
  - Robotik sistemlerin avantajları nelerdir?
  - Robotik sistemlerdeki gelişmeler nelerdir?
- Robotik sistemlerle ilgili mesleklerin mevcut ve gelecekteki olası durumları nelerdir?

- Yükseköğretim kurumlarında bulunan robotik lisans ve ön lisans programları nelerdir?

3. Robotik Sistemler

Robotik sistemler programlanabilen, belirli görevleri otonom veya yarı otonom olarak yerine getirebilen, mekanik, elektronik ve yazılımdan oluşan sistemlerdir. Bu sistemler çevresiyle etkileşim kurarak bilgi toplayan, topladığı bilgileri işleyen, bunun neticesinde çeşitli işlemler gerçekleştirebilen makinalardır.

Genellikle insanlar tarafından programlanan ve belirli kurallar çerçevesinde çalışabilen robotik sistemlerin yanı sıra yapay zekâ kullanarak öğrenme yeteneğine sahip robotik sistemler de bulunmaktadır.

Özellikle günümüzün en popüler teknolojik kavramlarından olan yapay zekâ ile gelişim gösteren robotik sistemlerin gelecekte hayatımızda daha çok yer alacağı, yalnızca üretim süreçlerinde değil günlük rutin işlemlerde de daha çok kullanılacağını söylemek mümkündür.

Robotik sistemlerin bileşenleri, buna bağlı olarak kullanım alanları farklılık göstermektedir. Bu bölümde robotik sistemlerin bileşenleri, kullanım alanları, avantajları ve robotik sistemlerdeki gelişmeler ele alınmıştır.

3.1. Robotik Sistemlerin Bileşenleri

Robotik sistemler, karmaşık sistemler olmasına karşın temelde 5 bileşenden meydana gelmektedir; mekanik sistemler, algılama sistemleri, kontrol sistemi, güç kaynağı ve aktüatörler. Bu bileşenler robotların hareket etmesini, hareket ettiği çevreyi algılayabilmesini, kendisinden beklenen çeşitli görev ve işlevleri yerine getirmesini sağlayan bileşenlerdir.

- Mekanik sistemler, robotun fiziksel yapısını oluşturan gövde, kollar, bacaklar, eklemler ve hareket mekanizmaları parçalarından oluşmaktadır. Gövde, robotun ana yapısıdır ve diğer tüm bileşenleri destekler. Kollar, bacaklar, eklemler ve hareket mekanizmaları, robotun hareket etmesini sağlamasının yanı sıra hareket kabiliyet ve sınırlılıklarını belirleyen unsurlardır.
- Algılama sistemleri, robotun kamera, lidar, ultrasonik sensör, dokunma sensörü ve GPS gibi algılayıcılar vasıtasıyla çevresi hakkında bilgi toplayabilmesini sağlar. Bu veriler mesafe, ışık veya sıcaklık verileri olabilir.
- Kontrol sistemi yazılım ve donanımdan oluşur. Kontrol sisteminde robot hareketlerinin planlanması, karar verme süreçleri ile robot

davranışlarının ve hareketlerinin yönetilmesi gerçekleşir. Robotun beyni olarak isimlendirilen mikroişlemcide tüm işlemler kontrol edilir ve diğer bileşenlerle iletişim sağlanır. Sensörlerden gelen veriler işlenir; bu veriler robotun istenilen görevleri yerine getirmesini sağlayacak şekilde anlamlı hale getirilir.

- Güç kaynağı, robotun çalışması için gerekli olan enerjiyi sağlayan birimdir. Güç kaynağı olarak genellikle pil, güneş enerji paneli veya harici enerji sistemleri tercih edilmektedir. Güç kaynakları robotların mobil veya sabit olmasına göre farklılık göstermektedir. Mobil robotlarda pil veya batarya; sabit robotlarda ise güç kaynağı kullanılmaktadır.
- Aktüatörler mekanik, elektrikli, hidrolik veya pnömatik motorlarla mekanik yapı sistemine güç sağlayan ve hareket kazandıran cihazlardır.

3.2. Robotik Sistemlerin Kullanım Alanları

Robotik sistemlerin günümüzde birçok sektörde çeşitli görevleri yapmak üzere kullanıldığı görülmektedir. Teknolojik gelişmelerle beraber robotik sistemlerin kullanımı da artmıştır. Dahası endüstride ilk kullanılmaya başlandığında rutin işlemleri gerçekleştiren robotlar artık robotik sistemlere dönüşmüştür. Bunun neticesinde daha karmaşık işlemleri gerçekleştirilebilen, yalnızca bir iş için değil başka işlemleri gerçekleştirmek üzere de programlanabilen, tek başına veya insanlarla iş birliği içinde ve yan yana çalışabilen kolaboratif robotlar (cobot) gerek üretimde gerekse diğer alanlarda daha görünür olmuştur. Dahası; önceleri yalnızca fabrikalardaki üretim süreçlerinde yer alan robotik sistemler artık günlük hayatta da kullanılmaya başlanmıştır.

Endüstri, sağlık, uzay ve askeri alanda; ev ve servis işlemlerinde robotik sistemlerin kullanımına rastlamak mümkündür. Örneğin; endüstride üretim süreçlerine ilişkin montajlama, kaynak yapma, boyama ve kalite kontrol işlemlerinde kullanılabilmektedir. Sağlık sektöründe robotik sistemlerin kullanım örnekleri mevcuttur. Öyle ki; cerrahi işlemlerde kullanılan robotlar, robotik cerrahi isminde alan yazında kendine yer bulmuştur. Bunlarla birlikte uzay araştırmalarında da keşif ve araştırma yapmak amacıyla robotlar kullanılmaktadır. Askeri alanda arazi keşfi, bomba imhası ve güvenlik devriyesi gibi işlemlerde robotik sistemlerden faydalanılmaktadır. Evlerde kullanılan temizlik ve mutfak robotları ise yoğun, yorucu ve stresli iş temposuna sahip bireylerin hayatlarını kolaylaştırır niteliktedir. Ayrıca, yaşlı veya bakıma muhtaç bireylerin hizmetlerini sağlamak amacıyla da robotların kullanıldığı görülmektedir.

3.3. Robotik Sistemlerin Avantajları

Doğrudan ve dolaylı birçok avantajı olmasına karşın robotik sistemlerin genel olarak avantajları şu şekildedir;

- Verimlilik, üretkenlik ve kalite: İnsanların aksine robotların kesintisiz çalışabilmesi sayesinde üretkenlik ve üretim kapasitesi arttırılmış olur. Robotlar, özellikle tekrarlayan işlemlerde hızlı ve hatasız işlem yapma kabiliyetlerine sahiptirler. Böylece işlemlerde hata azalır; üretim işlemlerinde tutarlılık, verimlilik ve kalite artar.
- Güvenlik: Robotların tehlike barındıran işlemlerde insanların yerine kullanılmasıyla olası risklerin minimize edilmesi ve insan sağlığının korunması sağlanır. Ayrıca insan hayatı için tehlikeli olan yüksek ısı, radyasyon veya kimyasal riskler içeren ortamlarda da kullanılarak iş kazaları önlenmiş olunur.
- Esneklik: Robotları çeşitli görevleri ve süreçleri yerine getirip gerçekleştirmek için tasarlamak ve programlamak mümkündür. Çok amaçlı kullanıma uygun olan robotlar, farklı sektörlerde farklı görevleri gerçekleştirebilir.
- Maliyet: Robotik sistemler, insana olan ihtiyacı azaltacağı için maliyetlerin düşürülmesine de katkı sağlar. Bununla birlikte insana oranla daha düşük hata oranı ve uzun süre aynı hassasiyette çalışabilme kabiliyeti neticesinde üretim süreçlerinde malzeme israfını da minimize eder.

3.4. Robotik Sistemlerdeki Gelişmeler

Robotik sistemler makine, mekatronik, bilgisayar, yazılım, kontrol ve otomasyon mühendisliklerini bünyesinde barındırmaktadır. Bu alanlarda ve teknoloji alanındaki gelişmelere paralel olarak robotik sistemlerde de gelişme görülecektir.

Daha önceleri rutin işlemler için kullanılan robotik sistemlerin günümüzde farklı bir noktaya evrildiği; kullanım alanlarının günden güne genişlediği gözlenmektedir. Özellikle yapay zekâ alanındaki gelişmeler, makinalar düşünebilir mi sorusuna yanıt verir niteliktedir.

Çok uzak olmayan gelecekteki hedeflerden biri de robotların insan seviyesine yakın zekaya sahip olmasıdır. Yapay zekâ alanındaki gelişmeler, bu süreci hızlandıracak en önemli etkenlerdendir. Bunun neticesinde daha akıllı robotları daha sık görmek mümkün olabilir.

Geliştirilen derin öğrenme ve makine öğrenmesi algoritmalarının robotik sistemlere entegre edilmesiyle robotların çevrelerini daha iyi tanımaları ve anlamaları, yeni durumları fark edebilmeleri, anomalileri belirleyebilmeleri, buna uygun çıkarımlar yapabilmeleri ve karar verebilmeleri robotik sistemleri güçlü kılacak özelliklerdendir.

Doğal dil işleme alanındaki gelişmeler, kullanıma açılan yapay zekâ teknolojileri ve uygulamaları neticesinde robotların insanlarla etkileşime geçebilmelerinin yolu açılmış bulunmaktadır. Robotların insanları anlaması ve hatta insanların duygu durumlarını belirleyerek buna uygun tepkiler vermesi, günlük yaşantıda robotlara daha sık rastlanacağının ve onların sosyal beceriler kazanabileceğinin işaretleri olarak görülebilir.

Daha hassas sensörlerle donatılan ve görüntü işleme yöntemlerini kullanan robotlar, çevrelerini daha iyi tanıma imkanına kavuşmuş olacaklardır. Bunun bir sonucu olarak robotlar etrafındaki objeleri daha iyi tanıyıp tespit edebilecek; böylece yüksek başarımlı ve daha güvenli işlemler gerçekleştirebileceklerdir.

Malzeme kalitesindeki iyileştirmeler, beraberinde robotları meydana getiren mekanik parçaların daha hafif ve dayanıklı olmasını sağlayacaktır. Öte yandan robotların modüler tasarlanarak farklı görevleri yerine getirecek şekilde üretilmeleri ve bu yeterliliklere sahip olmaları kullanımlarının yaygınlaşmasına katkı verecektir. Tüm bunların geliştirilmesi, iyileştirilmesi, düzenlenmesi ve tasarlanması, robotik sistemlerin bugün kullanıldığından daha geniş bir alanda kullanılmasını mümkün hale getirecektir.

4. Robotik Sistemlerle İlgili Mesleklerin Geleceği

Teknolojik gelişmeler, dönemi içerisinde bazı mesleklere olan ihtiyacı ortadan kaldırabileceği gibi bazı yeni mesleklerin de ortaya çıkmasına neden olur. Robotik sistemlerdeki gelişmeler insan gücüne dayalı işlemlerin ortadan kalkmasına sebebiyet verebilir. Özellikle tekrarlayan işlemlerde insanların yerini robotların alacağını söylemek mümkündür. Fakat günümüzde robotların henüz bütün işlemleri tek başına gerçekleştirebilecek yeterliliklere sahip olmadığını belirtmek gerekir. Bu bakımdan rutin işlemlerde robotlar kullanılabilecek olsa da daha karmaşık ve stratejik işlemlerin insanlar tarafından gerçekleştirileceği, robotların insana ihtiyacı tamamen ortadan kaldırmayacağı, ancak insanlarla iş birliği içerisinde çalışabilecek bir iş modelinin geliştirilebileceği veya yeni iş alanlarının ortaya çıkabileceği ifade edilebilir.

Robotik sistemlerin kullanımının yaygınlaşmasıyla gelecekte robot mühendisi, robotik teknisyeni, robotik eğitmeni, robotik uzmanı, robotik

etik uzmanı, yapay zekâ uzmanı, iş gücü analisti, otonom araç mühendisi, veri bilimci ve daha farklı mesleklerinin ortaya çıkabileceği, bu mesleklere olan ihtiyacın artacağı söylenebilinir.

Robotik sistemlerin hayatımıza girmesi ve iş gücü piyasasında yaygınlaşmasıyla robotla ilgili mesleklerde dinamik bir süreç yaşanacağı, bu meslekleri yapmak isteyenlerin sürekli kendilerini geliştirmelerinin gerekeceği vurgulanmalıdır.

5. Yükseköğretimde Robotik Programlar

Çalışmada robotik sistemlerin tanıtımlarının yanı sıra yükseköğretim lisans ve ön lisans düzeyindeki robotik programlarının genel durumlarının incelenmesi de gerçekleştirilmiştir. Bu amaçla program sayıları ile kontenjan ve yerleşen öğrenci sayıları verileri sunulmuştur.

Yükseköğretim Kurulu (YÖK) bünyesinde lisans ve ön lisans düzeyinde adında robotik geçen birer program bulunmaktadır. Lisans düzeyinde "Robotik ve Otonom Sistemleri Mühendisliği" programında (YÖK Program Atlası, 2024a); ön lisans düzeyinde ise "Robotik ve Yapay Zekâ" programında eğitim-öğretim faaliyeti yürütülmektedir (YÖK Program Atlası, 2024b).

5.1. Lisans Programları

Lisans düzeyindeki Robotik ve Otonom Sistemleri Mühendisliği programının bulunduğu üniversite, kontenjan ve yerleşen öğrenci sayıları Tablo 1'de verilmiştir. Lisans düzeyinde yalnızca İstanbul Teknik Üniversitesi'nde eğitim verilmekte olup, Türkçe ve İngilizce olarak yürütülen programın toplam kontenjan ve yerleşen öğrenci sayısı 82'dir.

Tablo 1. Robotik ve Otonom Sistemleri Mühendisliği Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
İstanbul Teknik Üniversitesi (İngilizce)	41	41
İstanbul Teknik Üniversitesi	41	41

Yükseköğretim Kurulu Başkanı Prof. Dr. Erol Özvar'ın "Kontrol ve Otomasyon Mühendisliği" programının adını "Robotik ve Otonom Sistemler Mühendisliği" olarak değiştirilmesine yönelik çalışmalara başlandığını bildirmesi sebebiyle her iki isimdeki program çalışmaya dahil edilmiştir (YÖK, 2024). Yıldız Teknik Üniversitesi'ndeki Kontrol ve Otomasyon Mühendisliği programının henüz adının değişmediği, Tablo 2 incelendiğinde bu programda Türkçe ve İngilizce eğitim verildiği, doluluk oranınınsa %100 olduğu görülmektedir.

Tablo 2. Kontrol ve Otomasyon Mühendisliği Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
Yıldız Teknik Üniversitesi (İngilizce)	57	57
Yıldız Teknik Üniversitesi	77	77

5.2. Ön Lisans Programları

Ön lisans düzeyindeki Robotik ve Yapay Zekâ programının bulunduğu üniversite, kontenjan ve yerleşen öğrenci sayılarına ait veriler Tablo 3'te sunulmuştur. Programa ilk olarak 2024 yılında öğrenci alınmaya başlanmıştır. 6 farklı üniversitede bulunan bu programdaki toplam kontenjan sayısı 203, doluluk oranı ise %100'dür. Ayrıca, Türkçe eğitim verilen bu programın tümü ücretsiz ve örgün olarak devlet üniversitelerinde faaliyet göstermektedir.

Tablo 3. Robotik ve Yapay Zekâ Ön Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
Eskişehir Teknik Üniversitesi	32	32
Gaziantep Üniversitesi	40	40
Harran Üniversitesi	40	40
Kocaeli Üniversitesi	32	32
Sakarya Uygulamalı Bilimler Üniversitesi	27	27
Trakya Üniversitesi	32	32

Robotik ve Otonom Sistemleri Mühendisliği ile Kontrol ve Otomasyon Mühendisliği lisans programlarının aksine, ön lisans düzeyindeki programların isimlerini henüz değiştirmediği; 2024 itibariyle Kontrol ve Otomasyon Teknolojisi adında 28 programın bulunduğu; bunların 2 tanesinin vakıf üniversitesinde (Tablo 4), 1 tanesinin de KKTC uyruklu adaylar için (Tablo 5) olduğu tespit edilmiştir. Bunlar dışında yer alan 25 devlet üniversitesindeki tüm programlarda (Tablo 6) Türkçe dilinde örgün eğitim verildiği ve genel kontenjanlar itibariyle programların tam olarak dolduğu belirlenmiştir.

Tablo 4. Vakıf Üniversitelerindeki Kontrol ve Otomasyon Teknolojisi Ön Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
Başkent Üniversitesi (Burslu)	6	6
Başkent Üniversitesi (%50 indirimli)	8	8

Tablo 5. KKTC Uyruklular İçin Kontrol ve Otomasyon Teknolojisi Ön Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
Kocaeli Üniversitesi	1	1

Tablo 6. Devlet Üniversiteleri Kontrol ve Otomasyon Teknolojisi Ön Lisans Programı (2024)

Üniversite	**Kontenjan**	**Yerleşen**
Akdeniz Üniversitesi	59	57
Artvin Çoruh Üniversitesi	42	42
Balıkesir Üniversitesi	37	37
Bilecik Şeyh Edebali Üniversitesi	32	32
Burdur Mehmet Akif Ersoy Üniversitesi	42	42
Düzce Üniversitesi	37	37
Ege Üniversitesi	31	31
Gazi Üniversitesi	41	41
Gaziantep Üniversitesi	40	40
İskenderun Teknik Üniversitesi	52	51
İstanbul Üniversitesi-Cerrahpaşa	62	62
Kayseri Üniversitesi	54	54
Kırıkkale Üniversitesi	54	52
Kırklareli Üniversitesi	32	32
Kocaeli Üniversitesi	54	53
Konya Teknik Üniversitesi	42	41
Manisa Celâl Bayar Üniversitesi	54	53
Marmara Üniversitesi	52	52
Mersin Üniversitesi	42	42
Necmettin Erbakan Üniversitesi	22	22
Nevşehir Hacı Bektaş Veli Üniversitesi	32	31
Pamukkale Üniversitesi	42	42
Sinop Üniversitesi	32	31
Tekirdağ Namık Kemal Üniversitesi	42	42
Zonguldak Bülent Ecevit Üniversitesi	37	36

6. Sonuç

Bu çalışmada robotik sistemler, bu sistemlerin bileşenleri, kullanım alanları, avantajları, robotik sistemlerdeki gelişmeler, robotik sistemler mesleğinin geleceği ile yükseköğretimdeki robotikle ilgili programların incelenmesi gerçekleştirilmiştir.

Her dönemde bazı mesleklerin ortadan kalktığı, bazı yeni mesleklerin ortaya çıktığı, bazı mesleklerin popüler olduğu, bazı mesleklere olan ilginin ise azaldığı görülebilmektedir. Konu, bu çalışmanın konusu olan robotik sistemler açısından değerlendirildiğinde robotik sistemlerin popülaritesinin arttığı söylenebilir. Robotik sistemler, bugün yalnızca üretim bantlarında görev yapan değil; günlük hayatta da kullanımına sıkça rastlanan makinalara dönüşmüştür. Örneğin, evlerde kullanılan temizlik robotları, insan hayatını kolaylaştıran ve zaman kazandıran özellikleri sayesinde birçok kişi tarafından tercih edilmektedir.

Kullanım alanı yalnızca evlerdeki bazı işlemlerin gerçekleştirilmesinden ibaret olmayan robotik sistemler, geniş kullanım alanına sahiptir. Bugün itibariyle endüstride, sağlıkta, uzay araştırmalarında ve askeri işlemlerde kullanılıyor olsa da gelecekte robotik sistemlerin daha da yaygınlaşacağını söylemek mümkündür.

Robotik sistemlerin üretimde verimlilik, üretkenlik ve kaliteyi arttırmaları; insan sağlığı ve hayatının tehlikeye atacak durumlarda kullanılabilme potansiyelleri; birden fazla işi yapacak şekilde tasarlanmaları ve programlanabilmeleri; insana olan ihtiyacın ortadan kalkmasını sağlayacak nitelikte olmaları ve bunun da maliyetlerin düşürülmesini sağlaması gibi doğrudan veya dolaylı çeşitli avantajları bulunmaktadır.

Gerek malzeme kalitesi gerekse de yapay zekâ alanında yaşanacak gelişmeler, beraberinde robotik sistemlerin de gelişmesini sağlayacak etkenlerdendir. Robotların derin öğrenme ve makine öğrenmesi algoritmalarını kullanmalarının yanı sıra daha hassas ekipmanlarla donatılmaları, çevresiyle uyumlu robotların ortaya çıkmasına katkı sağlayabilir. Ayrıca; robotların doğal dil işleme tekniklerini kullanmaları, insan-robot etkileşiminin seviyesini belirlemesi ve robotların insan benzeri davranışlar sergileyebilen görünüme kavuşması açısından önemlidir.

Robotik sistemler, üretimde ağırlıklı olarak sürekli tekrarlayan işlemlerde kullanılsalar da henüz bütün işlemleri tek başına yapacak düzeyde değillerdir. Bu sebeple en azından belirli bir zaman robotların insanlarla birlikte çalışması gerektiği söylenebilir. Ancak, robotik sistemlerin kabiliyetleri ve karar verme yetenekleri geliştiğinde durum farklılaşabilir. Öyle olduğunda

ise robot mühendisi, robotik teknisyeni, robotik eğitmeni, robotik uzmanı, robotik etik uzmanı mesleklerinin yanında şu andan öngörülemeyen yeni mesleklerin ortaya çıkması muhtemeldir.

Yükseköğretimde lisans düzeyinde Robotik ve Otonom Sistemleri Mühendisliği, ön lisans düzeyinde ise Robotik ve Yapay Zekâ programları bulunmaktadır. Adı 2024 yılında değişen ve İstanbul Teknik Üniversitesi'nde faaliyet gösteren Robotik ve Otonom Sistemleri Mühendisliği programında Türkçe ve İngilizce eğitim verilmektedir. 2024 yılında kurulan ve 6 farklı üniversitede öğrenci kabulü yapan ön lisans düzeyindeki Robotik ve Yapay Zekâ programında ise yalnızca Türkçe olarak eğitim-öğretim yürütülmektedir. Lisans ve ön lisans düzeyindeki tüm programların doluluk oranı %100'dür. Bu bilgiler ışığında, robotik programlarının açılması veya mevcutların revize edilmesi yönünde bir trend olduğu; üniversite adaylarının robotik programlarına olan ilgisinin yüksek olduğu ifade edilebilir.

Kaynakça

Akbaba, A. İ., & Gündoğdu, Ç. (2021). Bir servis robotu olarak telepresence (Uzabulunum) robotlar. *Pamukkale Üniversitesi İşletme Araştırmaları Dergisi*, *8*(2), 649-667. https://doi.org/10.47097/piar.1026348

Görçün, Ö. F. (2018). Lojistikte teknoloji kullanımı ve robotik. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *10*(24), 351-368. https://doi.org/10.20875/makusobed.397373

Işık, A. H., Alakuş, F., & Eskicioğlu, Ö. C. (2021). Hayvancılıkta robotik sistemler ve yapay zekâ uygulamaları. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *9*(6), 370-382. https://doi.org/10.29130/dubited.1015406

Kural, A. R., & Atuğ, F. (2010). Ürolojide robotik cerrahi uygulamaları. *Türk Üroloji Dergisi*, *36*(3), 248-257. https://urologyresearchandpractice.org/content/files/sayilar/10/buyuk/248-2571.pdf

Özfirat, M. K. (2009). Robotik sistemler ve madencilikte kullanımının araştırılması. *TÜBAV Bilim Dergisi*, *2*(4), 412-425. https://dergipark.org.tr/en/pub/tubav/issue/21517/230897

Peçe, F., Yarar, E., & Karabay, S. (2020). PID ve bulanık mantık kontrol sistemleri ile iki tekerlekli kendini dengeleyebilen robotik sistem tasarımı. *Kocaeli Üniversitesi Fen Bilimleri Dergisi*, *3*(1), 99-108. https://dergipark.org.tr/en/pub/koufbd/issue/52411/669175

Sivri, E. (2023). Kütüphanelerde yapay zekâ'nın geleceği: Farklı alanlardaki potansiyel uygulamalar ve yeni kullanım alanları oluşturma. *Library Archive and Museum Research Journal*, *4*(2), 175-184. https://doi.org/10.59116/lamre.1299783

YÖK (2024). https://www.yok.gov.tr/Sayfalar/Haberler/2024/yapay-zeka-dijitallesme-buyuk-veri-yeni-programlar.aspx (E.T.: 04.10.2024).

YÖK Program Atlası (2024a). Lisans Tercih Sihirbazı. https://yokatlas.yok.gov.tr/tercih-sihirbazi-t4.php (E.T.: 02.10.2024).

YÖK Program Atlası (2024b). Ön Lisans Tercih Sihirbazı. https://yokatlas.yok.gov.tr/tercih-sihirbazi-t3.php (E.T.: 02.10.2024).

Bölüm 2

Nesnelerin İnterneti (IoT)

Ali Erbey[1]

Özet

Bu çalışmada, günlük yaşamdan endüstriyel süreçlere kadar geniş bir uygulama yelpazesinde kullanılan nesnelerin İnterneti (IoT) teknolojisinin tanımı, bileşenleri ve uygulama alanları ele alınmıştır. Çalışmada, IoT kavramının toplumsal ve endüstriyel boyutlarda yarattığı dönüşüm ele alınmış, konuyla ilgili bilgi edinmek isteyen akademik çevreler ile profesyonellere kapsamlı bir analiz sunulması hedeflenmiştir. Ayrıca, IoT'nin teknolojik altyapısı, uygulama alanları ve sunduğu yenilikler ışığında, dijitalleşen dünyada yaşanan değişimlerin anlaşılmasına katkı sağlamayı, alan yazına ve profesyonel uygulamalara önemli bir referans olmayı amaçlamaktadır. Çalışmada akıllı ev sistemlerinde cihazların uzaktan kontrolü, tarımda akıllı sulama sistemleri ile verimlilik sağlanması ve sağlık sektöründe uzaktan hasta takibi gibi örneklerle bu teknolojiye olan talep ve faydalar açıklanmıştır. IoT'nin sunduğu verimlilik ve otomasyon avantajlarının yanı sıra güvenlik ve gizlilik konularına dikkat çekilmiştir. IoT cihazlarının siber saldırılara karşı savunmasız olabileceği belirtilmiş, güvenlik önlemlerinin artırılmasının gerekliliği vurgulanmıştır. IoT'nin topluma katkılarının artarak devam etmesi için güvenlik ve gizlilik politikalarının güçlendirilmesi gerektiğine değinilmiştir.

1. Giriş

Nesnelerin İnterneti (IoT), cihazların internete bağlı olduğu ve veri alışverişi yapabildiği bir sistemdir. (Paul & Jeyaraj, 2019). Bu kavram, günlük yaşamda kullanılan aletlerin, cihazların ve sistemlerin birbirleriyle iletişim kurabilme yeteneğini ifade etmektedir. IoT sensörler, yazılımlar ve diğer teknolojilerin bir araya gelmesiyle, nesnelerin akıllı hale gelmesini sağlar. Örneğin, bir buzdolabı, içindeki yiyeceklerin durumunu takip ederek kullanıcıya bilgi verebilmekte veya bir akıllı termostat, enerji tasarrufu sağlamak için ortam sıcaklığını otomatik olarak ayarlayabilmektedir.

1 Öğretim Görevlisi, Uşak Üniversitesi, Uzaktan Eğitim Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, ORCID: 0000-0002-0930-4081, ali.erbey@usak.edu.tr

https://doi.org/10.58830/ozgur.pub498.c2090

IoT endüstriyel, ticari ve kişisel birçok alanda değişikliklere yol açmaktadır (Zheng, Apthorpe, Chetty, & Feamster, 2018). Özellikle son yıllarda ortaya çıkan akıllı ev teknolojileri, kullanıcıların evdeki cihazları uzaktan kontrol etmelerine olanak tanımaktadır. Kişiler evlerinin aydınlatma, güvenlik sistemleri ve ısıtma gibi unsurlarını, mobil uygulamalar veya sesli komutlarla yönetebilmektedir. IoT ile evler yönetilebilirken şehirler de yönetilebilmektedir. Bu sayede IoT, şehirlerin daha verimli ve yaşanabilir hale gelmesine yardımcı olmaktadır. Trafik yönetim sistemleri, çevre izleme, enerji yönetimi gibi uygulamalar, şehirlerin kaynaklarını daha etkin bir şekilde kullanmasını sağlamaktadır.

Sağlık sektöründe ise IoT hasta takibi, uzaktan sağlık hizmetleri ve acil durum yönetimi gibi alanlarda kullanılmaktadır (Scarpato, Pieroni, Di Nunzio, & Fallucchi, 2017). Giyilebilir cihazlar, kullanıcıların sağlık verilerini izleyerek doktorlarla paylaşmalarına olanak tanımaktadır.

Tarımda verimliliği artırmak için kullanılan akıllı sulama sistemleri ve sensörler gibi çözümler sunar (Mekala & Viswanathan, 2017; Ruan et al., 2019). Bu uygulamalar su ve enerji tasarrufu sağlarken ürün kalitesini de artırmaktadır. Ayrıca, üretim süreçlerini optimize etmek için veri toplama ve analiz etme yeteneği sunarak sanayi devriminde önemli bir rol oynamaktadır. Akıllı fabrikalar, otomatikleştirilmiş üretim hatları ve uzaktan izleme sistemleri gibi uygulamalar, maliyetleri düşürürken verimliliği artırmaktadır.

IoT'nin bu alanlardaki etkisi daha akıllı, daha verimli ve daha sürdürülebilir bir geleceği mümkün kılmaktadır. Ancak, bu teknolojilerin benimsenmesiyle birlikte gelen zorluklar ve güvenlik endişelerinin de dikkate alınması gerekmektedir.

1.1. IoT Nedir?

IoT, fiziksel nesnelerin internete bağlanarak veri toplama, iletme ve işleme yeteneğine sahip olduğu bir sistemdir. Bu kavram, dünya genelinde milyonlarca cihazın birbirleriyle iletişim kurmasını, veri alışverişinde bulunmasını ve etkileşimde bulunmasını mümkün kılar.

IoT, çeşitli bileşenlerden oluşur. Bunlar arasında sensörler, yazılımlar, bağlantı teknolojileri ve veri analizi yöntemleri yer alır. IoT sistemlerinin temel yapı taşları sensörler ve aktüatörlerdir. Sensörler, çevresel verileri toplar (sıcaklık, nem, ışık düzeyi vb.) ve aktüatörler bu verileri kullanarak fiziksel değişiklikleri yapabilir (örneğin, bir motoru çalıştırmak). Bu iş ve işlemlerin gerçekleşebilmesi için bütün cihazların birbirleri ile bağlantı halinde olması gerekmektedir.

Bağlantı protokolleri ile IoT cihazlar birbirleriyle ve internet ile iletişim kurabilmektedir. Bu protokoller Wi-Fi, Bluetooth gibi çeşitli teknolojileri içerebilir (Salman & Jain, 2019). Bağlantı halindeki bu cihazlardan elde edilen veriler bulut veya yerel sunucularda analiz edilerek veri işleme ve analiz sürecine tabi tutularak anlamlı bilgilere dönüştürülür. Bu işlem, kullanıcıların karar verme süreçlerine yardımcı olabilecek yapıyı sağlamaktadır. Tüm bu süreçler kullanıcıların etkileşimde olabildiği kullanıcı arayüzleri ile gerçekleşmektedir. Bu arayüzler kullanıcıların IoT cihazları yönetmelerine ve izlemelerine olanak tanımaktadırlar. İyi yapılandırılmış mobil uygulamalar, web arayüzleri veya sesli asistanlar gibi arayüzler ise kullanıcı deneyimini artırmaktadır (Ahn & Park, 2018).

1.2. IoT'nin Önemi ve Etkisi

IoT, günümüzde hem bireysel hem de kurumsal düzeyde önemli değişimlere ve yeniliklere yol açmaktadır. IoT, süreçleri otomatikleştirerek insan müdahalesini azaltmakta ve verimliliği artırmaktadır. Cihazlar, gerçek zamanlı veri toplama ve izleme yeteneği sayesinde, kullanıcıların durumu anında değerlendirmesine olanak tanırlar ve toplanan veriler, daha bilinçli ve veri odaklı kararlar alınmasına yardımcı olur. Böylece kaynak kullanımı optimize edilerek maliyetler düşebilmektedir.

Bireysel olarak insan yaşantısı üzerindeki etkilerine bakıldığında konfor ve kolaylık sağlaması, kişiselleştirilmiş deneyimler ile yapılandırılmış ortamın yaratılması, sağlık süreçlerinin izlenebilirliğinin sağlanması ilk etapta karşımıza çıkan etkiler olarak söylenebilir. Akıllı evler, akıllı termostatlar konfor ve kolaylığı sağlarken alışkanlıklara ve ruhsal durumlara göre müzik ve film önerileri kişiselleştirilmiş deneyimleri sağlamaktadır. Giyilebilir cihazlar ise erken teşhis süreçleri gerçekleştirilebilmesi, böylece bireylerin sağlık durumlarının takibi sağlamaktadır. Bu vb. süreçler IoT'nin bireysel düzeyde önemine vurgu yapmaktadır.

IoT kurumsal düzeyde verimlilik ve üretkenlik, maliyet tasarrufu ve karar verme süreçlerinde önemli roller oynamaktadır. Endüstriyel IoT uygulamaları, üretim süreçlerini otomatikleştirerek verimliliği artırmakta gerçek zamanlı veri analizi yaparak süreçlerdeki aksaklıkların hızlı bir şekilde tespit edilmesine ve çözülmesine olanak tanımaktadır. Maliyet tasarrufu konusunda, IoT sistemleri, enerji tüketimini izleyerek maliyetleri düşürme fırsatları sunmaktadır. Özellikle akıllı enerji yönetimi, işletmelerin enerji israfını azaltmalarını sağlamaktadır. Karar verme süreçlerinde ise, büyük veri analitiği ile desteklenen karar verme süreçlerini iyileştirmektedir. İşletmeler, topladıkları verileri analiz ederek stratejik kararlar alabilir ve pazardaki değişimlere hızlı bir şekilde yanıt verebilmektedir.

IoT'nin ekonomik etkilerine bakıldığında ise, en önemli etkisi yeni iş modellerinin ortaya çıkmasıdır. IoT, birçok sektörde yeni iş fırsatları ve modellerinin ortaya çıkmasına sebep olmaktadır. Son yıllarda ürünlerin uzaktan izlenmesi ve yönetilmesi, "as a service" (hizmet olarak) iş modelinin yaygınlaşmasına yol açmıştır (Asir, Manohar, Anandaraj, & Sivaranjani, 2016). Bu vb. iş olanakları istihdam fırsatı olarak yansımaktadır. IoT'nin büyümesi, yazılım geliştirme, veri analizi, siber güvenlik gibi alanlarda yeni istihdam fırsatları yaratmaktadır. Bu durum, iş gücü piyasasında dönüşüme yol açmaktadır.

IoT'nin çevresel etkilerine baktığımızda sürdürülebilirlik ön plana çıkmaktadır. IoT uygulamaları, kaynakların daha verimli kullanılmasına olanak tanır. Akıllı tarım sistemleri su ve enerji tüketimini optimize ederken tarımsal verimlilik artmaktadır. Aynı zamanda çevresel etkilerde atık yönetimi düzenleyebilmektedir. Akıllı şehir projeleri, atık yönetimini optimize etmek için sensörler kullanarak atık miktarını izleyebilmektedir. Böylece, geri dönüşüm oranlarını artırılabilmekte ve çevresel etkileri azaltılabilmektedir.

Son yıllarda gelişen yapay zekâ, makine öğrenimi ve veri analitiği gibi teknolojilerle entegrasyon, daha akıllı ve etkileşimli sistemlerin ortaya çıkmasına yol açmaktadır. Teknolojik bağlamda olumlu etkisi olarak bakılabilecek bu süreçler varken aynı zamanda IoT'nin yaygınlaşması, siber güvenlik tehditlerini de beraberinde getirmektedir. Cihazların güvenliği, veri gizliliği ve güvenlik protokolleri üzerinde ciddi çalışmalar yapılması gerekmektedir.

IoT, bireyler işletmeler ve toplumlar için önemli fırsatlar sunarken aynı zamanda bazı zorlukları da beraberinde getirmektedir. IoT ile verimli, sürdürülebilir bir dünya oluşturulabilir. Ancak, bu teknolojilerin güvenli bir şekilde kullanılması ve olası risklerinde önüne geçilmesi gerekmektedir.

2. Nesnelerin İnterneti Tarihçesi

2.1. İlk Yıllar

IoT kavramı teknoloji ve iletişimdeki köklü gelişmelerin bir yansıması olarak ortaya çıkmıştır. IoT'nin temelleri, 1960'lı yıllarda bilgisayar ağlarının gelişmesiyle atılmıştır. Bu dönemde, bilgisayarlar arası veri paylaşımı ve iletişimin sağlanmasına yönelik çalışmalar yoğunlaşmıştır. Özellikle ARPANET (Advanced Research Projects Agency Network), modern internetin temelini atan ve bilgisayarlar arasında iletişimi mümkün kılan ilk ağ sistemi olarak öne çıkmıştır (Roberts, 1988).

1982 yılında Carnegie Mellon Üniversitesi'nden bir grup mühendis, bir Coca-Cola otomatını uzaktan izleyebilen bir sistem geliştirmiştir (England, 2020). Bu otomat, içeceklerin sıcaklıklarını ve stok durumlarını internet üzerinden gösteren internete bağlı ilk akıllı cihaz olma özelliğine sahiptir. Bu gelişme, fiziksel nesnelerin internetle bağlantı kurma potansiyelini ortaya koyarak IoT'nin yolunu açmıştır.

1999 yılında MIT'den Kevin Ashton, "Nesnelerin İnterneti" terimini ilk kez kullanarak fiziksel nesnelerin internet aracılığıyla veri toplayabileceği ve iletişim kurabileceği fikrini ortaya atmıştır (Ashton, 2009). Ashton'ın bu kavramsallaştırması, özellikle RFID (Radyo Frekansı ile Tanımlama) teknolojisinin gelişmesiyle ivme kazanmış ve nesnelerin izlenmesi ve tanımlanmasında devrim yaratmıştır.

2000'li yıllara gelindiğinde IoT uygulamaları hızla yaygınlaşmaya başlamıştır. 2005 yılında Uluslararası Telekomünikasyon Birliği (ITU), IoT'yi geleceğin iletişim paradigması olarak tanıtmış ve bu süreçte çeşitli kuruluşlar IoT teknolojileri için standartlar ve protokoller geliştirmeye başlamıştır. Bu standartlar, cihazların birbirleriyle uyum içinde çalışabilmelerini sağlamış ve IoT'nin yaygınlaşmasını hızlandırmıştır.

Günümüzde, IoT'nin etkisi her alanda hissedilmektedir. Akıllı evler, sağlık hizmetleri, tarım ve endüstri gibi birçok sektörde IoT uygulamaları aktif olarak kullanılmaktadır. 5G teknolojisi ve yapay zekâ entegrasyonu, IoT'nin gelecekteki gelişimini hızlandıracak önemli faktörlerdir. Bu teknolojilerin birleşimi, daha akıllı ve etkileşimli sistemlerin oluşmasına olanak tanıyacaktır.

IoT teknoloji ve iletişim alanındaki önemli gelişmelerin bir sonucu olarak ortaya çıkmıştır. İlk dönemlerde ortaya çıkan temel kavramlar ve teknolojiler, günümüzdeki gelişmeleri şekillendirmiştir. IoT'nin tarihçesi, bu alandaki yeniliklerin ve uygulamaların daha iyi anlaşılmasına yardımcı olmaktadır.

2.2. Teknolojik İlerlemeler

IoT teknolojisinin gelişimi, çeşitli yenilikçi teknolojik ilerlemelere dayanır. Bu gelişmeler, IoT'nin ana bileşenlerinin ve uygulamalarının oluşumunda önemli bir etki yaratmıştır. İnternet ve ağ teknolojilerindeki gelişmeler, süreci hızlandıran etkilerden biridir. Özellikle internetin gelişimi, IoT'nin en temel bileşenlerinden biridir. 1980'lerde başlayan ARPANET, sonrasında TCP/IP protokollerinin ortaya çıkması, cihazların veri iletimi için gerekli olan altyapıyı sağlamıştır. Bu ağ teknolojileri, IoT cihazlarının internete bağlanmasını ve veri paylaşımını mümkün kılmaktadır. İnternet ve ağ alt yapısının ardından donanımsal olarak mikroelektronik ve nanoteknoloji alanındaki ilerlemeler, daha küçük, daha ucuz ve daha hassas sensörlerin geliştirilmesine olanak

tanımıştır. Bu sensörler, fiziksel ortamdan veri toplama ve bu verileri işleme kapasitesine sahip olmaları sayesinde, IoT uygulamalarının yaygınlaşmasına öncü rol oynamaktadır.

Sensörlerin akıllı hale gelmesi ise, yerel verileri işleyebilme yeteneği kazanmaları ile mümkün olmuştur. Bu tür sensörler, bağlı oldukları sistemler üzerinde daha fazla kontrol sağlamaktadır. İnternet alt yapısı ile sensörler gelişirken radyo frekansı ile tanımlama (RFID) teknolojisi nesnelerin tanımlanması ve izlenmesi için önemli bir araç haline gelmiştir. 2000'li yıllarda RFID sistemlerinin maliyetinin düşmesi ve etkinliğinin artması perakende, lojistik ve sağlık sektörlerinde IoT uygulamalarının yaygınlaşmasına yardımcı olmuştur. RFID, fiziksel nesnelerin internet üzerinde tanımlanmasını ve izlenmesini kolaylaştırarak otomasyon süreçlerini hızlandırmıştır (Chen & Jin, 2012). Cihazların birbiri ile iletişimi artarken ortaya çıkan verilerin depolanması için yeni bileşenlerin devreye girmesi gerekmiş bunun çözüm için ise bulut bilişim ortaya çıkmıştır.

Bulut bilişim, IoT ekosisteminin kritik bir parçası haline gelmiştir. Cihazlardan gelen büyük veri yığınlarının işlenmesi ve saklanması için bulut altyapıları tercih edilmektedir. Bulut teknolojilerinin gelişimi, IoT uygulamalarının veri analitiği, depolama ve erişim konularında daha etkili bir şekilde kullanılmasını sağlamıştır. (Cai, Xu, Jiang, & Vasilakos, 2016). Bulut bilişim, cihazların veri paylaşımını kolaylaştırırken, ölçeklenebilirliği ve maliyet etkinliğini artırmaktadır. Bulut bilişim ile depolanan verilerin anlamlandırılması ve analiz edilmesi, işletmelerin daha bilinçli kararlar almasına olanak tanımaktadır. Veri analitiği teknolojilerinin gelişimi, IoT verilerinin daha etkili bir şekilde işlenmesini ve bu verilerden fayda sağlanmasını mümkün kılmıştır. Makine öğrenimi ve yapay zekâ, veri analitiği süreçlerini destekleyerek IoT uygulamalarını daha akıllı hale getirmiştir. Tüm bu süreçler, uygulamaları akıllı hale getirerek teknolojinin nihai amacı olan insan yaşamını kolaylaştırırken riskleri de beraber getirmektedir.

IoT'nin yaygınlaşmasıyla birlikte güvenlik ve veri gizliliği konuları daha da önem kazanmıştır. 2000'li yılların ortalarından itibaren IoT cihazları için özel güvenlik protokolleri ve şifreleme teknolojileri geliştirilmiştir. Bu teknolojiler, veri iletimi sırasında güvenliği artırmakta ve siber saldırılara karşı koruma sağlamaktadır.

Son yıllarda 5G teknolojisinin geliştirilmesi, IoT'nin hızını ve verimliliğini artırmak için önemli bir adım olmuştur. 5G, daha yüksek hız ve daha düşük gecikme süreleriyle daha fazla cihazın aynı anda bağlanabilmesine imkân tanımaktadır. Bu özellikler, IoT uygulamalarının daha geniş bir yelpazede kullanılmasını mümkün kılmaktadır. Ayrıca, LPWAN (Düşük Güç Geniş

Alan Ağı) gibi yeni iletişim protokolleri, IoT cihazlarının enerji verimliliğini artırarak uzun süreli kullanımı sağlamaktadır.

Teknolojik ilerlemeler, IOT'nin evrimini ve yaygınlaşmasını destekleyen temel unsurlardır. İnternet, sensör teknolojileri, bulut bilişim ve veri analitiği gibi alanlardaki gelişmeler, IoT'nin potansiyelini artırmakta ve çeşitli sektörlerde devrim niteliğinde değişikliklere yol açmaktadır. IoT'nin gelecekteki gelişimi, bu teknolojilerin entegrasyonu ve yenilikçi uygulamaların ortaya çıkması ile şekillenecektir.

IoT, günümüzde hızla gelişen bir teknoloji alanı haline gelmiştir. IoT uygulamaları, bireylerin günlük yaşamlarında, işletmelerin operasyonlarında ve kamu hizmetlerinde önemli bir rol oynamaktadır.

Bugün, dünya genelinde milyarlarca IoT cihazı bulunmaktadır. Akıllı telefonlar, akıllı ev aletleri, giyilebilir cihazlar, sensörler ve endüstriyel makineler gibi çeşitli ürünler, insanların yaşamlarını ve iş süreçlerini dönüştürmektedir. Örneğin, 2023 yılı itibarıyle, global IoT cihaz sayısının 30 milyardan fazla olduğu tahmin edilmektedir. Bu sayı, gelecekte daha da artması beklenen bir trendi yansıtmaktadır. IoT; akıllı ev teknolojileri, enerji yönetimi, güvenlik sistemleri, giyilebilir teknolojiler ve uzaktan sağlık izleme sistemleri, akıllı fabrikalar, akıllı tarım uygulamaları gibi birçok sektörde geniş uygulama alanlarına sahiptir. Bütün bu sektörlerde yer alan IoT küresel bir etkiye sahip olmaktadır.

Günümüzde IoT'nin küresel etkisi, iş süreçlerini dönüştürmekle kalmayıp, sosyal ve ekonomik yapıları da değiştirmektedir. IoT, gelişmekte olan ülkelerde ekonomik büyümeyi desteklerken, gelişmiş ülkelerde ise üretkenliği artırmaktadır. Ayrıca, IoT çözümleri, çeşitli sosyal sorunlara çözüm üretme potansiyeline sahip olabilir; trafik yönetimi, enerji tasarrufu ve sağlık hizmetlerinin iyileştirilmesi vb.

IoT, günümüzde birçok sektörde önemli bir yer tutmakta ve bireylerin yaşamlarını dönüştürmektedir. Ancak, bu teknolojinin yaygınlaşmasıyla birlikte güvenlik ve gizlilik konularında da dikkatli olunması gerekmektedir. IoT'nin geleceği teknoloji ve inovasyonun birleşimiyle şekillenecek ve daha akıllı, sürdürülebilir bir dünya yaratma potansiyeli sunacaktır.

3. Temel Bileşenler

3.1. Sensörler ve Aktüatörler

IoT sistemlerinin temel bileşenleri arasında sensörler ve aktüatörler önemli bir yer tutmaktadır. Bu bileşenler, fiziksel dünyayı algılamak, verileri

toplamak ve bu verilere dayalı olarak eylem gerçekleştirmekte kritik rol oynamaktadır.

Sensörler, çevresel verileri toplamak ve bu verileri dijital forma dönüştürmek için kullanılan cihazlardır. Sensörlerin belirli sınırlılıkları olsa da (Sinche et al., 2020) çeşitli ölçümler yapılabilmektedir. Sensörler, çeşitli fiziksel değişkenleri ölçebilir ve bu ölçümleri belirli bir arayüz üzerinden iletebilmektedirler.

Sensörlerin farklı türleri bulunmaktadır. Sıcaklık sensörleri, ortam sıcaklığını ölçebilirler ve genellikle HVAC sistemlerinde kullanılırlar. Nem sensörleri, havadaki nem oranını ölçerek iklim kontrol sistemlerinde kullanılırlar. Işık sensörleri, ortamın aydınlık düzeyini belirler ve akıllı aydınlatma sistemlerinde kullanılırlar. Hareket sensörleri, fiziksel hareketi algılar ve güvenlik sistemlerinde yaygın olarak kullanılırlar. Basınç sensörleri, hava basıncını ölçerek meteorolojik uygulamalarda kullanılırlar.

Sensörler, fiziksel çevrelerinden aldıkları verileri elektrik sinyallerine dönüştürür. Bu sinyaller daha sonra IoT sistemlerine iletilir, burada analiz edilir ve gerekli eylemler gerçekleştirilir. Örneğin, bir sıcaklık sensörü ortamın sıcaklığını algılayarak bu bilgiyi bir bulut sunucusuna gönderebilir.

Aktüatörler ise sensörlerden gelen verileri işleyerek fiziksel değişiklikler yapan cihazlardır. Sensörler tarafından sağlanan bilgiye dayalı olarak belirli bir eylemi gerçekleştirebilirler. Genellikle mekanik veya elektriksel güç kullanarak hareket ederler.

Aktüatörlerinde sensörler gibi farklı türleri bulunmaktadır. Elektrik motorları, dönme hareketi sağlamak için elektrik enerjisini mekanik enerjiye dönüştürebilirler. Hidrolik ve pnömatik aktüatörler, sıvı veya gaz basıncı kullanarak hareket sağlamaktadırlar. Isıtıcılar, ortamın sıcaklığını artırmak için kullanılırlar. Valfler, akış kontrolü sağlar, örneğin, su veya gaz akışını açma/kapama işlevi görür.

Aktüatörler, belirli bir kontrol sinyalini alarak fiziksel bir hareket gerçekleştirirler. Örneğin; bir termostatın sıcaklık sensörü, ortamın sıcaklığı belirli bir seviyenin altına düştüğünde ısıtıcıyı açmak için bir aktüatör sinyali gönderir. Bu şekilde, ortam sıcaklığı istenen seviyeye getirilir.

Sensörler ve aktüatörler, IoT sistemlerinin temel bileşenleri olarak kritik bir rol üstlenmektedir. Veri toplama sürecinde sensörler, çevresel koşulları sürekli izleyerek veri toplar. Bu veriler, IoT sistemlerinin karar alma süreçlerine temel teşkil eder. Otomasyon ve kontrol sürecinde aktüatörler, sensörlerden gelen verileri kullanarak otomatik eylemler gerçekleştirir. Bu, sistemlerin verimliliğini artırarak insan müdahalesini azaltır. Gerçek zamanlı

izleme sürecinde ise sensörler ve aktüatörler birlikte çalışarak, kullanıcıların ortamı gerçek zamanlı olarak izlemelerine ve yönetmelerine olanak tanır. Akıllı sistemlerin ortaya çıkmasında ise sensörler ve aktüatörler ile sistemler akıllı ve etkileşimli hale gelmektedir. Bu, enerji tasarrufu, güvenlik ve konfor gibi alanlarda önemli faydalar sunmaktadır

Sensörler ve aktüatörler, IoT sistemlerinin temel bileşenleridir. Bu bileşenler, fiziksel verilerin toplanması ve bu verilere dayalı eylemlerin gerçekleştirilmesi için kritik bir rol oynamaktadır. IoT uygulamalarında sensörler ve aktüatörler verimlilik, otomasyon ve akıllı kontrol sistemleri sağlamak için vazgeçilmez unsurlardır.

3.2. Bağlantı Protokolleri

IoT sistemlerinde, cihazların kendi aralarında ve bulut hizmetleriyle verimli bir şekilde iletişim kurmasını sağlamak için bağlantı protokolleri hayati bir önem taşımaktadır. Bu protokoller, veri iletiminde kullanılan kurallar ve standartlar setidir (Salman & Jain, 2019; Sinche et al., 2020). Farklı IoT uygulamaları için uygun bağlantı protokolü seçimi, sistemin verimliliği ve güvenliği açısından büyük önem taşımaktadır. Bu protokoller Wi-Fi, Bluetooth, Zigbee, MQTT olabilir.

3.2.1. Wi-Fi

Wi-Fi, kablosuz ağ iletişimi için en yaygın kullanılan protokollerden biridir. Yüksek veri hızları ve geniş alan kapsama alanı sunar. Yüksek veri aktarım hızı, geniş bir kullanıcı kitlesi ve destek mobil cihazlarla uyumluluğu avantajı olarak ön plana çıkarken enerji tüketiminin yüksek olması, kapsama alanının çevresel faktörlere bağlı olması dezavantajları olarak görülmektedir. Özellikle enerji tüketiminin yüksek olmasından dolayı pil ile çalışan cihazlarda önerilmez. Akıllı ev cihazları, Wi-Fi ile bağlı kamera sistemleri ve ofis otomasyonlarında kullanılmaktadır.

3.2.2. Bluetooth

Bluetooth, kısa mesafeli kablosuz iletişim için tasarlanmış bir protokoldür. Genellikle düşük enerji tüketimi ile öne çıkar. Düşük enerji tüketimi (Bluetooth Low Energy-BLE), kolay bağlantı ve düşük maliyet, kısa mesafelerde yüksek veri aktarım hızı avantajları olarak öne çıkarken kapsama alanın sınırlı olması (genellikle 10-100 metre) dezavantaj olarak görülmektedir. Giyilebilir cihazlar, akıllı telefonlarla bağlantılı aksesuarlar, ev otomasyonu sistemlerinde kullanılmaktadır.

3.2.3. Zigbee

Zigbee, az enerji tüketimi ve düşük veri aktarım hızları için geliştirilmiş bir kablosuz haberleşme protokolüdür. Düşük enerji tüketimi, uzun pil ömrü sağlaması, ağa bağlı cihaz sayısının yüksek olması (binden fazla cihaz), mesh topolojisi sayesinde genişletilebilir kapsama alanının olması avantajlarıdır. Dezavantajları ise düşük veri aktarım hızlarının olmasıdır. Akıllı aydınlatma sistemleri, ev otomasyonu, enerji izleme sistemlerinde kullanılmaktadır.

3.2.4. LoRaWAN (Long Range Wide Area Network)

LoRaWAN, düşük güç tüketimi ile uzun mesafelerde veri iletimi için tasarlanmış bir protokoldür. Genellikle şehirlerde ve kırsal alanlarda geniş alanlar için kapsama alanı sağlar. Uzun mesafelerde (10-15 km) veri iletimi, düşük enerji tüketimi ve büyük veri setlerini destekleme kapasitesi, avantajları olarak ön plana çıkmaktadır. Dezavantajları ise düşük veri aktarım hızı ve kapsama alanı için özel altyapı gerektirmesidir. Tarım, çevre izleme, akıllı şehir uygulamaları, akıllı sokak lambaları gibi uygulamalarda LoRaWAN protokolü tercih edilebilmektedir.

3.2.5. MQTT (Message Queuing Telemetry Transport)

MQTT, düşük bant genişliği ve yüksek gecikmeye dayanıklılık gerektiren IoT uygulamaları için geliştirilmiş bir haberleşme protokolüdür. Diğer bağlantı protokollerine göre avantajları olarak; düşük enerji tüketimi ve bant genişliği kullanımı, iletim güvenliği ve bağlantı güvenilirliği ve yaygın olarak kullanılması söylenebilir. Yüksek bant genişliği gerektiren uygulamalarda uygun olmaması ise dezavantajı olarak değerlendirilebilir. Akıllı ev sistemleri, sanayi otomasyonu ve sağlık izleme alanlarında kullanılmaktadır.

3.2.6. CoAP (Constrained Application Protocol)

CoAP, kısıtlı kaynaklara sahip cihazlar için geliştirilmiş bir haberleşme protokolüdür. RESTful mimariye dayalıdır ve düşük güç tüketimi ile çalışır (Ansari, Rehman, & Ali, 2018). Düşük güç tüketimi, iyi bir performans sunması ve web standartları ile uyumlu olması diğer avantajları olarak görülmektedir. Kapsama alanı ve veri aktarım hızının sınırlı olması ise dezavantajı bağlamında değerlendirilebilir. Akıllı ev uygulamaları, sensör izleme sistemlerinde kullanılmaktadır.

Bağlantı protokolleri, IoT sistemlerinin başarısı için hayati öneme sahiptir. Uygulamanın gereksinimlerine uygun bir protokol seçimi, sistemin performansını ve güvenliğini doğrudan etkiler. Her protokolün kendi

avantajları ve dezavantajları bulunmaktadır. Bu nedenle, IoT uygulamalarında doğru seçim yapılması önemlidir.

3.3. Veri Yönetimi ve Analitiği

IoT sistemleri, büyük miktarda veri üretir. Bu verilerin etkili bir şekilde yönetilmesi ve analiz edilmesi, IoT uygulamalarının başarısı için kritik öneme sahiptir (Mohindru, Mondal, & Banka, 2020). Veri yönetimi ve analitiği, toplanan verilerin anlamlandırılması, kullanılabilir bilgiye dönüştürülmesi ve karar alma süreçlerinde kullanılmasını sağlayan süreçlerdir.

IoT sistemleri sensörler ve cihazlar aracılığıyla sürekli olarak veri toplar. Bu veriler, çeşitli kaynaklardan gelir ve gerçek zamanlı, tarihsel veya etiketlenmiş veriler olabilir. Sensörlerden ve cihazlardan anlık olarak alınan verilere (örneğin, sıcaklık, nem, basınç) gerçek zamanlı veriler denilmektedir. Zamanla toplanan ve saklanan veriler tarihsel bağlamda değerlendirilebilir. Bu veriler, geçmiş eğilimlerin analizi için önemlidir. Cihazlar tarafından üretilen ve belirli bir anlam veya bağlam taşıyan veriler ise etiketlenmiş verilerdir. Bu verilerin toplama süreci, veri kaynağından (sensör, cihaz) verilerin uygun formatta toplanmasını ve sistemin veri tabanına veya bulut ortamına iletilmesini içermektedir.

Toplanan verilerin güvenli bir şekilde depolanması gerekmektedir. IoT sistemleri genellikle bulut depolama, yerel depolama veya hibrit depolama yöntemlerini kullanır. Bulut depolama, yüksek hacimli verilerin depolanmasını ve işlenmesini mümkün kılan merkezi bir sistemdir. Bulut hizmet sağlayıcıları, veri yedekleme, erişim ve analiz gibi olanaklar sunmaktadır. Yerel depolama, cihazların kendi belleklerinde veri saklamasıdır. Bu, hızlı erişim ve düşük gecikme süresi sağlar; ancak veri kaybı riski taşımaktadır. Hibrit depolama ise hem bulut hem de yerel depolama sistemlerinin kombinasyonunu içerir. Kritik veriler yerel olarak saklanırken, daha az önemli veriler buluta aktarılmaktadır. Aktarılan ve depolanan bu bilgiler veri işleme sürecinde anlamlandırılmaktadır.

Veri işleme, toplanan verilerin anlamlandırılması ve kullanılabilir bilgiye dönüştürülmesi sürecidir. Bu süreçte gerçek zamanlı işleme, büyük veri analizi veya veri madenciliği teknikleri kullanılmaktadır. Gerçek zamanlı işleme, anlık olarak verilerin anında analiz edilmesini ifade etmektedir. Örneğin, bir sıcaklık sensörü, belirli bir eşiğin üstüne çıktığında alarm vermek için kullanılabilir. Büyük ve karmaşık veri setlerinin işlenmesi için gerekli olan analiz yöntemleri ise büyük veri analizi ile gerçekleşmektedir.

Apache Hadoop ve Apache Spark gibi araçlar, büyük veri analizi için yaygın olarak kullanılan araçlardır (Nazari, Shahriari, & Tabesh, 2019).

Verilerden gizli kalıpların ve ilişkilerin ortaya çıkarılması süreci ise veri madenciliği yöntemleri ile gerçekleştirilir. Veriler işlendikten sonra veri analitiği sürecine geçilir.

Veri analitiği, işlenmiş verilerin analiz edilerek karar alma süreçlerine katkıda bulunmasıdır. IoT uygulamalarında sıkça kullanılan analitik türleri tanımlayıcı analitik, tahminsel analitik ve preskriptif analitiktir. Tanımlayıcı analitik, geçmiş verileri inceleyerek mevcut durumu anlamaya yönelik analizdir şeklidir. Örneğin, önceki enerji tüketim verileri ile mevcut tüketim karşılaştırılarak mevcut durumu anlama sürecine gidilebilir. Tahminsel analitik, geçmiş verilere dayanarak gelecekteki eğilimlerin tahmin edilmesine yardımcı olan analiz şeklidir. Örneğin, bir cihazın arıza süresini tahmin etmek için geçmiş veriler kullanılabilir. Preskriptif analitik ise olası sonuçları değerlendirerek en iyi kararların alınmasını öneren analizdir. Örneğin, enerji tüketimini azaltmak için en uygun stratejileri belirlemek gibi.

Veri yönetimi ve analitiği, IoT sistemlerinin verimliliğini artırmak ve daha bilinçli kararlar almak için kritik öneme sahiptir. Toplanan verilerin doğru bir şekilde işlenmesi ve analiz edilmesi, IoT uygulamalarının etkinliğini artırarak bireyler ve işletmeler için değer yaratabilir.

4. Uygulama Alanları

4.1. Akıllı Evler

Akıllı ev teknolojileri, kullanıcıların konforunu artırmak ve enerji verimliliğini sağlamak amacıyla evdeki cihazların uzaktan kontrol edilmesine olanak tanır. Akıllı ev sistemleri çeşitli sensörler, aktüatörler ve bağlantı protokolleri kullanarak günlük yaşamı daha pratik ve güvenli hale getirir. Kullanıcılar, aydınlatma sistemlerini mobil uygulamalar aracılığıyla kontrol edebilirler. Işıkların otomatik olarak açılıp kapanması veya belirli bir zamanda belirli bir aydınlatma seviyesinin ayarlanması gibi özellikler, enerji tasarrufu sağlayabilir.

Akıllı kameralar ve hareket sensörleri, evin çevresini sürekli izleyerek anlık bildirimler gönderebilir. Kullanıcılar, uzaktan erişimle kameraların görüntülerini izleyebilir ve güvenlik durumunu kontrol edebilirler. Akıllı termostatlar, evin sıcaklığını dış hava koşullarına göre otomatik olarak ayarlar. Bu, hem konforu artırır hem de enerji maliyetlerini düşürebilir.

Bu tür sistemlerin kurulumu, kullanıcıların yaşam kalitesini artırırken enerji tüketimini optimize ederek çevresel sürdürülebilirliğe katkıda bulunur.

4.2. Akıllı Şehirler

Akıllı şehirler, şehirlerin yönetiminde teknoloji ve IoT uygulamalarının entegrasyonu ile daha verimli ve sürdürülebilir bir yaşam alanı oluşturmayı hedeflemektedir. Bu uygulamalar, şehir kaynaklarının yönetimini kolaylaştırırken vatandaşların yaşam kalitesini artırmaktadır. Akıllı trafik ışıkları, gerçek zamanlı veri analizi ile trafik akışını optimize ederek trafik yönetimini sağlayabilmektedir. Sensörler, trafik yoğunluğunu algılar ve ışık sürelerini buna göre ayarlar. Bu, sıkışıklığı azaltır ve ulaşım sürelerini kısaltmaktadır. Akıllı çöp kutuları, doluluk seviyesini izleyerek belediyelere ne zaman boşaltılması gerektiğini bildirmektedir. Bu, atık toplama maliyetlerini azaltarak ve çevre dostu bir yaklaşım sağlamaktadır.

Akıllı şebekeler, enerji tüketimini optimize etmek için IoT cihazlarından gelen verileri kullanarak verimli bir enerji yönetimi gerçekleştirebilmektedir. Bu sistemler, enerji talebini dengeleyerek maliyetleri düşürürken, yenilenebilir enerji kaynaklarının entegrasyonunu artırmaktadır. Akıllı şehir uygulamaları hem yönetim verimliliğini artırır hem de yaşam alanlarını daha yaşanabilir hale getirmektedir.

4.3. Sağlık Hizmetleri

IoT, sağlık sektöründe önemli dönüşümlere neden olmaktadır. Uzaktan sağlık izleme sistemleri, giyilebilir cihazlar ve veri analitiği, sağlık hizmetlerinin kalitesini artırmakta ve hasta bakımını iyileştirmektedir. Kalp atış hızı, kan basıncı ve fiziksel aktivite gibi sağlık verilerini izleyen giyilebilir cihazlar, kullanıcıların sağlık durumlarını sürekli takip etmelerini sağlar. Kronik hastalığı olan bireyler sağlık verilerini evlerinden çıkmadan takip edebilirler. Doktorlar, hastalarının durumunu izleyebilir ve gerektiğinde hızlı bir şekilde müdahale edebilirler.

Hastaneler, IoT uygulamaları sayesinde hasta kayıtlarını ve tıbbi cihazları daha etkin bir şekilde yönetebilir. Sensörler, cihazların durumunu izleyerek bakım süreçlerini optimize edebilir. Bu ve vb. uygulamalar ile sağlık hizmetlerinde IoT, hastaların yaşam kalitesini artırırken, sağlık sistemlerinin verimliliğini de yükseltmektedir.

4.4. Tarım

IoT uygulamaları, tarım sektöründe verimliliği artırmak ve kaynakları daha etkin kullanmak noktasında önemli bir rol oynamaktadır. Akıllı tarım çözümleri, çiftçilere gerçek zamanlı veri sağlamaktadır. Akıllı sulama sistemleri ile toprak nem sensörleri, sulama ihtiyaçlarını belirler ve otomatik sulama sistemlerini yönetmektedir. Bu, su tasarrufu sağlarken bitkilerin

ihtiyaç duyduğu suyu da garanti eder. Hava durumu sensörleri, sıcaklık, nem ve rüzgâr hızı gibi verileri toplayarak çiftçilere bilgi sağlamaktadır. Bu veriler, tarım uygulamalarının optimize edilmesine yardımcı olmaktadır.

Tarım makinelerine entegre edilen sensörler, ürünlerin verimini izlemektedir. Bu veriler, çiftçilere doğru hasat zamanını belirlemeleri konusunda yardımcı olmaktadır. Tarımda IoT uygulamaları, sürdürülebilir tarım uygulamalarını teşvik ederken gıda güvenliğini artırır ve ekonomik kazanç sağlar.

4.5. Endüstriyel Uygulamalar

IoT, endüstriyel sektörde devrim niteliğinde değişikliklere yol açmaktadır. Akıllı fabrikalar, veri analitiği ve otomasyon sistemleri ile daha verimli üretim süreçleri sunmaktadır. Endüstriyel makineler, sensörler aracılığıyla sürekli olarak izlenir. Bu, bakım gereksinimlerinin önceden tahmin edilmesini sağlar ve arıza sürelerini azaltır.

Enerji tüketimini izleyen sistemler, enerji verimliliğini artırmak için kullanılabilir. Bu sistemler, enerji tüketimini optimize ederek maliyetleri düşürür. IoT otomasyon sistemleri ve robot teknolojilerinin entegrasyonunu artırır. Bu, üretim süreçlerini hızlandırır ve hataları azaltır. Endüstriyel uygulamalarda IoT, verimliliği artırmakta ve maliyetleri düşürmektedir. Bu da rekabetçi endüstride önemli avantajlar elde edilmesini sağlar.

5. Güvenlik ve Gizlilik

5.1. IoT Sistemlerinde Güvenlik Sorunları

IoT sistemleri veri iletimi ve cihazlar arası iletişim açısından büyük potansiyele sahipken bu sistemlerin güvenliği ile ilgili birçok sorun da taşımaktadır. Bu sorunlardan biri zayıf veya varsayılan kimlik bilgilerinin kullanılmasıdır. Birçok IoT cihazı, zayıf veya varsayılan kimlik bilgileri ile korunmaktadır. Bu durum, yetkisiz kullanıcıların cihazlara kolaylıkla erişmesine olanak tanıyabilmektedir. Bir diğer güvenlik açığı veri iletimi güvenliğinin tam sağlanmamasıdır. IoT cihazları arasında veri iletimi sırasında, verilerin şifrelenmemesi veya yetersiz şifrelenmesi, siber saldırganların verilere erişmesine ve bu verileri manipüle etmesine neden olabilmektedir. Bir diğer güvenlik açığı ise güncellemelerin ihmal edilmesidir. IoT cihazları için yazılım güncellemeleri genellikle ihmal edilmektedir. Güvenlik açıklarını kapatacak güncellemelerin yapılmaması, cihazların saldırılara karşı daha savunmasız hale gelmesine yol açmaktadır. Son güvenlik açığı ise fiziksel güvenlik açığıdır. Birçok IoT cihazı, fiziksel olarak kolayca erişilebilen

yerlerde bulunmaktadır. Bu durum, kötü niyetli bireylerin cihazlara zarar vermesini veya verileri çalmasını kolaylaştırmaktadır.

5.2. Gizlilik Endişeleri

IoT sistemleri, bireylerin ve işletmelerin hassas verilerini toplamakta ve iletmektedir. Bu durum, gizlilikle ilgili önemli endişeleri beraberinde getirmektedir. Toplanan veriler kullanıcının izni olmadan kullanılabilir. Kullanıcıların davranışlarını ve alışkanlıklarını izlemek için toplanan veriler olabilir. Toplanan verilerin üçüncü şahıslarla paylaşılması, gizlilik ihlallerine yol açabilir. Kullanıcılar, verilerinin nerede ve nasıl kullanılacağını bilmeyebilir. IoT sistemleri yöneten kişilerin toplamış olduğu veriler, sistemi yönetenler tarafından kullanılabileceği gibi yetersiz güvenlik önlemleri, kişisel verilerin sızmasına neden olabilir. Bu, kullanıcıların mahremiyetinin ihlal edilmesine ve olumsuz sonuçlara yol açabilir.

6. Gelecek Trendleri

6.1. IoT'deki Yenilikler

Nesnelerin İnterneti (IoT) sürekli olarak evrim geçirirken, teknolojik yenilikler ve uygulama alanlarındaki gelişmeler, bu alanın geleceğini şekillendirmektedir. Önümüzdeki yıllarda sensörlerin daha hassas ve enerji verimli hale gelmesi beklenmektedir. Yeni nesil sensörler, daha geniş veri setlerini toplayarak kullanıcıların ihtiyaçlarını daha iyi anlamaya yardımcı olacaktır. Toplanan verilerin gelişmiş veri analitiği teknikleri ile daha etkili bir şekilde işlenebilmesi sağlanabilir. İşlenen veriler aracılığıyla otonom araçlar, insansız hava araçları ve robotlar gibi otonom sistemlerin IoT ile entegrasyonu artacaktır. Bu sistemler, kendi başlarına veri toplayabilir ve analiz edebilir, bu da çeşitli endüstrilerde verimliliği artıracaktır.

IoT cihazlarının sayısının artmasıyla birlikte, bağlantı protokollerinin ve iletişim yöntemlerinin daha da geliştirilmesi beklenmektedir. Yeni nesil bağlantı çözümleri, daha hızlı ve güvenilir iletişim sağlamak için tasarlanacaktır. Şehirlerin akıllı hale gelmesi için IoT çözümleri daha fazla kullanılacaktır. Akıllı trafik sistemleri, enerji yönetimi ve çevresel izleme gibi uygulamalar, şehirlerin daha sürdürülebilir ve yaşanabilir olmasına katkıda bulunacaktır.

6.2. 5G ve IoT

5G teknolojisi, IoT'nin geleceği üzerinde büyük bir etkiye sahip olacaktır. 5G, daha yüksek veri hızları ve düşük gecikme süreleri sunarak IoT cihazlarının daha hızlı ve etkili bir şekilde iletişim kurmasına olanak tanır.

Bu, gerçek zamanlı veri iletimini ve uygulama performansını artırır. 5G, aynı anda daha fazla IoT cihazının bağlanmasına olanak tanır. Bu, özellikle akıllı şehirler ve endüstriyel uygulamalar için önemlidir. Çünkü çok sayıda cihazın aynı anda çalışabilmesi gerekir. 5G, daha güvenilir bağlantılar sunarak IoT sistemlerinin güvenliğini artırır. Bu, kritik uygulamaların daha güvenilir bir şekilde çalışmasını sağlar. 5G, IoT cihazlarının enerji verimliliğini artırarak daha uzun pil ömrü sunar. Bu, özellikle giyilebilir cihazlar ve uzaktan izleme sistemleri için önemlidir. 5G, artırılmış gerçeklik (AR) ve sanal gerçeklik (VR) gibi yeni uygulamaların geliştirilmesine olanak tanır. Bu, IoT'nin çeşitli sektörlerde daha yenilikçi çözümler sunmasına yardımcı olacaktır.

6.3. Yapay Zekâ ile Entegrasyon

Yapay zekâ (YZ), IoT sistemlerinin gelişimini hızlandırmakta ve bu sistemlerin daha akıllı hale gelmesine olanak tanımaktadır. YZ, büyük veri setlerini analiz ederek desenleri tanıma ve tahmin yapma yeteneği sunabildiği için işletmelerin daha bilinçli kararlar almasına yardımcı olabilecektir. IoT sistemleri, YZ algoritmaları sayesinde otomatik olarak kararlar alabilir. Örneğin, bir enerji yönetim sistemi, enerji tüketimini optimize etmek için verileri analiz ederek otomatik olarak ayarlamalar yapabilecektir. YZ, makinelerin ve cihazların arıza olasılıklarını tahmin edebilir. Bu, bakım maliyetlerini azaltır ve arıza sürelerini en aza indirebilir.

YZ, kullanıcıların alışkanlıklarını analiz ederek kişiselleştirilmiş deneyimler sunar. Akıllı ev sistemleri, kullanıcıların tercihlerini öğrenerek otomatik olarak ayarlamalar yapabilir.

YZ, IoT sistemlerinin güvenliğini artırmak için tehditleri tespit etme ve anormal davranışları analiz etme yeteneğine sahiptir. Bu, siber saldırılara karşı daha etkili bir koruma sağlar.

Gelecek trendleri IoT'nin evrimini şekillendiren yenilikçi gelişmeler, 5G teknolojisi ve yapay zekâ ile entegrasyonun birleşimi olarak ortaya çıkmaktadır. Bu gelişmeler, IoT uygulamalarının daha akıllı, daha verimli ve daha sürdürülebilir hale gelmesine katkıda bulunacaktır. IoT'nin geleceği, bu teknolojilerin etkili bir şekilde entegrasyonuna bağlı olarak daha parlak bir yol haritası çizecektir.

7. Sonuç ve Öneriler

IoT, insanların yaşam tarzlarını, iş süreçlerini ve şehir yönetimini dönüştüren bir teknolojidir. IoT'nin geleceği, hızla gelişen teknolojik altyapılar, artan veri miktarları ve kullanıcıların ihtiyaçlarına yanıt verebilen akıllı sistemlerin entegrasyonu ile şekillenmektedir. 5G teknolojisinin

sağladığı hızlı ve güvenilir bağlantılar, IoT cihazlarının daha verimli bir şekilde çalışmasını sağlayarak yeni uygulama olanaklarını ortaya çıkarmaktadır. Ayrıca, YZ ile entegrasyon, IoT sistemlerinin daha akıllı hale gelmesine ve daha iyi karar alma süreçlerine olanak tanımaktadır.

Önümüzdeki yıllarda IoT'nin sağlık, tarım, enerji yönetimi ve akıllı şehir uygulamaları gibi alanlarda daha da yaygınlaşması beklenmektedir. Bu durum, sürdürülebilirlik ve verimlilik konularında önemli katkılar sunarak toplumsal fayda sağlayacaktır. Ancak, bu dönüşüm sürecinde güvenlik ve gizlilik sorunlarının çözülmesi, IoT'nin benimsenmesi ve etkinliği için kritik bir öneme sahiptir. Özellikle güvenlik önlemlerinin güçlendirilmesi gerekmektedir. IoT sistemlerinde güvenliği artırmak için cihaz üreticileri, yazılım geliştiricileri ve kullanıcılar arasında iş birliği sağlanmalıdır. Kullanıcıların bilinçlendirilmesi, güçlü kimlik doğrulama yöntemleri ve düzenli yazılım güncellemeleri gibi önlemler, güvenliği risklerini azaltabilir. Ayrıca kullanıcı verilerinin nasıl toplandığı, saklandığı ve kullanıldığı hakkında şeffaflık sağlanmalıdır. Veri gizliliği politikaları geliştirilerek kullanıcı güveni artırılmalıdır. Kullanıcılarda IoT teknolojileri hakkında eğitim programları ve farkındalık kampanyaları yapılmalı, kullanıcılarda bu programlara aktif olarak katılmalıdır. Hem kullanıcılar hem de geliştiriciler için bilgi ve beceri geliştirme fırsatları sağlanmalıdır.

IoT günden güne insanların yaşamında önemli yer edinmektedir. Bu bağlamda IoT alanında yeni teknolojilerin ve uygulamaların geliştirilmesi için daha fazla araştırma ve geliştirme çalışması yapılmalıdır. Bu yaklaşım, yenilikçi çözümlerin ortaya çıkmasını sağlayacak ve mevcut sorunlara daha iyi yanıtlar sunacaktır. Kişiler tarafından IoT'nin benimsenmesini destekleyecek politika ve düzenlemelerin oluşturulması gerekmektedir. Bu, kullanıcıların haklarını koruyarak güvenli ve sürdürülebilir bir ortam yaratılmasına katkıda bulunacaktır. IoT uygulamaları, sağlık, tarım, enerji ve ulaşım gibi çeşitli sektörlerde daha etkili hale gelmek için disiplinler arası iş birliğini gerektirmektedir. Bu iş birliği, sistemlerin entegrasyonunu ve veri paylaşımını kolaylaştıracaktır.

IoT bireyler, işletmeler ve toplum için büyük fırsatlar sunan bir teknoloji alanıdır. Ancak, bu fırsatların gerçekleşebilmesi için güvenlik, gizlilik ve sürdürülebilirlik konularına dikkat edilmesi gerekmektedir. IoT'nin geleceği, yenilikçi çözümler ve iş birlikleri ile daha parlak bir yol haritasına sahip olacaktır.

Kaynakça

Ahn, M., & Park, N. (2018). A Study on UI prototyping based on personality of things for interusability in IoT environment. *Journal of the HCI Society of Korea*, *13*(2), 31–44.

Ansari, D. B., Rehman, A.-U., & Ali, R. (2018). Internet of things (iot) protocols: a brief exploration of mqtt and coap. *International Journal of Computer Applications*, *179*(27), 9–14.

Ashton, K. (2009). That 'internet of things' thing. *RFID Journal*, *22*(7), 97–114.

Asir, T. R. G., Manohar, H. L., Anandaraj, W., & Sivaranjani, K. N. (2016). IoT as a service. In *International Conference on Innovations in information, Embedded and Communication Systems (ICIIECS)* (Vol. 3, pp. 1093–1096).

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet of Things Journal*, *4*(1), 75–87. https://doi.org/10.1109/JIOT.2016.2619369

Chen, X.-Y., & Jin, Z.-G. (2012). research on key technology and applications for internet of things. *Physics Procedia*, 33, 561–566. https://doi.org/10.1016/J.PHPRO.2012.05.104

England, S. K. (2020). *Internet of things device cybersecurity and national security*. Utica College.

Mekala, M. S., & Viswanathan, P. (2017). A Survey: Smart agriculture IoT with cloud computing. In *2017 international conference on microelectronic devices, circuits and systems (ICMDCS)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICMDCS.2017.8211551

Mohindru, G., Mondal, K., & Banka, H. (2020). Internet of things and data analytics: A current review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(3), e1341.

Nazari, E., Shahriari, M. H., & Tabesh, H. (2019). BigData analysis in healthcare: Apache hadoop, apache spark and apache flink. *Frontiers in Health Informatics*, *8*(1), e14. https://doi.org/10.30699/fhi.v8i1.180

Paul, A., & Jeyaraj, R. (2019). Internet of things: A primer. *Human Behavior and Emerging Technologies*, *1*(1), 37–47.

Roberts, L. (1988). The Arpanet and computer networks. In *A history of personal workstations* (pp. 141–172).

Ruan, J., Jiang, H., Zhu, C., Hu, X., Shi, Y., Liu, T., Chan, F. T. S. (2019). Agriculture IoT: Emerging trends, cooperation networks, and outlook. *IEEE Wireless Communications*, *26*(6), 56–63. https://doi.org/10.1109/MWC.001.1900096

Salman, T., & Jain, R. (2019). A survey of protocols and standards for internet of things. *ArXiv Preprint ArXiv:1903.11549*. https://doi.org/10.48550/arXiv.1903.11549

Scarpato, N., Pieroni, A., Di Nunzio, L., & Fallucchi, F. (2017). E-health-IoT universe: A review. *Management*, *21*(44), 46.

Sinche, S., Raposo, D., Armando, N., Rodrigues, A., Boavida, F., Pereira, V., & Silva, J. S. (2020). A survey of IoT management protocols and frameworks. *IEEE Communications Surveys and Tutorials*, 22(2), 1168–1190. https://doi.org/10.1109/COMST.2019.2943087

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–20. https://doi.org/10.1145/3274469

Bölüm 3

Siber Güvenliğin Temelleri: Tehditler, Koruma Yöntemleri, Açık Kaynak Yazılımlar, Yapay Zekâ ve Trend Analizleri ile Güvenlik Uyum Yönetimi

Hüseyin Parmaksız[1]

Özet

Bu çalışmada siber güvenliğin temelleri, güncel tehditler, korunma yöntemleri, açık kaynak yazılımlar, yapay zekâ uygulamaları ve trend analizleri incelenmektedir. Keycloak, PacketFence, Wazuh, OPNsense, Coroza ve OpenCTI gibi açık kaynak araçlarının güvenlik stratejilerindeki öneminin yanı sıra MITRE ATT&CK, OWASP ve NIST gibi çerçeveler vurgulanmaktadır. Yapay zekâ tehdit tespiti, anomali analizi ve otomatik yanıt sistemlerindeki potansiyeli ile hem savunma hem de saldırı amaçlı kullanılmaktadır. Yapay zekâ destekli eğitim programları güvenlik duvarlarının ve Web Uygulaması Güvenlik Duvarlarının (WAF) etkinliğini artırmaktadır. Bununla birlikte, çalışmada sosyal mühendislik saldırıları, şifre kırma ve deepfakes gibi kötüye kullanım potansiyeli de tartışılmaktadır. Python Pytrends kütüphanesi ve Google Trends verileri kullanılarak siber güvenlik trend analizleri gerçekleştirilmekte ve önemli siber güvenlik trendlerini belirlemek ve görselleştirmek için TF-IDF yöntemi kullanılmaktadır. Çalışmada ayrıca otonom siber güvenlik sistemleri, kuantum kriptografi ve gizliliği artıran teknolojilerin potansiyel etkileri de tartışılmaktadır. Güvenlik uyum yönetiminin rolü ile yapay zekâ ve makine öğreniminin gelecekteki potansiyel etkileri de incelenmektedir.

1. Giriş

Siber güvenlik, bilgi sistemlerini, ağları ve verileri güvence altına almak için kullanılan çeşitli yöntem ve teknolojilerin incelenmesidir. Siber güvenlik alanındaki en acil sorunlardan biri, bir sistemin güvenliğini ihlal etmeye yönelik kasıtlı girişimler olan siber tehditlerdir. Stallings'in (2018) belirttiği

1 Dr. Öğr. Üyesi, Bilecik Şeyh Edebali Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, ORCID: 0000-0001-8455-5625, huseyin.parmaksiz@bilecik.edu.tr

https://doi.org/10.58830/ozgur.pub498.c2091

üzere; saldırganlar hassas bilgileri çalmak veya yayınlamak için kötü amaçlı yazılım, fidye yazılımı, sosyal mühendislik ve veri ihlallerini kullanmaktadırlar. Veri ihlalleri, yetkisiz erişim nedeniyle hassas bilgilerin çalınması veya yayınlanmasını içerir ve istismar olasılığı yüksektir. Bilgisayar korsanlığı, kötü amaçlı amaçlarla bilgisayar sistemlerine yetkisiz erişim sağlama eylemi olarak ifade edilmektedir. Andress ve Winterfeld (2013) siber savaşın karmaşık yapısını ve bunun güvenlik uygulayıcıları üzerindeki etkilerini inceleyerek bu alandaki tehditlerin sürekli evrildiğini vurgulamaktadırlar. Siber güvenliğin temel amacı, bu tehditleri önlemek ve etkilerini en aza indirmektir.

Siber güvenlik teknolojileri ve teknik operasyonlar, sistem güvenliğini ve tehdit önlemeyi sağlamak için çok önemlidir. Şifreleme ve kriptografi, verilere yalnızca yetkili kullanıcılar tarafından erişilebilmesini sağlayan depolama teknolojileridir. Güvenlik duvarları, ağ bağlantılarını izlemek ve istenmeyen erişimi önlemek için temel güvenlik tekniklerini uygulamaktadır. Saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS), düşmanca süreçleri belirleyerek engellemektedir (Singh, 2023). Sıfırıncı gün güvenlik açıkları, saldırganlar için önemli bir fırsat sunmaktadır. Dağıtılmış hizmet reddi saldırıları (DDoS), yoğun trafik nedeniyle bir sistemi çalışmaz hale getirebilir. Kimlik doğrulama ve yetkilendirme, güvenlik sistemlerinde kritik kavramlardır (Zargar, Joshi, & Tipper, 2013); erişim kontrolü (AC) (De Capitani di Vimercati, Paraboschi, & Samarati, 2003), kaynaklara kimin erişebileceğini yönetmektedir. Bu yaklaşımlar ve teknolojiler, sistem güvenliği ve tehdit önlemenin temelini oluşturmaktadır.

Siber güvenlik planları ve politikaları, bir kuruluşun dijital varlıklarını korumak için kritik öneme sahiptir. Risk yönetimi, olası tehditleri tespit ederek bunları azaltmak için uygun önlemleri uygulamaktadır. Bir ihlal durumunda, hızlı bir şekilde yanıt vermek üzere tasarlanmış sistemlerle olay müdahalesi esastır. Yönetim kavramları siber güvenlik prosedürlerini yönetirken uyumluluk politikaları yasal ve düzenleyici standartları karşılamaktadır. Tehdit istihbaratı, olası riskleri belirleyerek bunlar hakkında bilgi verir ve proaktif güvenlik eylemlerini mümkün kılar. Siber güvenlik önlemleri siber saldırıları önlerken adli teknikler siber suçları araştırır ve failleri belirler. Bu süreçlerin başarısı, sistemlerin dayanıklılığına yakından bağlıdır. Gizlilik ilkeleri, kişisel verileri koruyarak kullanıcı güvenliğini ve gizliliğini vurgular. Bu stratejik teknikler, siber güvenlik yönetiminde kapsamlı bir savunma sağlamaktadır.

Akademik araştırma ve teknikler açısından, siber güvenlik uygulamalarının etkinliğini artırmak için oluşturulan birçok kavram ve teknik yaklaşım, mevcut güvenlik altyapılarının geliştirilmesinde hayati öneme sahiptir.

Çerçeve, bu uygulamaların metodik bir şekilde uygulanmasını garanti ederken; modelleme yaklaşımı tehdit ve sistem simülasyonu yoluyla olası güvenlik açıklarının erken keşfedilmesini sağlar. Simülasyon yaklaşımları, gerçek dünya durumlarını simüle ederek güvenlik sistemlerinin verimliliğini değerlendirmek için kullanılır.

Yapay zekâ (YZ) ve makine öğrenimi büyük veri analiziyle entegre edildiğinde riskleri otomatik olarak belirleyip sınıflandırarak insan müdahalesine olan ihtiyacı en aza indirerek siber güvenliği devrimleştirebilirler. Algoritmalar, büyük veri kümelerini değerlendirmek, olası riskleri belirlemek ve güvenlik süreçlerini geliştirmek için gereklidir. Dahası, YZ destekli tespit sistemleri, anormal faaliyetleri hızla tanıyarak güvenlik ihlallerini önlemek için mükemmel bir teknik sağlar. YZ sistemleri, saldırı türlerini tahmin ederek proaktif risk azaltımı sağlar. Bu entegre yaklaşım, siber güvenliğin sürekli değişen doğasını ele almak için gereken esnek ve dinamik çözümleri sunmaktadır.

Güncel siber güvenlik trendleri, teknoloji hızla ilerledikçe güvenlik yöntemlerini değiştirmektedir. Bulut güvenliği, bulut tabanlı hizmetleri korumak için teknikler uygulayarak veri gizliliği ve erişim kontrolü zorluklarına önemli katkılarda bulunmaktadır. Aynı zamanda, nesnelerin interneti (IoT) güvenliği, bağlantılı cihazların sayısının artması nedeniyle bu cihazların güvenliğini güvence altına almak için yeni yolların geliştirilmesini gerektirmektedir. Blockchain güvenliği, dağıtılmış defter teknolojisinin entegrasyonunu kolaylaştırdığı için veri bütünlüğünü sağlamak için mükemmel bir seçenek olmaktadır (Banerjee, Lee, & Choo, 2018). Buna karşılık; kuantum kriptografisi, klasik şifreleme yaklaşımlarından daha sağlam bir güvenlik mimarisi oluşturmak için kuantum mekanik kavramları kullanmaktadır. Siber güvenlikteki YZ, tehdit algılama ve yanıt operasyonlarını otomatikleştirerek güvenlik analistlerinin verimliliğini artırmaktadır. Sıfır Güven Mimarisi, varsayılan olarak her kullanıcıya ve cihaza güvenmeme yaklaşımını benimseyerek güvenlik duvarlarını geliştirmektedir. Siber-fiziksel sistemlerin fiziksel ve dijital dünyalara entegrasyonu yeni güvenlik endişeleri yaratır; bu ortamda, uç bilgi işlem güvenliği, veri işleme ve depolama faaliyetlerini güvence altına almak için önemli bir konu olarak ortaya çıkmaktadır. Ayrıca, içeriden gelen saldırılar ve gelişmiş sürekli tehditler (APT), siber güvenlik çözümlerini karmaşık hale getirir (Chen, Desmet, & Huygens, 2014). Bu dinamik ve karmaşık değişimler, siber güvenliğin sürekli değişen doğasını yansıtarak daha dayanıklı ve uyarlanabilir güvenlik çözümlerine olan ihtiyacı vurgulamaktadır.

2. Siber Güvenlikte Tehditler ve Koruma Yöntemleri

Saldırı vektörleri, sistemlere, ağlara veya cihazlara yetkisiz erişim elde etmek için kullanılan siber tehditlerdir. Kötü amaçlı yazılım, kimlik avı, zayıf parolalar ve sosyal mühendislik gibi taktikler kullanarak güvenlik açıklarını, insan hatalarını ve zayıflıkları hedef almaktadır (Stallings & Brown, 2015). Bu vektörleri anlamak, tehditleri erken tespit etmek ve etkili güvenlik önlemleri geliştirmek için çok önemlidir (Sunit & Nina, 2011). Saldırılara karşı korunmak için güçlü parolalar, çok faktörlü kimlik doğrulama, düzenli yazılım güncellemeleri, siber güvenlik eğitimi ve güvenli ağ bağlantılarının kullanılması gerekmektedir. Özellikle Wi-Fi ağlarının güvenliğini artırmak için güçlü şifreleme yöntemleri kullanılmalı, misafir ağları ayrı bir yapılandırma ile yönetilmeli ve ağda bağlı cihazların birbirinden izole edilmesi sağlanmalıdır.

Ayrıca, etkili bir güvenlik stratejisi için log kayıtları düzenli olarak tutulmalı (Schmidt, Phillips, & Chuvakin, 2012); bu kayıtlar, 5651 sayılı Kanun (Türkiye Cumhuriyeti, 2007) kapsamında gerektiği gibi günlüklerin saklanarak, geriye dönük tespit ve faillerin belirlenmesi için önemli bir kaynak oluşturmalıdır. Kod analizi süreçlerinde ise açık kaynak ve lisanslı ürünler kullanılarak programlama dillerine özgü güvenlik açıklarının tespit edilmesi hedeflenmelidir (McGraw, 2012). Bu savunmaları tanımak ve uygulamak, sağlam bir siber güvenlik stratejisinin önemli bir parçasıdır.

2.1. Tehditler

Siber güvenlikte tehditler, sistemlere yönelik saldırıları ve bilgi hırsızlığı girişimlerini içermektedir. Bu tehditlerle başa çıkmanın iki temel yöntemi; saldırgan güvenlik ve savunma güvenliğidir (Melis v.d., 2023). Saldırgan güvenlik stratejileri, sistemlerdeki zayıflıkları tespit edip gidermeyi amaçlayan proaktif yöntemler kullanmaktadır. Bu kapsamda penetrasyon testi, sosyal mühendislik saldırıları ve uygulama güvenliği testleri gibi yöntemler öne çıkmaktadır. Bu yaklaşımlar, sistemlerdeki olası zafiyetleri keşfetmek için yapılan saldırı simülasyonlarına dayanmaktadır.

Saldırı vektörleri, siber saldırganların bir ağa, sisteme veya cihaza zarar vermek ya da yetkisiz erişim sağlamak için kullandıkları yolları ifade etmektedir. Zararlı yazılım (malware), oltalama (phishing), zayıf şifreler, açık ağ bağlantıları ve sosyal mühendislik gibi yöntemler sıkça kullanılan saldırı vektörleri arasında yer almaktadır (Gupta, Singhal, & Kapoor, 2016). Bu vektörlerin anlaşılması saldırıların erken tespit edilmesi ve güvenlik önlemlerinin iyileştirilmesi açısından kritik öneme sahiptir.

Siber güvenlik alanında sosyal mühendislik yöntemleri, bireyleri manipüle ederek gizli bilgi edinmeyi amaçlayan teknikler olarak öne çıkmaktadır. Bu yöntemler, kullanıcıların güvenini istismar ederek sistemlerin zayıf noktalarına ulaşılmasını kolaylaştırmaktadır. Bu bağlamda penetrasyon testleri uygulamaları, organizasyonların güvenlik durumunu değerlendirmek için kritik rol oynamaktadır (Wang, Sun, & Zhu, 2020). Bu testler, potansiyel zafiyetleri belirlemek amacıyla sistemlerin özenle analiz edilmesini sağlamaktadır. Botnet'ler, kontrol altına alınmış çok sayıda cihazdan oluşan ağlar olarak Dağıtık Hizmet Reddi (DDoS), siber saldırılarda geniş bir yelpazede kullanılmakta ve ciddi güvenlik tehditleri oluşturabilmektedir. Sosyal mühendislik testlerine yönelik çeşitli araçlar da bulunmaktadır. Kali Linux işletim sistemi üzerinde çalışan popüler bir araç olan Social Engineering Toolkit (SET) kullanıcıları kandırmaya yönelik senaryolar geliştirmeyi kolaylaştırmaktadır (Pavković & Perkov, 2011). Metasploit Framework, hem penetrasyon testlerinde hem de sosyal mühendislik saldırılarında kullanılabilecek kapsamlı bir platform olarak yer almaktadır.

2.2. Siber Güvenlik Hizmeti Olarak (Cyber Security as a Service-CSaaS)

Siber Güvenlik Hizmeti (CSaaS), siber güvenlik tehditlerinin çeşitlenmesi ve değişmesi nedeniyle giderek daha popüler hale gelmektedir. CSaaS, Güvenlik ve İzleme Yönetimi, Uç Nokta Güvenliği, Ağ Güvenliği, Veri Güvenliği, Kimlik ve Erişim Yönetimi, Yönetilen Algılama ve Yanıt (MDR), Güvenlik Açığı Yönetimi ve Güvenlik Uyumluluk Yönetimi dahil olmak üzere çeşitli güvenlik katmanları sunmaktadır (Morris et v.d., 2023). Bu hizmetler, tehditlerin erken tespiti ve yönetimi, cihazların korunması, ağ güvenliği çözümleri, veri şifreleme, veri kaybı önleme ve bulut politikaları sağlamaktadır. Ayrıca şirketlerin siber güvenliklerini güvence altına alarak riskleri azaltmalarına yardımcı olmaktadır. Hizmetler arasında varlık yokluğu, artırılmış risk parlaklığı ve yama yönetimi gibi özellikler de bulunmaktadır. Genel olarak, CSaaS şirketlerin güvenlik harcamalarını daha etkili bir şekilde karşılamalarına yardımcı olmaktadır.

2.3. Koruma Yöntemleri

Siber güvenliğin güçlendirilmesi amacıyla bir dizi strateji uygulanmakta ve çeşitli araçlar kullanılmaktadır. Bu bağlamda tehdit istihbaratı, güvenlik açığı yönetimi, ağ segmentasyonu ve felaket kurtarma planları gibi savunma stratejileri hem saldırganların hem de savunma yaklaşımlarının tamamlayıcı unsurları olarak önemli bir rol oynamaktadır. Etkili korunma yöntemleri arasında güçlü şifrelerin ve çok faktörlü kimlik doğrulamanın kullanılması

(Ometov v.d., 2018), yazılımların güncel tutulması, çalışanların siber güvenlik tehditlerine karşı eğitilmesi ve güvenli ağ bağlantılarının sağlanması yer almaktadır. Bu stratejiler, organizasyonların tehditlere karşı güçlü bir savunma oluşturmasına olanak tanırken saldırganların yöntemlerine karşı kapsamlı bir siber güvenlik yaklaşımı sunmaktadır.

Çalışanların düzenli eğitim programları ile bilinçlendirilmesi, sosyal mühendislik saldırılarına karşı en etkili savunma yöntemlerinden biridir ve bunlar insan hatası kaynaklı risklerin azaltılmasına da katkı sağlar. Ayrıca; güvenlik duvarları ve izleme sistemleri, ağ güvenliği kapsamında potansiyel tehditlerin erken tespitine olanak tanırken; penetrasyon testleri, sistemlerin zayıf noktalarının belirlenmesi ve bu zayıflıkların giderilmesi açısından kritik bir öneme sahiptir (Artsın & Parmaksız, 2023). Güvenli erişim yönetimi kimlik doğrulama ve yetkilendirme süreçlerini güçlendirerek yetkisiz erişimlerin önüne geçmektedir. Tüm bu yöntemler, organizasyonların siber güvenliklerini proaktif bir yaklaşımla artırırken sürekli gelişen tehditlere karşı da daha dirençli hale gelmelerini sağlamaktadır.

Sistemleri yöneten personelin, cihazların ve sistemlerin güncel tutulması siber güvenlik açısından büyük önem taşımaktadır. Bu süreç, güvenlik yamalarının düzenli olarak uygulanması ile sağlanmalıdır. Yazılım güncellemeleri ve güvenlik yamaları, bilinen güvenlik açıklarını kapatarak kötü niyetli saldırganların sistemlere sızma olasılığını azaltmaktadır. Güncel yazılımlar, yeni güvenlik tehditlerine karşı koruma sağlamak için en son güvenlik önlemlerini içermektedir. Sistem yöneticileri, tüm cihazların ve uygulamaların güncellenmesini sağlamak için düzenli bakım planları oluşturmalı ve bunları titizlikle uygulamalıdır. Bu sayede organizasyonlar, siber saldırılara karşı daha dayanıklı hale gelir ve veri güvenliğini artırarak siber tehditlerin etkisini minimize edebilirler. Ayrıca, güvenlik yamalarının zamanında uygulanması, düzenleyici uyumluluk gerekliliklerini karşılamada da kritik bir rol oynamaktadır.

2.4. Siber Güvenlikte Uzmanlık Sertifikalarının Rolü

Siber güvenlik risklerine karşı etkili bir şekilde mücadele edebilmek için, bireylerin deneyim, profesyonel kimlik bilgileri ve teknik bilgi ve yeteneklere sahip olmaları gerekmektedir. Bu bağlamda, çeşitli sertifikalar, uzmanların yetkinliklerini artırarak siber güvenlik alanında daha etkili olmalarını sağlamaktadır.

Sertifikalı Etik Hacker (CEH) sertifikası, etik bilgisayar korsanlarının sistem açıklarını tespit etme ve bu açıkları etik normlara uygun olarak simüle edilmiş saldırılarla kapatma kapasitesini geliştirmektedir. CEH

sertifikası, siber suçluların stratejilerini anlamayı ve bu stratejilere karşı savunma mekanizmaları geliştirmeyi öğretmektedir (Graves, 2010). Saldırgan Güvenlik Sertifikalı Profesyonel (OSCP) programı, siber güvenlik uzmanlarına pratik saldırı taktikleri sunarak savunma mekanizmaları oluşturma ve saldırı yollarını tahmin etme yeteneklerini geliştirmektedir. OSCP, uygulamalı bir sınav süreci ile katılımcıların penetrasyon testi becerilerini gerçek dünya senaryolarında kullanmalarını sağlamaktadır. CompTIA PenTest+ sertifikası ise penetrasyon testi, güvenlik açığı değerlendirmesi ve ağ güvenliği yönetimi konularında bilgi sağlayarak sistem korumasını güçlendirmektedir. Bu sertifika, özellikle orta düzeyde beceriye sahip siber güvenlik profesyonelleri için uygundur ve güvenlik açıklarını yönetme becerilerini geliştirmektedir. Sertifikalı Bilgi Sistemleri Güvenlik Uzmanı (CISSP) sertifikası, bilgi güvenliği mimarisi, operasyonları ve risk yönetimi alanlarında kapsamlı bilgi sunarak güvenli ağ yapılandırmaları ve çok faktörlü kimlik doğrulama gibi stratejilerin kullanımını teşvik eder. CISSP, profesyonel itibarı arttıran uluslararası düzeyde tanınan bir sertifikadır (Davri v.d., 2021). GIAC Penetration Tester (GPEN) sertifikası, penetrasyon testi metodolojileri konusunda derinlemesine bilgi sağlayarak Wi-Fi ağ güvenliği için kritik koruma stratejilerine odaklanmaktadır. GPEN sertifikası, yasal konularla başa çıkma yeteneği de dahil olmak üzere kapsamlı bir eğitim sunmaktadır.

Türk Standartları Enstitüsü (TSE), sızma testi yapan firmalar için TSE 13638 standardına dayalı bir sertifikasyon sunmaktadır. Bu sertifika, firmaların belirli kalite ve güvenlik standartlarına uygun olarak sızma testleri gerçekleştirdiğini kanıtlamaktadır (Doğan & Karacan, 2022). TSE 13638 standardı, Türkiye'deki sızma testlerinin belirli bir güvenlik seviyesinde yapılmasını sağlayarak bu testlerin nasıl gerçekleştirileceği, hangi araçların kullanılacağı ve sonuçların nasıl raporlanacağı konusunda rehberlik etmektedir. TSE onaylı sızma testi belgesi, işletmelerin bilgi sistemlerini ulusal standartlara uygun bir şekilde değerlendirdiğini göstermektedir. Bu belgeyi almak için, firmaların TSE'nin belirlediği kriterlere göre testler yapması ve sonuçları TSE'ye raporlaması gerekmektedir. Bu sertifikalar, siber güvenlik uzmanlarının siber tehlikelerini erken fark etmelerini ve etkili savunma stratejileri geliştirmelerini sağlayarak kariyerlerinde önemli avantajlar elde etmelerine yardımcı olmaktadır.

3. Siber Güvenlikte Açık Kaynak Yazılımlar

Açık kaynak yazılımlar, siber güvenlik alanında maliyet etkin çözümler sunarak organizasyonların güvenliğini artırmalarına yardımcı olmaktadır. Bu araçlar hem tehditlerin tespit edilmesi hem de olaylara hızlı yanıt verilmesi

açısından kritik öneme sahiptir. Siber güvenlik uzmanları, bu yazılımları kullanarak sistemlerini daha iyi koruyabilir ve potansiyel zayıf noktaları belirleyebilirler.

3.1. Açık Kaynaklı Yazılımlar

Siber güvenlik alanında kullanılan çeşitli açık kaynak yazılımlar, farklı işlevleri ve kullanım yapılarıyla kuruluşların güvenliğini artırmada önemli katkılar sağlamaktadır. Bu yazılımlar kimlik ve erişim yönetiminden ağ güvenliğine, tehdit izleme ve yanıta kadar geniş bir yelpazede hizmet sunmaktadır. Kimlik ve erişim yönetimi (IAM) için güçlü bir araç olan Keycloak, kullanıcıların kimlik doğrulama ve yetkilendirme süreçlerini etkin bir şekilde yönetmelerine olanak tanır; çok faktörlü kimlik doğrulama (MFA) ve sosyal oturum açma gibi özellikleriyle kullanıcıların tek bir kimlik bilgisi setiyle birden fazla uygulamaya erişimini sağlamaktadır. Açık kaynaklı ayrıcalıklı erişim yönetimi (PAM) çözümleri, şirket güvenliğini iyileştirmek ve yetkisiz erişimi engellemek için kritik öneme sahiptir.

FreeIPA, LDAP, Kerberos ve DNS gibi teknolojiler aracılığıyla kullanıcı erişimini ve ayrıcalıklarını yönetirken kimlik doğrulama, yetkilendirme ve muhasebe bilgilerini merkezileştiren bir güvenlik bilgi yönetim sistemidir. HashiCorp Vault, hassas verileri depolamak ve korumak için popüler bir çözümdür; CyberArk Conjur ise DevOps ortamları için tasarlanmıştır.

Ağ Erişim Kontrolü (NAC) sağlayan PacketFence, yetkisiz erişimi önleyerek güvenli ağlara erişimi düzenlemekte ve cihazları ağa bağlanmadan önce kimlik doğrulaması yaparak ağ güvenliğini artırmaktadır. Wazuh, güvenlik bilgi ve olay yönetimi (SIEM), genişletilmiş algılama ve yanıt (XDR) çözümleri sunarak tehdit izleme ve yanıt süreçlerini etkinleştirirken (Sridharan & Kanchana, 2022). OpenCTI, siber tehdit istihbaratı yönetimi için bir platform olarak tehdit bilgilerini toplamakta, analiz etmekte ve dağıtmaktadır.

Velociraptor, uç nokta görünürlüğü ve toplama aracılığıyla derinlemesine analizler gerçekleştirirken GoAccess, gerçek zamanlı web günlüğü analizcisi olarak kullanıcı davranışlarını izleyerek olası tehditleri tespit etmektedir. Syncthing, kullanıcıların dosyalarını güvenli bir şekilde senkronize etmelerini sağlarken TacacsGUI, TACACS+ protokolü üzerine inşa edilen bir erişim kontrol sunucusu olarak kimlik doğrulama, yetkilendirme ve hesap yönetimini merkezi olarak gerçekleştirmektedir. T-Pot, birden fazla honeypot çözümünü entegre eden kapsamlı bir platform olarak kötü amaçlı faaliyetleri tespit etme ve saldırganların tekniklerini anlama konusunda kritik bir öneme sahiptir. Son olarak SELKS, Debian tabanlı bir IDS, IPS

ve ağ güvenliği izleme platformu olarak ağ trafiğini izleyerek potansiyel tehditleri tespit etmeye ve ağ faaliyetlerini analiz etmeye olanak tanımaktadır (Baykara & Daş, 2019). Bu yazılımlar, açık kaynaklı yapıları sayesinde geniş bir topluluk tarafından desteklenmekte ve sürekli olarak geliştirilerek siber güvenlik alanındaki yenilikleri takip etmeyi kolaylaştırmaktadır.

3.2. Çerçeveler

Açık Siber Tehdit İstihbaratı (OpenCTI), siber tehdit istihbaratını yönetmek için kullanılan açık kaynaklı bir platformdur. Kullanıcıların tehdit verilerini merkezi bir sistemde toplamasına, analiz etmesine ve paylaşmasına olanak tanıyarak tehditlere karşı daha etkili bir savunma geliştirmelerine yardımcı olur.

MITRE ATT&CK, siber saldırı tekniklerinin, taktiklerinin ve prosedürlerinin sistematik bir kütüphanesi olarak güvenlik uzmanlarının saldırı senaryolarını daha iyi anlamalarını ve savunma stratejilerini geliştirmelerini sağlamakta önemli bir kaynak işlevi görmektedir (Mitre Corporation, 2020).

Açık Web Uygulaması Güvenlik Projesi (OWASP) ise web uygulama güvenliği konularında en iyi uygulamaları ve standartları geliştiren bir topluluktur; "OWASP Top Ten" gibi projelerle, uygulama güvenliğinde yaygın olan zayıflıkları belirleyerek bu zayıflıklarla başa çıkma yöntemleri sunmaktadır (Helmiawan et al., 2020).

Açık Güvenlik Açığı ve Değerlendirme Dili (OVAL), güvenlik açıklarının ve sistem konfigürasyonlarının tanımlanması ve değerlendirilmesi için standart bir format sağlayarak, güvenlik uzmanlarının zafiyetleri sistematik bir şekilde analiz etmelerine yardımcı olmaktadır.

Güvenlik açıklarının ciddiyetini değerlendirmek için kullanılan bir standart olan Ortak Güvenlik Açığı Puanlama Sistemi (CVS), güvenlik uzmanlarının önceliklendirme yapmalarına yardımcı olmaktadır. Yaygın Güvenlik Açıkları ve Maruz Kalmalar (CVE), belirli güvenlik açıklarını tanımlamak için kullanılan bir veri tabanıdır ve zafiyetlerin genel tanımlarını sunmaktadır. Ortak Zayıflık Sayımı (CWE) ise yazılım zayıflıklarını sınıflandırmak için kullanılan bir referans kaynağıdır. Ayrıca yazılım güvenliği konularında farkındalığı artırmaya yönelik önemli bilgiler sağlamaktadır (Martin, 2019).

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), siber güvenlik alanında en iyi uygulamaları ve standartları belirleyen önemli bir kuruluş olarak öne çıkar. NIST'in Siber Güvenlik Çerçevesi, organizasyonların siber risklerini yönetmelerine yardımcı olmak için bir dizi rehberlik ve araç

sunar. Bu çerçeve, siber güvenlik stratejilerini geliştirmek ve uygulamak için kapsamlı bir yol haritası sağlar. Bu araçlar ve çerçeveler, mevcut siber güvenlik çözümlerini tamamlayarak organizasyonların güvenlik stratejilerini güçlendirmelerine katkı sağlamakta; böylece siber güvenlik alanında daha kapsamlı bir anlayış sunmaktadır (Schlenoff, Scott, & Balakirsky, 2011).

3.3. Zafiyet Analizi

Penetrasyon testi ve güvenlik açığı taraması için kullanıcı dostu bir platform olan Archery, insanların sistemlerini incelemelerini ve kusurları belirlemelerini sağlar. OpenVAS, ağları tarayan ve kullanıcılara güvenlik durumunu analiz etmek için güncel bir veritabanı sağlayan açık kaynaklı bir güvenlik açığı değerlendirme sistemidir. Vuls, açık kaynaklı ve ajan gerektirmeyen bir güvenlik açığı tarayıcısı olarak, siber güvenlik alanında kritik bir rol oynamaktadır.

Ulusal Güvenlik Açığı Veritabanı (NVD), OVAL gibi kaynaklardan elde edilen bilgilerle çalışarak sistemlerdeki potansiyel güvenlik açıklarını tespit eder ve bu açıkların etkilerini analiz eder. Vuls, organizasyonların güvenlik açıklarını proaktif bir şekilde yönetmelerine olanak tanırken, tarama süreçlerini basit ve etkili hale getirir. Graylog, makine öğrenimini kullanarak anormallik algılama ve olay yanıt prosedürlerini geliştiren merkezi bir günlük yönetimi ve güvenlik analitiği çözümüdür. Suricata, ağları gerçek zamanlı olarak analiz eden ve çoklu iş parçacığı yeteneği sayesinde yüksek hızlarda çalışabilen yüksek performanslı, açık kaynaklı bir IDS/IPS'dir. Cuckoo Sandbox, kullanıcıların izole bir ortamda şüpheli dosyaları izlemelerine ve sonuçlarını öğrenmelerine olanak tanıyan bir kötü amaçlı yazılım analiz aracıdır. Bu teknolojiler, sibergüvenlikteki kapsamlı değerlendirme ve analiz prosedürleri aracılığıyla sistem güvenliğinin iyileştirilmesine yardımcı olmaktadır (Wiley, 2008).

4. Siber Güvenlikte Yapay Zekâ, Trend Analizleri ve Uyum Yönetimi

YZ, bilgisayarlarda insan zekâsını taklit eden ve robotların daha önce insanlar tarafından yapılan görevleri yerine getirmesini sağlayan bir teknolojidir. 1950'de Alan Turing'in fikirleriyle başlayan YZ, siber güvenlikte önemli ilerlemelere neden olmaktadır (Muggleton, 2014).

YZ, büyük veri kümelerini analiz edebilir, tehditleri daha etkili bir şekilde belirleyebilir, yanlış pozitifleri ortadan kaldırabilir ve gerçek dünya tehlikelerine göre eylemleri önceliklendirebilir. Ayrıca şüpheli e-postaları tespit edebilir (Qabajeh, Thabtah, & Chiclana, 2018), sosyal mühendislik

saldırılarını simüle edebilir ve olaylarla ilgili verileri hızla değerlendirerek güvenlik ekiplerinin derhal yanıt vermesini sağlayabilir.

YZ, siber güvenlikte veri koruması ve maliyet tasarrufu için çok önemlidir ve bu da onu işletmeler için onu önceliklendirmektedir (Geluvaraj, Satwik, & Ashok Kumar, 2019). YZ destekli siber güvenlik ürünleri için küresel pazarın 2021'de 15 milyar dolardan 2030'a kadar 135 milyar dolara çıkması beklenmektedir.

4.1. Yapay Zekânın Siber Güvenlikte Rolü ve Uygulama Alanları

Günümüzde YZ, siber güvenlikte giderek daha önemli bir rol oynamaktadır. Hem saldırganlar hem de savunucular için bir silah olarak YZ, siber tehditlerin doğasını ve ele alınmasını kökten değiştirmektedir.

4.1.1. Siber Güvenlikte Yapay Zekânın İyiye Kullanımı

Çalışan eğitimi siber güvenlikte çok önemlidir. YZ destekli eğitim programları, personeli sosyal mühendislik saldırılarına daha iyi hazırlamak için kişiselleştirilmiş materyaller sunmaktadır. Araştırmalar, personel eğitimine yatırım yapmanın veri ihlallerinin maliyetini önemli ölçüde düşürebileceğini göstermiştir.

YZ, büyük veri analitiği ve makine öğrenimi tekniklerini kullanarak olası tehlikeleri hızla tespit edebilmektedir. Bu sistemler, olağan etkinlik kalıplarını değerlendirerek anormallikleri tespit edebilir ve saldırıları tahmin edebilir. YZ tabanlı sistemler, virüsleri ve şüpheli etkinlikleri tespit etmek için ağ trafiğini izleyebilmektedir.

Olay müdahalesi, YZ'nin önemli bir safhası olarak bilinmektedir. Bir güvenlik ihlali durumunda, YZ sistemleri tehlikeye atılan bilgisayarları hemen izole edebilmekte veya şüpheli IP adreslerini engelleyebilmektedir. Bu hızlı tepki mekanizması, insan hatasını azaltarak kurumsal güvenliği iyileştirmektedir (Steinke v.d., 2015).

Coroza, ModSecurity ve Naxsi (Garn et al., 2021) gibi YZ destekli güvenlik duvarları ve açık kaynaklı WAF'lar, gelen iletişimleri analiz ederek, potansiyel tehditleri belirleyerek ve gerçek zamanlı tehdit koruması için dinamik kurallar sağlayarak siber güvenliği iyileştirmektedir. Bu durum, kuruluşların dijital dönüşüm geçirirken stratejilerini yeniden düşünmelerini gerekli hale getirmektedir.

YZ gelişmeleri, kuruluşların veri güvenliği operasyonlarını optimize etmelerini sağlarken aynı zamanda ortaya çıkan tehditlerle başa çıkma kapasitelerini de artırmaktadır.

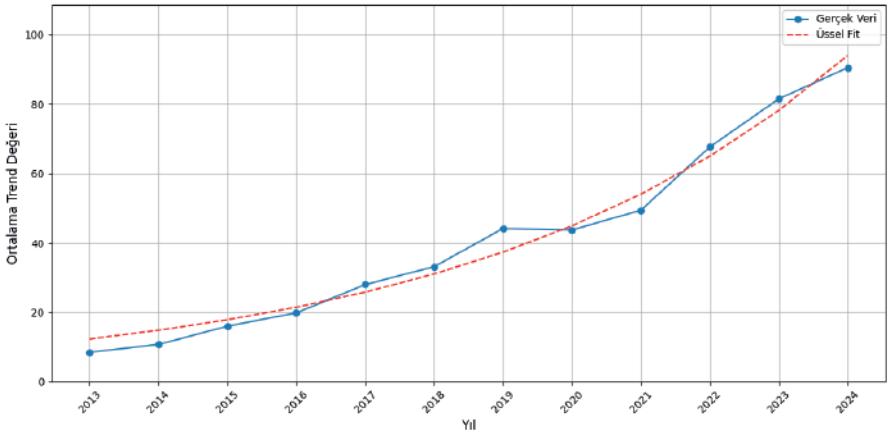
4.1.2. Siber Güvenlikte Yapay Zekânın Kötüye Kullanımı

Siber suçlular, sosyal mühendislik, parola kırma, deepfake ve veri zehirleme gibi çeşitli yöntemlerle YZ'yi kullanırlar. Ayrıca suçlular sosyal mühendislik yoluyla başkalarını etkilerler, kritik bilgileri ifşa ederler veya güvenlik ihlalleri gerçekleştirirler. YZ, bu saldırılarda otomasyonu iyileştirerek daha özel ve etkili mesajlaşma sağlar. Gelişmiş parola kırma algoritmaları verimliliği artırarak daha hızlı ve daha kesin tahminler yapılmasını sağlar.

Deepfake teknolojisi sahte ses ve video bilgilerinin yanı sıra sosyal mühendislik ve şantaj gibi dolandırıcılık taktikleri oluşturmak için kullanılmaktadır (Westerlund, 2019). Veri zehirleme, aldatıcı sonuçlar sağlamak için YZ sistemlerinin eğitim verilerinin kasıtlı olarak manipüle edilmesidir. Bu ise karar alma süreçleri üzerinde olumsuz bir etkiye sahiptir ve keşfi zorlaştırır. YZ'nin kötüye kullanılması, siber güvenlik tehditlerinin karmaşıklığını ve tehlikesini artırır.

4.2. Siber Güvenlik Trend Analizleri

Python Pytrends kütüphanesi aracılığıyla Google Trends web sitesinde sunulan sonuçları, Google Trends API'sini kullanarak analiz etmemizi kolaylaştırmaktadır (Hogue & DeWilde, 2023). Şekil 1'de bu kütüphane kullanılarak son on yılda siber güvenlik alanında değişim trendi verilmektedir.



Şekil 1. Pytrends ile Son 10 Yılın Siber Güvenlik Analizi

Web Of Science'ta siber güvenlik alanında son on yılda 821 yayın bulunmaktadır. Tablo 1'de en çok yayına sahip ilk on kategori verilmiştir.

Tablo 1. WOS ile Son 10 Yılın Siber Güvenlik Yayınlarının Dağılımı

WOS (Kategoriler)	Sayı	%
Bilgisayar Bilimleri Bilgi Sis.	241	%29.35
Mühendislik Elektrik Elektronik	196	%23.87
Telekomünikasyon	99	%12.06
Mühendislik Multidisipliner	62	%7.55
Uygulamalı Fizik	62	%7.55
Bilgisayar Bil. Disiplinler Arası Uygulamalar	58	%7.07
Bilgisayar Bilimleri Teori Yön.	58	%7.07
Kimya Analitik	49	%5.97
Enerji Yakıtları	49	%5.97
Bilgisayar Bilimleri Yapay Zekâ	46	%5.60

Terim Frekansı-Tersine Doküman Frekansı (TF-IDF), en temel ifade ile bir metin vektörleştirme yöntemidir. TF-IDF ile bir metindeki veya dizideki kelimelerin metinle ne kadar ilgili olduğunun hesaplanması gerçekleştirilmektedir (Bafna, Pramod, & Vaidya, 2016). TF-IDF Makine öğrenmesi, metin madenciliği, doğal dil işlemi gibi uygulamalarda sıkça kullanılmaktadır. Bu yöntem, bir belgede kelimenin kaç kez görüldüğü (TF) ve bir dizi belgede (farklı belgelerde) kelimenin ters belge sıklığı (IDF) ölçümlerini kullanmaktadır. TF-IDF yöntemiyle siber güvenlik alanında belirleyici önemli kelimeler Şekil 2'de kelime bulutu olarak sunulmaktadır.

Şekil 2. Siber Güvenlikteki Belirleyici Kelime Bulutu.

Siber güvenliğin artan önemi, günümüzde YZ'nin sağladığı yaratıcı çözümlerin yanı sıra çeşitli güncel metodolojilerinde oluşturulmasına olanak tanımaktadır (Lu, 2018). Bu bağlamda, otonom siber güvenlik sistemleri saldırıları otomatik olarak tespit etme ve bunlara yanıt verme kapasiteleriyle

öne çıkmaktadır. Bu sistemler, sürekli öğrenme yetenekleri sayesinde yeni tehditlere hızla yanıt verirken sistem güvenliğini güçlendirmede önemli bir rol oynamaktadır. Ayrıca, özellikle büyük dil modelleri olmak üzere yeni nesil YZ teknikleri, daha karmaşık ve ikna edici sosyal mühendislik saldırılarına olanak tanımaktadır. Bu tür saldırılar, insanların psikolojik durumlarını hedef alır ve daha büyük hedefli manipülasyon taktiklerinin kullanılmasına olanak tanımaktadır. Diğer yandan kuantum kriptografisi, kuantum bilgi teknolojisinin büyümesiyle birlikte, siber güvenlikte yenilikçi çözümlerin yaratılmasını sağlama potansiyeline sahiptir (Gisin, Ribordy, Tittel, & Zbinden, 2002). Bu yeni kriptografik teknolojiler, veri koruma prosedürlerini artırmak için YZ ile birleştirildiğinde güvenlik kontrollerinin etkinliğini büyük ölçüde iyileştirme potansiyeline sahiptirler. YZ ve kuantum teknolojileri, siber güvenlik stratejilerinin büyümesinde önemli bir rol oynar ve bu alandaki tehditlerle mücadele için yaratıcı ve etkili yöntemler sağlamaktadır (Nair, Deshmukh, & Tyagi, 2024).

4.3. Siber Güvenlik Uyum Yönetimi

Güvenlik uyumluluk yönetimi, bir kuruluşun bilgi güvenliği politikalarının düzenlemeler, endüstri standartları ve iç politikalarla uyumlu olmasını sağlamak için önemli bir etkendir. Risk yönetimi, yasal yükümlülükler, itibar koruması ve güven oluşturma için çok önemlidir.

4.3.1. Güvenlik Uyumluluk Yönetiminin Önemi

Güvenlik uyumluluk yönetimi, işletmelerin düzenleyici yükümlülükleri ve endüstri standartlarını karşıladıklarından emin olmaları için kritik derecede önemlidir. Sadece veri koruma düzenlemelerini güçlendirmekle kalmaz; aynı zamanda güvenlik risklerini azaltarak siber saldırılara karşı dirençli olmayı sağlamaktadır. Bu teknik ayrıca, şirketlerin güvenlik ihlallerinden kaynaklanan itibar zararını azaltarak kamu imajlarını korumalarına yardımcı olmaktadır. Dahası; güvenliğe ve gizliliğe bağlılık göstererek tüketici güvenini oluşturmaktadır. Güvenlik uyumluluk yönetimi ayrıca prosedürleri ve kontrolleri standart hale getirerek ve operasyonel verimliliği artırarak işletmelerin daha verimli ve sürdürülebilir bir şekilde çalışmasını sağlamaktadır. Temel güvenlik uyumluluk standartları ve kuralları, işletmelerin veri güvenliğini güvence altına almasına yardımcı olmaktadır.

Genel Veri Koruma Yönetmeliği (GDPR) veri işleme, depolama ve aktarımı için sıkı yönergeler belirlerken Türkiye'nin Kişisel Verilerin Korunması Kanunu (KVKK) yerel kısıtlamalarını içermektedir. Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) güvenli kredi kartı işleme, depolama ve aktarımı için belirtilen gereksinimleri belirlemektedir.

ISO/IEC 27001, bilgi güvenliği yönetim sistemleri için kapsamlı bir çerçeve tanımlamaktadır. Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası (HIPAA), Amerika Birleşik Devletleri'nde sağlık bilgilerinin gizliliğini ve güvenliğini korumaktadır. SOC 2, hizmet işletmelerinin güvenlik, erişilebilirlik, işlem bütünlüğü, gizlilik ve mahremiyet kontrollerini değerlendirmektedir.

4.3.2. Güvenlik Uyumluluk Yönetimi Süreci

Güvenlik uyumluluk yönetimi süreci, veri güvenliğini iyileştirmenin ve işletmelerde yasal uyumluluğu sağlamanın sistematik bir adımı olarak bilinmektedir. Uygulanabilir kuralları ve endüstri standartlarını belirleyerek başlar, ardından kuruluşun güvenlik politikalarını, süreçlerini ve kontrollerini değerlendirir. Uygunsuzluk riskleri tanınır ve bunları azaltmak için yöntemler belirlenir. Güvenlik politikaları ve prosedürleri geliştirilir ve güncellenir, teknik ve idari güvenlik önlemleri alınır. Personelin uyumluluk standartlarını kavraması için düzenli eğitim ve farkındalık kampanyaları gerekmektedir. İzleme ve denetim aşaması, uyumluluk önlemlerinin sürekli izlenmesini ve periyodik denetimleri içermektedir. Sürekli geliştirme, düzenli uyumluluk durumu raporlaması ve denetim sonuçlarına dayalı iyileştirme stratejilerinin geliştirilmesini gerektirmektedir. Bu seviyeler, bir kuruluşun güvenlik durumunu iyileştirerek, yasal gerekliliklerini karşılamasına yardımcı olmaktadır.

4.3.3. Güvenlik Uyumluluk Yönetiminin Geleceği

Güvenlik uyumluluk yönetiminin geleceği, teknoloji ilerledikçe ve siber riskler daha yaygın hale geldikçe değişmektedir. YZ ve makine öğrenimi uyumluluk değerlendirme ve risk analizi prosedürlerinde kapsamlı bir şekilde uygulanacak ve sürekli uyumluluk doğrulama sistemlerine olanak tanıyacaktır. Otonom uyumluluk sistemleri, self servis uyumluluk yönetimi platformlarına olanak tanıyacak ve süreç verimliliğini artıracaktır. Küresel uyumluluk çerçeveleri, mevzuatı uluslar ve endüstriler arasında uyumlu hale getirirken; gizliliği artıran teknoloji (PET) veri gizliliğini koruyarak uyumluluğu garanti edecektir. Bu gelişmeler, güvenlik uyumluluk yönetimini işletmelerin yasal gereklilikleri karşılaması, riskleri yönetmesi ve itibarlarını koruması için kaçınılmaz bir prosedür haline getirmiştir. Proaktif, risk odaklı ve teknoloji destekli bir uyumluluk yönetimi yaklaşımı, firmaların dijital çağda güvenli ve karlı bir şekilde işlev görmesine yardımcı olabilecektir.

5. Sonuç

Bu çalışma, siber güvenlik alanının karmaşık ve sürekli gelişen doğasını kapsamlı bir şekilde ele almıştır. Araştırmamız, siber tehditlerin giderek daha sofistike hale geldiğini ve geleneksel güvenlik önlemlerinin artık yeterli olmadığını göstermektedir. Özellikle açık kaynak yazılımların siber güvenlik alanında sunduğu fırsatlar ve zorluklar, gelecekteki savunma stratejilerinin şekillenmesinde kritik bir rol oynayacaktır. Bu bağlamda, Keycloak, PacketFence, Wazuh gibi araçların etkin kullanımı, organizasyonların güvenlik duruşunu önemli ölçüde güçlendirebilir.

YZ teknolojilerinin siber güvenlik alanındaki uygulamaları hem savunma hem de saldırı perspektifinden incelenmiştir. Bulgularımız, YZ'nin tehdit tespiti, anomali analizi ve otomatik yanıt sistemlerinde devrim niteliğinde değişiklikler getirdiğini ortaya koymaktadır. Ancak, YZ'nin kötü niyetli aktörler tarafından da kullanılabileceği gerçeği, siber güvenlik profesyonellerinin sürekli olarak yeni stratejiler geliştirmesini zorunlu kılmaktadır.

Trend analizlerimiz, bulut güvenliği, IoT güvenliği ve kuantum kriptografisi gibi alanların gelecekte daha da önem kazanacağını göstermektedir. Bu gelişmeler, siber güvenlik eğitiminin ve farkındalığının tüm organizasyon seviyelerinde artırılması gerektiğini vurgulamaktadır. Ayrıca, güvenlik uyum yönetiminin geleceği, yasal düzenlemelerin ve endüstri standartlarının sürekli evrimiyle şekillenecektir.

Sonuç olarak, bu çalışma siber güvenliğin multidisipliner doğasını ortaya koyarak teknoloji, insan faktörü ve politika arasındaki karmaşık ilişkiyi vurgulamaktadır. Gelecekteki araştırmalar, bu alanlar arasındaki etkileşimi daha derinlemesine incelemeli ve bütünsel güvenlik çözümleri geliştirmeye odaklanmalıdır. Siber güvenliğin geleceği proaktif, adaptif ve işbirlikçi yaklaşımların benimsenmesine bağlı olacaktır. Bu bağlamda, sürekli eğitim, araştırma ve geliştirme faaliyetleri, siber tehditlere karşı etkili savunma stratejilerinin temelini oluşturacaktır.

Kaynakça

Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. *Elsevier*.

Artsın, M., & Parmaksız, H. (2023, October). Bilişim teknolojileri eğitiminde siber güvenlik: Zafiyet tarama ve sızma testlerinin önemi. *In 16. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu* (Eskişehir).

Bafna, P., Pramod, D., & Vaidya, A. (2016, March). Document clustering: TF-IDF approach. *In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 61-66). IEEE. https://doi.org/10.1109/ICEEOT.2016.7754750

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks, 4*(3), 149-160. https://doi.org/10.1016/j.dcan.2017.10.006

Baykara, M., & Daş, R. (2019). Saldırı tespit ve engelleme araçlarının incelenmesi. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 10*(1), 57-75. https://doi.org/10.24012/dumf.449059

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. *In Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014*, Aveiro, Portugal, September 25-26, 2014. Proceedings 15 (pp. 63-72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

Davri, E. C., Darra, E., Monogioudis, I., Grigoriadis, A., Iliou, C., Mengidis, N., ... & Farah, M. A. B. (2021, July). Cyber security certification programmes. *In 2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 428-435). IEEE. https://doi.org/10.1109/CSR51186.2021.9527974

De Capitani di Vimercati, S., Paraboschi, S., & Samarati, P. (2003). Access control: Principles and solutions. *Software: Practice and Experience, 33*(5), 397-421. https://doi.org/10.1002/spe.513

Doğan, Ö., & Karacan, H. (2022). Türkiye'deki e-ticarete özgü blokzincir tabanlı dijital kimlik güven çerçevesi önerisi. *Bilgi Yönetimi, 5*(2), 256-279. https://doi.org/10.33721/by.1113558

Garn, B., Lang, D. S., Leithner, M., Kuhn, D. R., Kacker, R., & Simos, D. E. (2021, April). Combinatorially XSSing web application firewalls. *In 2021 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (pp. 85-94). IEEE. https://doi.org/10.1109/ICSTW52544.2021.00026

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. *In International Conference on Computer Net-*

works and Communication Technologies: ICCNCT 2018 (pp. 739-747). Springer Singapore. https://doi.org/10.1007/978-981-10-8681-6_67

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145

Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. *In 2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 537-540). IEEE. https://doi.org/10.1109/CCAA.2016.7813778

Helmiawan, M. A., Firmansyah, E., Fadil, I., Sofivan, Y., Mahardika, F., & Guntara, A. (2020, October). Analysis of web security using open web application security project 10. *In 2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE. https://doi.org/10.1109/CITSM50537.2020.9268856

Hogue, J., & DeWilde, B. (2023). pytrends: Pseudo API for Google Trends. https://pypi.org/project/pytrends (E.T.: 20.10.2024).

Lu, Y. (2018). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management, 3*(04), 1850014. https://doi.org/10.1142/S2424862218500148

Martin, B. (2019). Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Quality Enumeration (CQE): Attempting to systematically catalog the safety and security challenges for modern, networked, software-intensive systems. *ACM SIGAda Ada Letters, 38*(2), 9-42. https://doi.org/10.1145/3375408.3375410

Melis, A., Al Sadi, A., Berardi, D., Callegati, F., & Prandini, M. (2023). A systematic literature review of offensive and defensive security solutions with software defined network. *IEEE Access, 11*, 93431-93463. https://doi.org/10.1109/ACCESS.2023.3276238

McGraw, G. (2012). Software security: Building security in. *Datenschutz und Datensicherheit-DuD, 36*(9), 662-665.

Mitre Corporation. (2020). ATT&CK® framework for enterprise: Techniques used by adversaries and mitigations for them. Retrieved from https://attack.mitre.org/

Morris, J., Tatschner, S., Heinl, M. P., Heinl, P., Newe, T., & Plaga, S. (2023). Cybersecurity as a service. *In Cybersecurity Vigilance and Security Engineering of Internet of Everything* (pp. 141-161). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-45162-1_9

Muggleton, S. (2014). Alan Turing and the development of artificial intelligence. *AI Communications, 27*(1), 3-10.

Nair, M. M., Deshmukh, A., & Tyagi, A. K. (2024). Artificial intelligence for cyber security: Current trends and future challenges. *In Automated Secure Computing for Next-Generation Systems* (pp. 83-114). Springer. https://doi.org/10.1002/9781394213948.ch5

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography, 2*(1), 1. https://doi.org/10.3390/cryptography2010001

Pavković, N., & Perkov, L. (2011, May). Social engineering toolkit—A systematic approach to social engineering. *In 2011 Proceedings of the 34th International Convention MIPRO* (pp. 1485-1489). IEEE.

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review, 29*, 44-55. https://doi.org/10.1016/j.cosrev.2018.05.003

Schlenoff, C., Scott, H., & Balakirsky, S. (2011). Performance evaluation of intelligent systems at the National Institute of Standards and Technology (NIST). *International Test and Evaluation Association (ITEA) Journal, 32*(1), 59-67.

Schmidt, K., Phillips, C., & Chuvakin, A. (2012). Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management. *Newnes.*

Fuchsberger, A. (2005). Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report, 10*(3), 134-139. http://dx.doi.org/10.5121/ijcnc.2014.6407

Sridharan, A., & Kanchana, V. (2022, November). SIEM integration with SOAR. *In 2022 International Conference on Futuristic Technologies (INCOFT)* (pp. 1-6). IEEE. https://doi.org/10.1109/INCOFT55651.2022.10094537

Stallings, W., & Brown, L. (2015). Computer security: Principles and practice. *Pearson*.

Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley Professional.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13*(4), 20-29. https://doi.org/10.1109/MSP.2015.71

Sunit, B., & Nina, G. (2011). Cyber security: Understanding cybercrimes, computer forensics and legal perspectives. *Wiley India*.

Türkiye Cumhuriyeti. (2007). 5651 sayılı Kanun: İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele hakkında kanun. Resmî Gazete. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&MevzuatTertip=5 (E.T.: 20.10.2024).

Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity. *IEEE Access, 8*, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11). https://doi.org/10.22215/timreview/1282

Wiley, J. (2008). Security engineering: A guide to building dependable distributed systems (2nd ed., pp. 239-274).

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046-2069. https://doi.org/10.1109/SURV.2013.031413.00127

Bölüm 4

Yönetim Bilişim Sistemleri Perspektifinden Dijital Dönüşüm: Stratejiler ve Organizasyonel Etkileri

Üzeyir Fidan[1]

Özet

Bu çalışma, dijital dönüşümün işletme süreçleri ve Yönetim Bilişim Sistemleri (YBS) üzerindeki etkilerini stratejik bir perspektiften ele almaktadır. Amaç, dijitalleşme süreçlerinin YBS ile entegrasyonunu, bu entegrasyonun işletmeler üzerindeki etkilerini ve dijital dönüşüm projelerinin nasıl yönetildiğini incelemektir. Çalışma, teknolojik altyapı gereksinimlerinden iş süreçlerinin otomatikleştirilmesine, veri yönetiminin önemine ve iş süreçlerinin inovasyonuna kadar geniş bir yelpazede analizler sunmaktadır. Dijital dönüşümün işletmelerin karşılaştığı fırsatları ve zorlukları nasıl şekillendirdiği, YBS'nin bu süreçteki kritik rolüyle birlikte incelenmiştir. Literatürdeki boşlukları doldurmak amacıyla büyük veri analitiği, iş süreçleri inovasyonu ve bilgi güvenliği gibi konulara dikkat çekilmiştir. Ayrıca, dijital dönüşüm projelerinin başarıya ulaşabilmesi için proje yönetim metodolojileri ve değişim yönetimi süreçleri de kapsamlı bir şekilde değerlendirilmiştir. Sonuç olarak, dijital dönüşüm ve YBS'nin işletmelerin rekabet avantajını artırmada ne kadar önemli olduğu vurgulanmış ve gelecekteki dijitalleşme süreçlerine dair stratejik öneriler sunulmuştur.

1. Giriş

Dijital dönüşüm, 21. yüzyılın en önemli organizasyonel değişim süreçlerinden biri olarak kabul edilmektedir. Bu süreç, yalnızca teknolojik gelişmeleri içermez; aynı zamanda iş modellerinin, operasyonel süreçlerin, değer zincirlerinin ve müşteri deneyimlerinin kökten bir dönüşümünü de kapsamaktadır (Westerman, Bonnet & McAfee, 2014). Teknolojik yeniliklerin hızla geliştiği günümüz dünyasında, işletmelerin rekabet avantajı elde etmeleri

1 Dr., Uşak Üniversitesi, Uzaktan Eğitim Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, ORCID: 0000-0003-3451-4344, uzeyir.fidan@usak.edu.tr

https://doi.org/10.58830/ozgur.pub498.c2092

ve sürdürülebilirliklerini güvence altına almaları, dijital teknolojileri etkin bir şekilde benimsemelerine bağlıdır (Hussein, Albadry, Mathew, Al-Romeedy, Alsetoohy, Abou Kamar & Khairy, 2024). Bu dijitalleşme dalgası, sadece büyük şirketleri değil, küçük ve orta ölçekli işletmelerden (KOBİ) kamu kuruluşlarına kadar geniş bir yelpazeyi etkilemektedir. Dijitalleşmenin artan etkisi, her ölçekten organizasyonun stratejik karar alma süreçlerini yeniden şekillendirmelerini zorunlu kılmaktadır (Alsedrah, 2023).

Dijital dönüşüm, Yönetim Bilişim Sistemleri (YBS) açısından değerlendirildiğinde, bu süreç işletmelerin bilgi yönetimi, karar verme mekanizmaları ve iş operasyonlarını doğrudan etkilemektedir. Dijital teknolojilerin sunduğu olanaklar, bilgiye erişimi hızlandırmakta, veri odaklı kararların alınmasını kolaylaştırmakta ve operasyonel süreçlerde verimliliği artırmaktadır. Bu bağlamda, dijital dönüşümün başarısı, organizasyonların bilişim sistemleri altyapılarını nasıl yapılandırdıkları ve bu sistemleri stratejik hedeflere nasıl entegre ettikleri ile yakından ilişkilidir. İyi tasarlanmış bilişim sistemleri, organizasyonların yalnızca teknolojik yeniliklere ayak uydurmasını sağlamakla kalmayarak; aynı zamanda rekabetçi bir avantaj elde etmelerine, piyasa şartlarına hızla uyum sağlamalarına ve uzun vadede sürdürülebilir bir büyüme elde etmelerine de olanak tanımaktadır (Fidan, 2024).

Bu çalışma, dijital dönüşüm sürecinin kavramsal çerçevesini YBS perspektifinden ele almayı amaçlamaktadır. Dijital dönüşüm stratejileri, yalnızca teknolojik araçların seçimi ve entegrasyonu ile sınırlı olmayıp organizasyonların bilgi yönetimi süreçleri, karar verme mekanizmaları ve iş operasyonları üzerinde derin etkiler yaratmaktadır. Bu süreçte doğru stratejilerin belirlenmesi, dijital dönüşümün başarıyla gerçekleştirilmesinde oldukça önemli bir rol oynamaktadır. Dijitalleşmenin hızla evrildiği günümüz dünyasında, teknoloji odaklı yeniliklerin iş dünyasına etkileri giderek daha önemli bir hale gelmektedir. Özellikle bilişim sistemlerinin sunduğu imkanlar, organizasyonların dijital dönüşüm süreçlerini daha etkin bir şekilde yönetmelerini sağlamaktadır. Çalışmanın odak noktası, dijital dönüşüm sürecinde organizasyonların YBS çerçevesinde nasıl bir strateji geliştirmesi gerektiği ve bu stratejilerin kurum kültürü, organizasyonel yapı, bilgi akışı ve iş süreçleri üzerindeki etkilerini kapsamlı bir şekilde açıklamaktır.

Dijital dönüşüm süreci, organizasyonel yapıların yeniden şekillendirilmesini gerektiren çok boyutlu ve dinamik bir süreçtir. Kurumlar, teknolojik altyapılarını güncellerken aynı zamanda kültürel değişimlere ve yeni iş yapma biçimlerine uyum sağlamak zorundadır. Bu nedenle, dijital dönüşüm sadece bir teknoloji geçişi değil; aynı zamanda organizasyonel bütünlüğü ve sürdürülebilir büyümeyi destekleyen bir dönüşüm olarak da ele alınmalıdır.

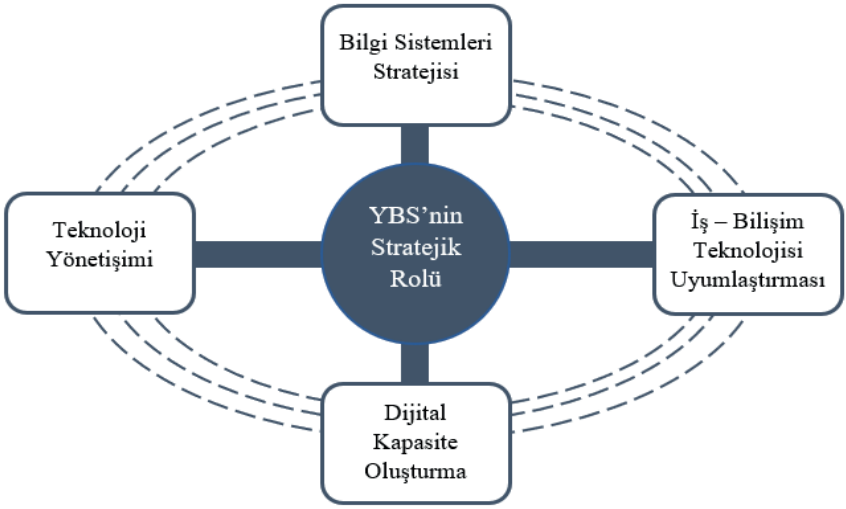
Dijital dönüşümün başarılı bir şekilde yönetilmesi, kurumların gelecekteki varlıklarını ve rekabet güçlerini doğrudan etkileyecektir. Bu süreçte belirlenen stratejiler ve bunların uygulama süreçleri, sadece akademik araştırmalar için değil; aynı zamanda işletmeler ve uygulayıcılar için de önemli bir rehber niteliği taşımaktadır. Bu çalışma, dijital dönüşümün organizasyonel yapılar üzerindeki etkilerini anlamak ve bu süreçte bilişim sistemlerinin oynadığı rolü daha iyi kavrayabilmek adına önemli bir katkı sağlamayı amaçlamaktadır.

2. YBS ve Dijital Dönüşüm Etkisi

Dijital dönüşüm, günümüz iş dünyasında kuruluşların rekabet avantajı elde etme süreçlerinde büyük önem arz etmektedir. YBS, bu dönüşüm sürecinde işletmelere stratejik bir çerçeve sunmaktadır. YBS'nin sunduğu stratejik yön, organizasyonların dijital yetkinliklerini geliştirmekte ve dijital dönüşüm süreçlerine rehberlik etmektedir.

2.1. YBS'nin Stratejik Rolü

YBS, dijitalleşme stratejilerinin temel yapı taşını oluşturmaktadır. Bu sistemler, işletmelerin dijital dönüşüm süreçlerini yönlendirmekte ve rekabet avantajı elde etmelerinde stratejik bir rol üstlenmektedir. YBS'nin stratejik rolü dört ana başlık altında incelenmektedir (Şekil 1):



Şekil 1. YBS'nin Stratejik Rolü (Kaynak: Yazar tarafından oluşturulmuştur.)

Bilgi sistemleri stratejisi: Kuruluşların dijital dönüşüm süreçlerinin merkezinde yer almaktadır. Bu strateji, işletmelerin bilgi teknolojileri (BT) yatırımlarını optimize etmekte ve iş hedeflerine uyumlu hale getirmektedir.

Bilgi sistemleri, verinin etkin bir şekilde kullanılmasını sağlamakta ve karar alma süreçlerini desteklemektedir (Henderson & Venkatraman, 1999).

İş-Bilişim teknolojisinin uyumlaştırılması: İş süreçleri ile bilgi teknolojilerinin uyumlu bir şekilde yönetilmesi, dijital dönüşümün başarılı olabilmesi için gereklidir. YBS, iş süreçleri ile BT altyapıları arasında bir köprü görevi görmektedir. İşletmelerin stratejik hedefleri ile BT'nin kapasite ve yetenekleri uyumlaştırılmakta, bu sayede verimlilik artırılmaktadır (Sledgianowski & Luftman, 2005).

Dijital kapasite oluşturma: YBS, işletmelerin dijital yetkinliklerini geliştirmede kilit bir unsur olarak öne çıkmaktadır. Dijital kapasitenin oluşturulması, işletmelerin dijital platformlar ve araçlar ile etkin bir şekilde çalışabilmesini sağlamaktadır. Bu süreç hem insan kaynağı hem de teknoloji altyapısının dijitalleşmesini kapsamaktadır (Roy, Sharaput & Toze, 2019).

Teknoloji yönetişimi: Dijital dönüşüm süreçlerinin düzenli ve sürdürülebilir bir şekilde yönetilmesini sağlamaktadır. YBS, teknoloji yatırımlarının ve projelerinin stratejik hedefler doğrultusunda yönetilmesine olanak tanımaktadır. Böylece, teknoloji kullanımı işletme değerleri ile uyumlu hale getirilmektedir (Wu, Straub & Liang, 2015).

2.2. Dijital Dönüşümde YBS'nin Konumu

Dijital dönüşüm sürecinde YBS'nin konumu oldukça merkezi bir role sahiptir. Bu sistemler, organizasyonların dijital dönüşüm süreçlerinde stratejik planlamadan değer yaratma süreçlerine kadar geniş bir yelpazede önemli katkılar sunar.

Dijital dönüşüm stratejik bir yaklaşımla ele alınmakta ve bu sürecin yönetimi için planlamalar yapılmaktadır. YBS, dijital dönüşümün stratejik olarak tasarlanmasında ve bu stratejilerin uygulanmasında merkezi bir rol üstlenmektedir. Stratejik planlama süreçlerinde YBS'nin sağladığı veri analitiği ve iş zekâsı araçları, işletmelerin dijital stratejilerini güçlendirmektedir (Wallace, 1988). Teknolojinin iş süreçleri ile entegre edilmesi, dijital dönüşümün en önemli adımlarından biridir. YBS, teknolojik altyapı ile iş süreçlerinin entegre çalışmasını sağlamakta ve bu entegrasyon sürecinde performansın iyileştirilmesine olanak tanımaktadır (Puspitasari & Jie, 2020).

YBS, işletmelerin değer yaratma süreçlerini yeniden yapılandırmakta ve dijital platformlar aracılığıyla daha verimli iş modelleri geliştirmektedir. Bu süreçler, dijitalleşmenin sunduğu yenilikçi fırsatlarla desteklenmektedir. YBS veri analitiği ve iş süreçleri otomasyonu gibi teknolojilerle değer yaratma sürecine doğrudan katkı sağlamaktadır (Pagani, 2013). Dijital dönüşüm

süreçlerinin başarısını değerlendirmek için performans ölçümleri yapılmakta ve YBS, performans verilerinin toplanmasını ve analiz edilmesini sağlayarak işletmelerin dijital dönüşüm sürecindeki ilerlemelerini takip etmektedir. Performans ölçümleri, süreçlerin sürekli iyileştirilmesine de olanak tanımaktadır (Nudurupati, Bititci, Kumar & Chan, 2011).

Bilgi sistemleri altyapısı, dijital dönüşüm süreçlerinin temelini oluşturmaktadır. Teknolojik altyapının doğru ve etkin bir şekilde kurulması, işletmelerin dijitalleşme yolculuklarında başarıya ulaşmaları için bir gerekliliktir. Bu bağlamda, bilgi sistemleri altyapısı çeşitli bileşenlerden oluşmakta ve modern bilgi sistemleri mimarisiyle desteklenmektedir.

2.3. Teknoloji Altyapısı Bileşenleri

Teknoloji altyapısı, dijital dönüşüm süreçlerinin uygulanmasında merkezi bir rol oynamaktadır. Dijital dünyanın taleplerini karşılayabilmek için güçlü ve esnek bir teknoloji altyapısına sahip olmak gerekmektedir. Bu altyapı dört ana bileşenden oluşmaktadır (Schulz, 2017):

Donanım sistemleri: Bu sistemler, dijital dönüşüm süreçlerinin temel yapı taşlarından biridir. Bilgi işlem gücünü sağlayan sunucular, depolama üniteleri ve kullanıcı cihazları gibi donanım bileşenleri, dijital altyapının temelini oluşturmaktadır. Bu sistemlerin güvenilir, ölçeklenebilir ve yüksek performanslı olması, dijital dönüşüm süreçlerinin başarısı için oldukça önemlidir.

Yazılım platformları: Donanım sistemlerinin üzerine inşa edilen yazılım platformları, işletmelerin dijital dönüşüm stratejilerini desteklemektedir. Kurumsal yazılım çözümleri, uygulama geliştirme platformları ve veri yönetim sistemleri gibi yazılım bileşenleri, iş süreçlerinin dijitalleştirilmesinde kullanılmaktadır. Bu platformlar, esnek ve kullanıcı dostu olmalıdır, böylece dijital dönüşüm süreçleri sorunsuz bir şekilde ilerleyebilmektedir.

Ağ ve iletişim sistemleri: Dijital dönüşümde işletmelerin iletişim ve veri paylaşımını etkin bir şekilde yönetmeleri gerekmektedir. Ağ altyapısı, bu sürecin başarısını doğrudan etkilemektedir. Yüksek hızlı internet bağlantıları, güvenli iletişim ağları ve veri merkezleri, işletmelerin dijital işlemlerini kesintisiz ve güvenilir bir şekilde yürütmelerini sağlamaktadır.

Veri depolama ve yönetim sistemleri: Dijital çağda veri, işletmelerin en değerli varlıklarından biri haline gelmiştir. Veri depolama ve yönetim sistemleri, büyük veri yığınlarının depolanmasını, işlenmesini ve analiz edilmesini sağlamaktadır. Etkin bir veri yönetimi, dijital dönüşüm sürecinde işletmelerin rekabet avantajı elde etmelerine yardımcı olmaktadır.

2.4. Modern Bilgi Sistemleri Mimarisi

Geleneksel bilgi sistemleri mimarisi, dijital dönüşüm süreçlerinde yetersiz kalmaktadır. Bu nedenle, modern bilgi sistemleri mimarisi işletmelerin daha esnek, ölçeklenebilir ve modüler yapılarla dijital dönüşüm yolculuklarına uyum sağlamalarına yardımcı olmaktadır (Teubner & Stockhinger, 2020).

Mikroservis mimarisi: Bu mimari, yazılım uygulamalarının küçük ve bağımsız hizmetlere bölünerek yönetilmesini sağlamaktadır. Her bir mikroservis, belirli bir işlevi yerine getirmekte ve diğer mikroservislerle uyumlu bir şekilde çalışmaktadır. Bu yapı, esnekliği artırmakta ve dijital dönüşüm süreçlerinde hızlı adaptasyona olanak tanımaktadır.

API ekonomisi: API'ler (Uygulama Programlama Arayüzleri), dijital platformlar ve uygulamalar arasında veri alışverişini sağlayan köprülerdir. API ekonomisi, işletmelerin yeni iş modelleri geliştirmelerini ve dijital ekosistemlerle entegre olmalarını sağlamaktadır. API'ler, dijital dönüşümün hızlandırılmasında tetikleyici bir rol oynamaktadır.

Bulut bilişim altyapısı: Bulut bilişim, dijital dönüşüm süreçlerinde işletmelere büyük avantajlar sunmaktadır. Esnek depolama ve işlem gücü sağlayan bulut altyapıları, işletmelerin dijital dönüşüm stratejilerini hızla hayata geçirmelerine olanak tanımaktadır. Ayrıca, bulut bilişim, maliyet tasarrufu sağlamakta ve ölçeklenebilirliği artırmaktadır.

Hibrit sistemler: Hibrit bilgi sistemleri, geleneksel veri merkezleri ile bulut bilişim altyapılarını birleştirmektedir. Bu sistemler, işletmelere hem güvenlik hem de esneklik sunmakta; dijital dönüşüm sürecinde veri yönetimi ve iş sürekliliği açısından önemli avantajlar sağlamaktadır.

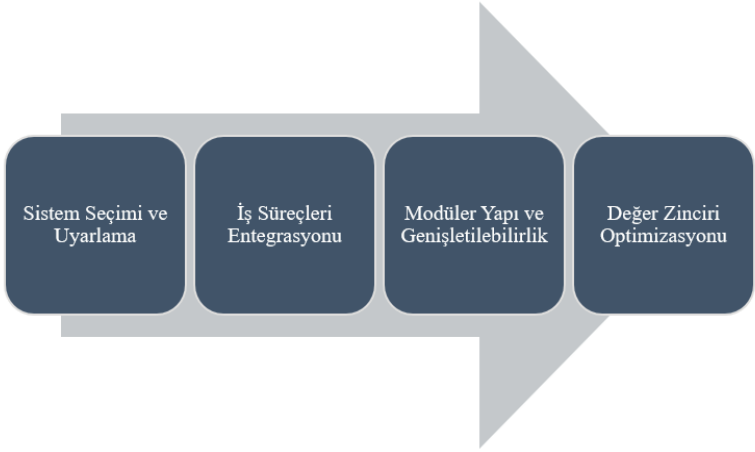
3. Kurumsal Sistemler ve Dijital Entegrasyon

Dijital dönüşüm sürecinde, kurumsal sistemler işletmelerin verimliliklerini artırmak ve iş süreçlerini dijitalleştirmek amacıyla önemli bir rol üstlenmektedir. Bu sistemler, organizasyonel süreçlerin bütünleşmesini ve dijital entegrasyonun sağlanmasını kolaylaştırmaktadır. Kurumsal kaynak planlaması (ERP), müşteri ilişkileri yönetimi (CRM) ve tedarik zinciri yönetimi (SCM) gibi sistemler, dijital dönüşüm sürecinin vazgeçilmez bileşenleri arasında yer almaktadır.

3.1. Kurumsal Kaynak Planlaması (ERP)

ERP sistemleri, işletmelerin tüm kaynaklarını entegre bir şekilde yönetmelerini sağlayan yazılımlardır. ERP sistemleri, işletmelerin iş süreçlerini otomatikleştirerek verimliliği artırmakta ve maliyetleri düşürmektedir

(Kitsantas, Vazakidis & Stefanou, 2020). Bu süreçlerin dijital entegrasyonu, işletmelerin hızla değişen pazar koşullarına uyum sağlamalarını mümkün kılmaktadır (Şekil 2).



Şekil 2. ERP Sistemleri (Kaynak: Yazar tarafından oluşturulmuştur.)

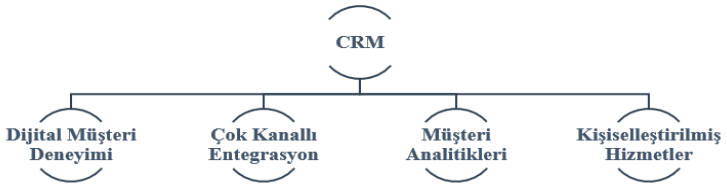
ERP sistemleri, işletmelerin ihtiyaçlarına göre özelleştirilebilmektedir. Sistem seçimi, işletmenin ölçeği, sektörü ve iş süreçlerine uygun olarak yapılmaktadır. Uyarlama sürecinde, ERP sistemlerinin işletme gereksinimlerine göre optimize edilmesi sağlanmakta ve bu sayede sistemin verimliliği artırılmaktadır (Yılmaz Börekçi, Büyüksaatçı Kiriş & Batmaca, 2020). ERP sistemleri, farklı iş birimlerinin süreçlerini entegre ederek etkinliği artırmaktadır. Satın alma, üretim, satış ve finans gibi süreçlerin tek bir sistem üzerinden yönetilmesi, işletmelerin karar alma süreçlerinde hız ve doğruluk kazanmalarına yardımcı olmaktadır (Wijaya & Utomo, 2021; Abikoye, Akinwunmi, Adelaja, Umeorah & Ogunsuji, 2024).

Modüler bir yapıya sahip olan ERP sistemleri, işletmelerin ihtiyaçlarına göre ek modüller eklemelerine olanak tanımaktadır. Bu yapı, ERP sistemlerinin zamanla genişletilebilmesini ve yeni işlevlerin kolayca entegre edilebilmesini sağlamaktadır. Ayrıca, ERP sistemleri işletmelerin değer zincirini optimize ederek tüm süreçlerde verimlilik artışı sağlamaktadır. Hammaddeden son ürüne kadar olan süreçlerin izlenmesi ve yönetilmesi, ERP sistemleri ile etkin bir şekilde gerçekleştirilmektedir (Jawad & Balázs, 2024).

3.2. Müşteri İlişkileri Yönetimi (CRM)

CRM sistemleri, dijital çağda müşteri memnuniyetini ve sadakatini artırmak için önemli bir araç haline gelmiştir (Tuna & Görmez, 2024).

CRM sistemleri, müşteri verilerini toplayarak ve analiz ederek, işletmelerin müşterilerine daha iyi hizmet sunmalarını sağlamaktadır. Dijital dönüşüm sürecinde, CRM sistemlerinin etkin kullanımı rekabet avantajı yaratmaktadır (Gao, Melero & Sese, 2020). CRM sistemi işleyici dört temel başlıkta ele alınmıştır (Şekil 3).



Şekil 3. CRM Sistemleri (Kaynak: Yazar tarafından oluşturulmuştur.)

Dijital müşteri deneyimi: CRM sistemleri, müşterilere sunulan dijital deneyimi optimize etmektedir. Müşteri etkileşimlerinin her aşamasında kişiselleştirilmiş deneyimler sunarak, müşteri memnuniyeti artırılmaktadır.

Çok kanallı entegrasyon: CRM sistemleri, işletmelerin müşterileriyle birden fazla kanal üzerinden iletişim kurmasını sağlamaktadır. Sosyal medya, e-posta, telefon gibi kanalların entegre edilmesi, müşteri ilişkilerinin bütüncül bir yaklaşımla yönetilmesine imkân tanımaktadır.

Müşteri analitikleri: CRM sistemleri, müşteri davranışları ve tercihleri hakkında veri toplamakta ve bu verileri analiz etmektedir. Müşteri analitikleri, işletmelerin daha etkili pazarlama stratejileri geliştirmelerine ve müşteri ilişkilerini optimize etmelerine olanak verir.

Kişiselleştirilmiş hizmetler: CRM sistemleri, müşterilere kişiselleştirilmiş hizmetler sunulmasını kolaylaştırmaktadır. Müşteri profilleri oluşturularak, her müşteriye özel çözümler sunulmakta ve bu sayede müşteri sadakati artırılmaktadır.

3.3. Tedarik Zinciri Yönetimi (SCM)

SCM sistemleri, işletmelerin tedarik zinciri süreçlerini dijitalleştirerek, süreçlerin daha verimli ve şeffaf bir şekilde yönetilmesini sağlamaktadır (Sahoo, Goswami, Sarkar & Mitra, 2023). Dijital dönüşüm, tedarik zincirinin her aşamasında izlenebilirlik ve entegrasyon sağlamaktadır (Şekil 4).

Şekil 4. SCM Sistemlerinin Dijitalleşmesinin Avantajları (Kaynak: Yazar tarafından oluşturulmuştur.)

Dijital tedarik zinciri: Dijital tedarik zinciri, tedarikçiden müşteriye kadar olan tüm sürecin dijital platformlar üzerinden yönetilmesini sağlamaktadır. Tedarik zincirindeki her aşamanın dijitalleşmesi, verimliliği artırmakta ve maliyetleri düşürmektedir.

Gerçek zamanlı izleme: SCM sistemleri, tedarik zinciri süreçlerinin gerçek zamanlı olarak izlenmesine olanak tanımaktadır. Üretim, lojistik ve dağıtım süreçlerinin her aşamasında anlık veriler elde edilmekte ve bu veriler, operasyonel kararların hızla alınmasını sağlamaktadır.

Tedarikçi entegrasyonu: Tedarik zincirinde yer alan tedarikçilerin dijital sistemlerle entegre edilmesi, süreçlerin daha etkin bir şekilde yönetilmesine olanak tanımaktadır. Tedarikçilerin performansı izlenmekte ve bu veriler ışığında tedarik zinciri optimizasyonu gerçekleştirilmektedir.

Lojistik optimizasyonu: Dijital SCM sistemleri, lojistik süreçlerin optimize edilmesini sağlamaktadır. Sevkiyatların planlanması, envanter yönetimi ve dağıtım süreçlerinin optimize edilmesiyle işletmeler, maliyet avantajı elde etmekte ve müşteri memnuniyetini artırmaktadır.

Dijital dönüşüm süreçlerinde veri, en değerli kaynaklardan biri haline gelmiştir. Verinin etkin bir şekilde yönetilmesi ve analiz edilmesi, işletmelere rekabet avantajı sağlamakta ve stratejik karar alma süreçlerini iyileştirmektedir. Veri yönetimi ve analitik, işletmelerin dijital çağda başarılı olabilmeleri için hayati öneme sahiptir.

3.4. Kurumsal Veri Yönetimi

Kurumsal veri yönetimi, işletmelerin sahip oldukları büyük veri yığınlarının düzenlenmesi, korunması ve etkin bir şekilde kullanılması süreçlerini kapsamaktadır. Dijital dönüşümün başarıya ulaşması, verinin doğru şekilde yönetilmesine bağlıdır (Nambiar & Mundra, 2022). Veri yönetiminde dört temel unsur ön plana çıkmaktadır:

Veri mimarisi: Veri mimarisi, işletmelerin veri kaynaklarını nasıl düzenleyeceklerini ve veriyi nasıl yöneteceklerini belirleyen yapısal bir çerçevedir. İyi tasarlanmış bir veri mimarisi, verinin farklı sistemler ve süreçler arasında entegre edilmesini sağlamakta ve işletmelerin veri yönetim stratejilerini optimize etmektedir.

Veri kalitesi: Dijital dünyada verinin kalitesi, işletmelerin stratejik karar alma süreçlerinde büyük önem taşımaktadır. Veri kalitesinin sağlanması, doğru ve güvenilir veriye dayalı kararların alınmasını mümkün kılmaktadır. Veri yönetimi süreçlerinde veri kalitesinin iyileştirilmesi, işletmelerin verimliliğini artırmaktadır.

Master veri yönetimi: Master veri yönetimi, işletmelerin stratejik veri varlıklarını tek bir çatı altında bütüncül bir şekilde yönetmelerine imkân tanıyan bir süreçtir. Bu yönetim modeli, işletme genelinde tutarlılığı ve doğruluğu artırmakta, veri kaynaklarının birbiriyle uyumlu olmasını sağlamaktadır.

Veri yönetişimi: Veri yönetişimi verinin bütünlüğünü, güvenliğini ve gizliliğini koruma süreçlerini kapsamaktadır. İşletmelerin veri politikaları ve düzenlemelere uygunluğu, veri yönetişimi süreçleri ile sağlanmaktadır. Bu süreçler, veri güvenliğini artırmakta ve işletmelerin dijital dönüşüm süreçlerinde güvenilir veri altyapılarına sahip olmasına olanak tanımaktadır.

3.5. İş Zekâsı ve Analitik

İş zekâsı ve analitik, verilerin işletmeler için anlamlı bilgilere dönüştürülmesi sürecini kapsamaktadır. Dijital dönüşüm ile birlikte veri analitiğinin önemi artmakta ve işletmelerin stratejik kararlarını desteklemektedir. Analitik yaklaşımlar (Şekil 5), verinin sadece geçmişi anlamak için değil, geleceği öngörmek ve kararları yönlendirmek için de kullanılmasına olanak tanımaktadır.

Şekil 5. Analitik Türleri (Kaynak: Yazar tarafından oluşturulmuştur.)

Tanımlayıcı analitik: Tanımlayıcı analitik, geçmiş verileri analiz ederek, işletmelerin geçmişte neler yaşandığını anlamalarına yardımcı olmaktadır (Raghupathi & Raghupathi, 2021). Bu analizler, işletmelerin mevcut durumu değerlendirmelerine ve iyileştirme fırsatlarını belirlemelerine olanak tanımaktadır.

Teşhis analitiği: Teşhis analitiği, bir olayın ya da durumun neden meydana geldiğini anlamak amacıyla kullanılan bir analiz türüdür. Geçmiş verilerden elde edilen bulguların arkasındaki nedenleri araştırarak, işletmelerin performans düşüşleri, müşteri kayıpları ya da diğer olumsuz sonuçlar hakkında daha derinlemesine bilgi edinmelerine olanak sağlar (Wolniak & Grebski, 2023). Bu analiz, işletmelerin geçmişteki hataları belirlemelerine ve bu hataların tekrarını önlemeye yönelik stratejiler geliştirmelerine katkıda bulunmaktadır.

Tahminsel analitik: Tahminsel analitik, geçmiş verileri kullanarak gelecekteki olası eğilimleri ve sonuçları öngörmeye yönelik bir analiz türüdür (Chen, Li & Wang, 2022). Makine öğrenimi ve istatistiksel modeller kullanılarak yapılan bu analizler, işletmelere gelecekteki pazar koşulları ve müşteri davranışları hakkında değerli içgörüler sunmaktadır.

Normatif analitik: Normatif analitik, işletmelere belirli bir problem veya fırsat karşısında ne yapmaları gerektiği konusunda öneriler sunmaktadır (Wissuchek & Zschech, 2024). Bu tür analizler, karar destek sistemleri ile birlikte kullanılarak işletmelerin daha etkin stratejik kararlar almasına olanak tanımaktadır.

4. Dijital İş Süreçleri Yönetimi

Dijital dönüşüm, işletmelerin iş süreçlerini daha verimli ve esnek hale getirmek amacıyla iş süreçleri yönetiminde devrim niteliğinde değişiklikler sunmaktadır. Dijital iş süreçleri yönetimi, süreçlerin otomasyonu ve iyileştirilmesi yoluyla işletmelerin daha rekabetçi ve yenilikçi olmasını sağlamaktadır.

4.1. Süreç Otomasyonu

Süreç otomasyonu, dijital dönüşümün en temel yapı taşlarından biri olarak öne çıkmaktadır. İş süreçlerinin otomatik hale getirilmesi, insan hatalarının minimize edilmesi, verimliliğin artırılması ve maliyetlerin düşürülmesi gibi birçok avantaj sağlamaktadır. Özellikle tekrarlayan işlerin otomatik sistemler tarafından gerçekleştirilmesi yoluyla operasyonel etkinlik artırılmaktadır (Chakraborti, Isahagian, Khalaf, Khazaeni, Muthusamy, Rizk & Unuvar, 2020). Robotik Süreç Otomasyonu (RPA), yazılım robotlarının insan müdahalesine gerek kalmadan belirli iş süreçlerini yürütmesine olanak tanımaktadır. Bu teknoloji, özellikle rutin ve tekrarlayan görevlerde kullanılarak iş gücü maliyetlerini azaltmakta ve verimliliği artırmaktadır. RPA, işletmelerin dijital süreç yönetimine geçişini hızlandırmaktadır. İş akışı yönetimi, iş süreçlerinin belirli bir düzen içinde otomatik olarak gerçekleştirilmesini sağlamaktadır. İş akışı yönetim sistemleri, süreçlerin belirli adımlarla ilerlemesini ve farklı departmanlar arasında işlerin organize bir şekilde yürütülmesini kolaylaştırmaktadır. Süreç madenciliği, mevcut iş süreçlerinin nasıl işlediğini analiz etmek ve iyileştirme fırsatlarını belirlemek için kullanılan bir tekniktir. Bu teknik, dijital sistemler üzerinde gerçekleşen süreçlerin veri izlerini analiz ederek süreçlerin performansını artırmaya yönelik içgörüler sunmaktadır. Akıllı otomasyon ise yapay zekâ ve makine öğrenimi gibi ileri teknolojiler kullanarak süreçlerin otomatik hale getirilmesini sağlamaktadır (Erbey & Barışçı, 2022). Bu tür otomasyon, sadece belirli adımları değil, aynı zamanda karar alma süreçlerini de otomatikleştirerek iş süreçlerini daha etkin ve akıllı hale getirmektedir.

4.2. Süreç İyileştirme ve İnovasyon

Dijitalleşme ile iş süreçlerinde sürekli iyileştirme ve inovasyon fırsatları ortaya çıkmaktadır. Dijital süreç iyileştirme, süreçlerin daha verimli hale getirilmesi ve inovasyonun teşvik edilmesi yoluyla işletmelere rekabet avantajı sağlamaktadır. Bu süreç, hem mevcut iş süreçlerinin optimize edilmesini hem de tamamen yeni süreçlerin tasarlanmasını içermektedir (Ahmad & Van Looy, 2020).

Süreç analizi, mevcut iş süreçlerinin performansını değerlendirmek ve iyileştirme alanlarını belirlemek için yapılan bir çalışmadır (Zhang, 2013). Süreç modelleme ise bu süreçlerin görselleştirilmesi ve optimize edilmesi için kullanılan bir tekniktir (Mili, Tremblay, Jaoude, Lefebvre, Elabed & Boussaidi, 2010). Dijital dönüşüm, bu analiz ve modelleme çalışmalarını daha detaylı ve veriye dayalı bir hale getirmektedir.

Süreç optimizasyonu, iş süreçlerinin daha verimli hale getirilmesi için yapılan iyileştirme çalışmalarını kapsamaktadır. Dijital süreç optimizasyonu, işletmelerin kaynaklarını daha etkin kullanmasını sağlarken operasyonel maliyetleri de düşürmektedir. Veri analizine dayalı süreç optimizasyonu, işletmelerin rekabet avantajı elde etmesine olanak tanımaktadır.

Dijital süreç transformasyonu, iş süreçlerinin tamamen dijital bir yapıya dönüştürülmesini ifade etmektedir (Zaoui & Souissi, 2020). Bu dönüşüm, dijital araçlar ve platformlar kullanılarak süreçlerin daha hızlı, verimli ve esnek hale getirilmesini sağlamaktadır. İşletmeler, dijital dönüşüm yolculuklarında bu süreç transformasyonu sayesinde yenilikçi iş modelleri geliştirmektedir.

Çevik süreç yönetimi ise hızlı değişimlere yanıt verebilen esnek ve uyumlu iş süreçleri oluşturmayı hedeflemektedir (Erickson, Lyytinen & Siau, 2005). Dijital dönüşüm, çevik yaklaşımlar sayesinde işletmelerin hızla değişen pazar koşullarına uyum sağlamasına ve sürekli iyileştirme süreçlerini daha etkin bir şekilde yönetmesine olanak tanımaktadır.

Dijital dönüşüm projeleri, işletmelerin rekabet avantajı kazanmasını sağlayan stratejik inisiyatiflerdir. Ancak bu projelerin başarılı bir şekilde hayata geçirilmesi, etkin bir proje yönetimi ve değişim yönetimi süreci gerektirmektedir. Hem geleneksel hem de çevik yaklaşımlar dijital dönüşüm projelerinde kullanılmakta ve organizasyonel değişim sürecinin titizlikle yönetilmesi gerekmektedir.

4.3. Proje Yönetim Metodolojileri

Dijital dönüşüm projelerinin yönetiminde, proje yönetim metodolojileri büyük önem taşımaktadır. Projelerin büyüklüğüne, karmaşıklığına ve organizasyon yapısına bağlı olarak farklı metodolojiler (Şekil 6) benimsenmektedir (Al-Saqqa, Sawalha & AbdelNabi, 2020).

Şekil 6. Proje Yönetiminde Metodoloji (Kaynak: Yazar tarafından oluşturulmuştur.)

Geleneksel metodolojiler: Geleneksel proje yönetim metodolojileri, aşamalı ve yapılandırılmış bir yaklaşıma dayanmaktadır. Bu metodolojiler, projelerin belirli bir plan çerçevesinde ilerlemesini sağlamakta ve her bir aşamanın tamamlanmasıyla bir sonraki aşamaya geçiş yapılmaktadır. Özellikle büyük ve sabit projelerde tercih edilmektedir.

Çevik metodolojiler: Çevik metodolojiler, hızla değişen dijital projelerde esneklik ve adaptasyon sağlamaktadır. Scrum ve Kanban gibi çevik yaklaşımlar, projelerin daha küçük parçalara bölünmesini ve bu parçaların iteratif olarak geliştirilmesini teşvik etmektedir. Dijital dönüşüm projelerinde çevik metodolojiler, müşteri taleplerine hızlı yanıt verme ve dinamik bir proje yönetimi süreci oluşturma imkânı sunmaktadır.

Hibrit yaklaşımlar: Hibrit metodolojiler geleneksel ve çevik yaklaşımların bir arada kullanıldığı proje yönetim yaklaşımlarını içermektedir. Bu yöntem, projelerin belirli kısımlarında planlama ve yapılandırılmış süreçlere bağlı kalırken diğer kısımlarında çevik yaklaşımlar ile esneklik sağlamaktadır. Özellikle karmaşık dijital dönüşüm projelerinde sıklıkla tercih edilmektedir.

DevOps uygulamaları: DevOps, yazılım geliştirme ve operasyon süreçlerini birleştirerek, projelerin daha hızlı ve hatasız bir şekilde hayata geçirilmesini sağlamaktadır. DevOps uygulamaları, sürekli entegrasyon, otomasyon ve süreç optimizasyonu yoluyla dijital projelerin başarıya ulaşmasını hızlandırmaktadır.

4.4. Değişim Yönetimi

Dijital dönüşüm projeleri, sadece teknolojik bir dönüşüm değil; aynı zamanda organizasyonel bir değişim anlamına gelmektedir. Bu nedenle değişim yönetimi, dijital dönüşüm projelerinin başarısı için dikkate alınması gereken bir süreçtir. Etkili değişim yönetimi, organizasyonel kültürün dönüşüm sürecine uyum sağlamasını ve çalışanların bu sürece adapte olmasını desteklemektedir (Hanelt, Bohnsack, Marz & Antunes Marante, 2021).

Organizasyonel hazırlık: Dijital dönüşüm projelerine başlamadan önce organizasyonun bu değişime hazır olup olmadığının değerlendirilmesi gerekmektedir. Organizasyonel hazırlık süreci, mevcut iş gücünün dijital dönüşüme adaptasyon yetkinliklerinin değerlendirilmesi ve gerekli kaynakların sağlanmasını kapsamaktadır.

Dijital yetkinlik geliştirme: Dijital dönüşüm projelerinin başarılı olabilmesi için çalışanların dijital yetkinliklerinin artırılması gerekmektedir (Yılmaz, 2023). Eğitim programları ve dijital beceri geliştirme çalışmaları, organizasyonun dijital dönüşüm sürecinde daha verimli olmasına katkıda bulunmaktadır. Bu süreç, çalışanların yeni dijital araçları ve platformları kullanabilme kapasitelerini artırmayı hedeflemektedir.

İletişim stratejileri: Dijital dönüşüm projelerinde değişim yönetiminin en önemli unsurlarından biri etkili iletişimdir. İletişim stratejileri, organizasyondaki tüm paydaşların projeye dair bilgilendirilmesini ve projeye destek vermesini sağlamaktadır. İyi yapılandırılmış bir iletişim planı, projenin her aşamasında tüm tarafların katılımını ve uyumunu artırmaktadır.

Direnç yönetimi: Değişim süreçlerinde organizasyonel direnç, kaçınılmaz bir durumdur. Dijital dönüşüm projelerinde de bazı çalışanlar değişime karşı direnç gösterebilir. Direnç yönetimi, bu dirençleri önceden tespit etmek ve çözüm yolları geliştirmek için stratejik bir yaklaşımdır. Etkili bir direnç yönetimi, dijital dönüşümün daha sorunsuz bir şekilde uygulanmasını sağlamaktadır.

5. Bilgi Sistemleri Güvenliği ve Risk Yönetimi

Dijital dönüşüm süreçlerinde, bilgi sistemlerinin güvenliği ve risk yönetimi işletmelerin en önemli önceliklerinden biri haline gelmiştir. Teknolojinin iş süreçlerine entegrasyonu, aynı zamanda çeşitli siber tehditleri de beraberinde getirmekte ve bu tehditlere karşı proaktif bir güvenlik ve risk yönetimi yaklaşımı gerekmektedir (Saeed, Altamimi, Alkayyal, Alshehri & Alabbad, 2023). Bu bağlamda, bilgi sistemleri güvenliği stratejik bir şekilde ele alınmalıdır.

5.1. Siber Güvenlik Stratejileri

Siber güvenlik stratejileri, işletmelerin dijital varlıklarını koruma, tehditleri tespit etme ve bu tehditlere karşı koyma süreçlerini kapsar (Şekil 7).

Şekil 7. Siber Güvenlik Stratejileri (Kaynak: Yazar tarafından oluşturulmuştur.)

Güvenlik mimarisi: İşletmelerin siber güvenlik altyapısının yapı taşlarını oluşturmaktadır. Bu mimari, güvenlik duvarları, ağ güvenliği, veri şifreleme ve diğer güvenlik önlemlerinin entegrasyonunu içerir. Güvenlik mimarisi, dijital altyapının her seviyesinde güvenliği sağlamak üzere tasarlanmıştır.

Tehdit yönetimi: Siber saldırılara ve güvenlik ihlallerine karşı sürekli izleme ve müdahale süreçlerini kapsamaktadır. Bu süreçte, siber tehditlerin önceden tespit edilmesi ve bu tehditlere hızlı bir şekilde yanıt verilmesi önemlidir. Tehdit yönetimi sistemleri, işletmelerin güvenlik açıklarını tespit etmelerine ve bu açıkları gidermelerine yardımcı olmaktadır.

Kimlik ve erişim yönetimi: Yetkisiz erişimleri önlemek ve kullanıcıların sadece gerekli bilgilere erişimini sağlamak için kullanılan bir güvenlik stratejisidir. Bu süreç, kullanıcı kimlik doğrulama yöntemleri, erişim kontrol politikaları ve izleme mekanizmaları ile desteklenmektedir.

Uyum ve denetim: İşletmeler, bilgi güvenliği düzenlemelerine ve standartlarına uyum sağlamak zorundadır. Uyum süreçleri hem işletmenin iç politikaları hem de ulusal ve uluslararası güvenlik düzenlemeleri çerçevesinde yürütülmektedir. Denetim ise, işletmelerin siber güvenlik önlemlerini düzenli olarak değerlendirmek ve iyileştirmek için yapılan bir süreçtir.

5.2. Risk Yönetimi

Risk yönetimi, işletmelerin bilgi teknolojileri altyapısında karşılaşabilecekleri riskleri önceden belirlemeyi ve bu risklere karşı proaktif önlemler almayı amaçlamaktadır (Şekil 8). BT risk yönetimi, işletmenin iş sürekliliğini sağlamada ve veri güvenliğini korumada hayati öneme sahip bir süreçtir (Oudada & Daoui, 2023).

Şekil 8. Risk Yönetimi Bileşenleri (Kaynak: Yazar tarafından oluşturulmuştur.)

BT risk değerlendirmesi: İşletmenin karşı karşıya olduğu potansiyel riskleri belirlemek ve bu risklerin olası etkilerini değerlendirmek için yapılan bir analiz sürecidir. Risk değerlendirmesi siber tehditler, veri ihlalleri, sistem arızaları ve insan hataları gibi çeşitli unsurları dikkate almaktadır.

İş sürekliliği planlaması, bir siber saldırı, sistem arızası ya da doğal afet durumunda işletmenin operasyonlarını sürdürebilmesi için geliştirilen stratejileri içermektedir. Bu planlama süreci, önemli iş süreçlerinin kesintisiz olarak devam etmesini ve veri kayıplarının en aza indirilmesini hedeflemektedir.

Felaket kurtarma: Kurtarma planları ciddi bilgi güvenliği ihlalleri ya da felaket senaryolarında işletmenin veri ve operasyonel altyapısını hızla geri kazanmasını sağlamaktadır. Bu planlar, veri yedekleme stratejileri ve sistemlerin hızla yeniden ayağa kaldırılması için gerekli prosedürleri içerir.

Güvenlik politikaları: İşletmenin dijital güvenlik konusundaki genel yaklaşımını belirlemektedir. Bu politikalar, kullanıcıların güvenlik bilincini artırmak, siber saldırılara karşı tedbir almak ve işletmenin genel güvenlik stratejilerini yönlendirmek için oluşturulmaktadır. Güvenlik politikaları, işletmenin güvenlik kültürünü güçlendiren önemli bir unsurdur.

6. Sonuç ve Öneriler

Dijital dönüşüm, günümüz işletmeleri için yalnızca teknolojik bir yenilik değil; aynı zamanda stratejik bir zorunluluk haline gelmiştir. YBS, bu dönüşüm sürecinde işletmelerin stratejik hedeflerine ulaşmalarını destekleyen önemli bir yapı taşı olarak öne çıkmaktadır. Bu çalışma, YBS perspektifinden dijital dönüşümün temel bileşenlerini ve bu süreçteki stratejik rolünü ele alarak, organizasyonların dijitalleşme sürecinde nasıl bir yol izlemeleri gerektiğine dair kapsamlı bir inceleme sunmaktadır.

İlk olarak, YBS'nin stratejik rolü, bilgi sistemlerinin yalnızca operasyonel bir araç değil, aynı zamanda rekabet avantajı sağlayan bir unsur olduğunu göstermektedir. YBS, işletmelerin bilgi teknolojileri stratejilerini iş süreçleri ile uyumlu hale getirerek dijital kapasitenin artırılmasına ve teknoloji yönetişiminin daha etkin bir şekilde gerçekleştirilmesine olanak tanımaktadır. Bu sayede işletmeler, dijitalleşmenin sunduğu fırsatlardan maksimum faydayı elde edebilmektedir.

Dijitalleşmenin başarılı olabilmesi için işletmelerin stratejik planlama süreçlerini dijitalleştirmeleri, iş süreçlerini teknoloji ile entegre etmeleri ve sürekli olarak performans ölçümü yaparak bu süreçleri iyileştirmeleri gerekmektedir. Bu yaklaşım, dijital dönüşümün işletmelere uzun vadeli değer yaratma potansiyelini ortaya koymaktadır.

Bilgi sistemleri altyapısının dijital dönüşüm üzerindeki etkisi de önemli bir başlık olarak ele alınmıştır. Donanım sistemleri, yazılım platformları, ağ ve iletişim sistemleri gibi altyapı bileşenleri, dijital dönüşüm süreçlerinin temel yapı taşlarını oluşturmaktadır. Ayrıca, mikroservis mimarisi, API ekonomisi, bulut bilişim ve hibrit sistemler gibi modern bilgi sistemleri mimarileri, işletmelere daha esnek ve ölçeklenebilir dijital altyapılar sunarak dönüşüm süreçlerini hızlandırmaktadır.

Kurumsal sistemler ve dijital entegrasyon ise işletmelerin iş süreçlerini daha verimli hale getirmekte ve değer zincirinde optimizasyon sağlamaktadır. ERP, CRM ve SCM gibi kurumsal sistemler, dijital dönüşüm süreçlerinde iş süreçlerinin entegrasyonunu kolaylaştırarak işletmelerin dijitalleşme yolculuğunu desteklemektedir. Bu sistemler hem iç hem de dış paydaşlar arasındaki etkileşimi optimize ederek işletmelere daha rekabetçi ve müşteri odaklı bir yapıya kavuşma imkânı sunmaktadır.

Veri yönetimi ve analitik, dijital çağın en kilit unsurlarından biri haline gelmiştir. Verinin doğru bir şekilde yönetilmesi, işletmelere stratejik karar alma süreçlerinde önemli bir avantaj sağlamaktadır. Ayrıca, iş zekâsı ve analitik araçlar, geçmişi analiz etmekle kalmayıp geleceği öngörme ve kararları yönlendirme konusunda da işletmelere güçlü bir altyapı sunmaktadır. Bu, işletmelerin daha öngörülü ve esnek olmasına katkı sağlamaktadır.

Dijital iş süreçleri yönetimi, süreç otomasyonu ve süreç iyileştirme konularında önemli kazanımlar sağlamaktadır. Robotik süreç otomasyonu, iş akışı yönetimi ve akıllı otomasyon gibi yenilikçi teknolojiler, iş süreçlerini optimize etmekte ve işletmelere operasyonel verimlilik kazandırmaktadır. Ayrıca, çevik süreç yönetimi ve dijital süreç transformasyonu, işletmelerin sürekli değişen dijital dünyaya uyum sağlamalarına olanak tanımaktadır.

Bilgi sistemleri güvenliği ve risk yönetimi ise dijital dönüşüm süreçlerinin başarısı için hayati öneme sahiptir. Güvenlik tehditlerinin arttığı dijital çağda, siber güvenlik stratejileri ve BT risk yönetimi süreçleri işletmelerin dijital altyapılarını koruma altına almalarını sağlamaktadır. Bu süreçlerin etkin bir şekilde yönetilmesi, dijital dönüşüm sürecinde güvenliği artırarak iş sürekliliğini garanti altına almaktadır.

Ayrıca dijital dönüşüm projelerinin yönetimi, proje yönetim metodolojileri ve değişim yönetimi süreçleri ile ele alınmıştır. İşletmelerin dijital dönüşüm süreçlerini başarılı bir şekilde hayata geçirebilmeleri için çevik, hibrit ve DevOps gibi metodolojileri benimsemeleri gerekmektedir. Aynı zamanda, değişim yönetimi süreçleri ile organizasyonel hazırlık, dijital yetkinlik geliştirme ve direnç yönetimi gibi unsurların titizlikle ele alınması, dönüşümün sürdürülebilirliğini sağlamaktadır. Bu değerlendirmeler ışığında, YBS perspektifinden dijital dönüşüm, işletmelerin sadece teknolojik bir değişim değil; aynı zamanda stratejik bir dönüşüm gerçekleştirmelerine olanak tanımaktadır. İşletmelerin bu süreçte stratejik bir bakış açısıyla hareket etmeleri, modern teknolojileri etkin bir şekilde kullanmaları ve organizasyonel dönüşüme uyum sağlamaları dijital dönüşümün başarısı için kritik öneme sahiptir.

YBS, sürekli gelişen teknolojiler ve iş modelleri ile evrilmektedir. Yapay zekâ, otomasyon ve diğer yeni nesil teknolojiler, YBS'nin geleceğini şekillendirmekte ve organizasyonel dönüşüm süreçlerinde önemli rol oynamaktadır. Yapay zekâ ve otomasyon teknolojileri, YBS'nin geleceğinde büyük bir etki yaratmakta; AI ile iş süreçleri daha akıllı ve verimli hale getirilmekte, otomasyon sayesinde manuel işlemler en aza indirilmektedir. Bu teknolojiler, YBS'nin iş süreçlerini dönüştürmek adına yeni fırsatlar sunmaktadır. Bulut bilişim, nesnelerin interneti (IoT), blokzincir ve 5G gibi yeni nesil teknolojiler, YBS'nin altyapısını dönüştürmekte; verilerin daha hızlı işlenmesini, paylaşılmasını ve analiz edilmesini mümkün kılarak, işletmelerin dijital dönüşüm süreçlerinde daha yenilikçi çözümler geliştirmelerini sağlamaktadır.

Dijital dönüşüm süreçleriyle birlikte, işletmelerde yeni yetkinliklere duyulan ihtiyaç da artmakta; çalışanların dijital becerilerinin geliştirilmesi ve yeni teknolojilere uyum sağlaması kritik bir öneme sahip olmaktadır. İşletmeler, bu süreçte dijital yetkinliklerini artırarak rekabet avantajı elde edebilecektir.

YBS'nin geleceğinde organizasyonel yapıların dijital dönüşüme daha fazla uyum sağlaması beklenmektedir. Daha esnek, çevik ve teknolojiye dayalı organizasyon modelleri, işletmelerin dijital dünyaya daha iyi adapte olmasını

sağlayacak ve YBS, bu organizasyonel dönüşümün temel yapı taşlarından biri olacaktır.

Dijital dönüşüm süreçlerinde başarıya ulaşmak için stratejik bir yaklaşım benimsemek hayati öneme sahiptir. İşletmelerin dijital olgunluklarını değerlendirmeleri, dönüşüm için net bir yol haritası oluşturmaları ve kaynaklarını etkili bir şekilde planlamaları, dönüşüm süreçlerinin sürdürülebilirliğini sağlamaktadır.

Dijital dönüşüme başlamadan önce, işletmelerin dijital olgunluk seviyelerini değerlendirmesi gerekmektedir. Bu değerlendirme, işletmenin mevcut dijital yetkinliklerini ve eksikliklerini belirlemeye, dönüşüm sürecinin hangi aşamada olduğunu göstermeye yardımcı olur. Dijital olgunluk değerlendirmesi, stratejik karar alma süreçlerinde işletmelere önemli bir rehberlik sunacaktır.

Dijital dönüşümün başarılı olabilmesi için net bir yol haritası oluşturulmalıdır. Yol haritası, işletmenin kısa, orta ve uzun vadeli hedeflerini belirlemekte ve dijital dönüşüm projelerinin aşamalı olarak gerçekleştirilmesini sağlamaktadır. Planlı bir dönüşüm süreci, işletmelerin kaynaklarını verimli kullanmalarına ve stratejik hedeflerine ulaşmalarına katkı sağlayacaktır. Bu süreçte kaynak planlaması da önemli bir yere sahiptir. Dijital dönüşüm projeleri, finansal, teknolojik ve insan kaynağı açısından etkili bir planlama gerektirir. Kaynakların doğru bir şekilde tahsis edilmesi ve dönüşüm maliyetlerinin öngörülerek gerekli kaynakların ayrılması, dönüşüm projelerinin başarısını artıracaktır.

Son olarak; dijital dönüşüm sürekli gelişen bir süreç olduğu için sürdürülebilir bir dönüşüm yaklaşımı benimsemek gerekmektedir. İşletmeler, yalnızca kısa vadeli kazançları hedeflemek yerine uzun vadede rekabet avantajı sağlayacak sürdürülebilir dijital stratejiler geliştirmelidir. Bu süreç, inovasyonu teşvik etmeyi ve dijital dünyada sürekli yenilikçi çözümler üretmeyi içermektedir.

Kaynakça

Abikoye, B. E., Akinwunmi, T., Adelaja, A. O., Umeorah, S. C., & Ogunsuji, Y. M. (2024). Real-time financial monitoring systems: Enhancing risk management through continuous oversight. *GSC Advanced Research and Reviews*, *20*(1), 465-476. https://doi.org/10.30574/gscarr.2024.20.1.0287

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Ahmad, T., & Van Looy, A. (2020). Business process management and digital innovations: A systematic literature review. *Sustainability*, *12*(17), 6827. https://doi.org/10.3390/su12176827

Al-Saqqa, S., Sawalha, S., & AbdelNabi, H. (2020). Agile software development: Methodologies and trends. *International Journal of Interactive Mobile Technologies*, *14*(11), 246-270. https://doi.org/10.3991/ijim.v14i11.13269

Alsedrah, I. (2023). Digitalization and small & medium enterprise performance: a research to improve business practices. *Business Review of Digital Revolution*, *3*(1), 20-29. https://doi.org/10.62019/BRDR.03.01.03

Chakraborti, T., Isahagian, V., Khalaf, R., Khazaeni, Y., Muthusamy, V., Rizk, Y., & Unuvar, M. (2020). From Robotic Process Automation to Intelligent Process Automation: –Emerging Trends–. In *Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2020 Blockchain and RPA Forum, Seville, Spain, Proceedings 18* (215-228). Springer International Publishing.

Chen, Y., Li, C., & Wang, H. (2022). Big data and predictive analytics for business intelligence: A bibliographic study (2000–2021). *Forecasting*, *4*(4),767-786. https://doi.org/10.3390/forecast4040042

Erbey, A., & Barışçı, N. (2022). A survey on lip-reading with deep learning. *International Journal of Engineering Research and Development*, *14*(2), 844-860. https://doi.org/10.29137/umagd.1038899

Erickson, J., Lyytinen, K., & Siau, K. (2005). Agile modeling, agile software development, and extreme programming: the state of research. *Journal of Database Management (JDM)*, *16*(4), 88-100. https://doi.org/10.4018/jdm.2005100105

Fidan, Ü. (2024). Assessment of Türkiye's Digitalization Performance within the Framework of the UN Sustainable Development Index. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, *8*(1), 1-14. https://doi.org/10.33461/uybisbbd.1373965

Gao, L., Melero, I., & Sese, F. J. (2020). Multichannel integration along the customer journey: a systematic review and research agenda. *The Service*

Industries Journal, *40*(15-16), 1087-1118. https://doi.org/10.1080/02642069.2019.1652600

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. *Journal of management studies*, *58*(5), 1159-1197. https://doi.org/10.1111/joms.12639

Henderson, J. C. & Venkatraman H. (1999).Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 38(2.3), 472-484. https://doi.org/10.1147/SJ.1999.5387096.

Hussein, H., Albadry, O. M., Mathew, V., Al-Romeedy, B. S., Alsetoohy, O., Abou Kamar, M., & Khairy, H. A. (2024). Digital leadership and sustainable competitive advantage: Leveraging green absorptive capability and eco-innovation in tourism and hospitality businesses. *Sustainability*, *16*(13), 5371. https://doi.org/10.3390/su16135371

Jawad, Z. N., & Balázs, V. (2024). Machine learning-driven optimization of enterprise resource planning (ERP) systems: a comprehensive review. *Beni-Suef University Journal of Basic and Applied Sciences*, *13*(1), 4. https://doi.org/10.1186/s43088-023-00460-y

Kitsantas, T., Vazakidis, A., & Stefanou, C. (2020). Integrating Activity Based Costing (ABC) with Enterprise Resource Planning (ERP) for Effective Management: A Literature Review. Technium: Romanian Journal of Applied Sciences and Technology, 2(7), 160–178. https://doi.org/10.47577/technium.v2i7.1882

Mili, H., Tremblay, G., Jaoude, G. B., Lefebvre, É., Elabed, L., & Boussaidi, G. E. (2010). Business process modeling languages: Sorting through the alphabet soup. *ACM Computing Surveys (CSUR)*, *43*(1), 1-56. https://doi.org/10.1145/1824795.1824799

Nambiar, A., & Mundra, D. (2022). An overview of data warehouse and data lake in modern enterprise data management. *Big data and cognitive computing*, *6*(4), 132. https://doi.org/10.3390/bdcc6040132

Nudurupati, S. S., Bititci, U. S., Kumar, V., & Chan, F. T. (2011). State of the art literature review on performance measurement. *Computers & Industrial Engineering*, *60*(2), 279-290. https://doi.org/10.1016/j.cie.2010.11.010

Oudada, G., & Daoui, D. (2023). The Perspectives For Risk-Management In The Age Of Digitalization: A Systematic Literature Review. *Journal of Namibian Studies: History Politics Culture*, *36*, 191-204. https://doi.org/10.59670/jns.v36i.4786

Pagani, M. (2013). Digital business strategy and value creation: Framing the dynamic cycle of control points. *Mis Quarterly, 37*(2), 617-632.

Puspitasari, I., & Jie, F. (2020). Making the information technology-business alignment works: a framework of IT-based competitive strategy. *International Journal of Business Information Systems*, *34*(1), 59-82. https://doi.org/10.1504/IJBIS.2020.106796

Raghupathi, W., & Raghupathi, V. (2021). Contemporary business analytics: An overview. *Data*, *6*(8), 86. https://doi.org/10.3390/data6080086

Roy, J., Sharaput, M. & Toze, S. (2019). Building digital capacity report on the training needs analysis. Dalhouseie University. https://pro.europeana.eu/page/building-digital-capacity#step-2-defining-digital-transformation. (E. T: 19.09.24).

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Sahoo, S. K., Goswami, S. S., Sarkar, S., & Mitra, S. (2023). A review of digital transformation and industry 4.0 in supply chain management for small and medium-sized enterprises. *Spectrum of Engineering and Management Sciences*, *1*(1), 58-72. https://doi.org/10.31181/sems1120237j

Schulz, G. (2017). *Software-Defined Data Infrastructure Essentials: Cloud, Converged, and Virtual Fundamental Server Storage I/O Tradecraft*. Auerbach Publications. https://doi.org/10.1201/9781315369426

Sledgianowski, D., & Luftman, J. (2005). IT-business strategic alignment maturity: A case study. *Journal of Cases on Information Technology*, *7*(2), 102-120. https://doi.org/10.4018/jcit.2005040107

Teubner, R. A., & Stockhinger, J. (2020). Literature review: Understanding information systems strategy in the digital age. *The Journal of Strategic Information Systems*, *29*(4), 101642. https://doi.org/10.1016/j.jsis.2020.101642

Tuna, M. F., & Görmez, Y. (2024). Evrişimsel sinir ağları tabanlı derin öğrenme yöntemiyle müşteri şikayetlerinin sınıflandırılması. *Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *8*(1), 31-46. https://doi.org/10.33399/biibfad.1362160

Wallace, R. E. (1988). What If You Don't Plan? *Journal of Information Systems Management, 5*(4), 78–80. https://doi.org/10.1080/07399018808962947

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press.

Wijaya, M. I., & Utomo, D. (2021). Enterprise Resource Planning Modification: A Literature Review. *ComTech: Computer, Mathematics and Engineering Applications*, *12*(1), 33-43. https://doi.org/10.21512/comtech.v12i1.6610

Williams, J. A., Torres, H. G., & Carte, T. (2022). A review of IS strategy literature: current trends and future opportunities. *Journal of Computer Information Systems*, *62*(1), 1-11. https://doi.org/10.1080/08874417.2019.1681327

Wissuchek, C., & Zschech, P. (2024). Prescriptive analytics systems revised: a systematic literature review from an information systems perspective. *Information Systems and e-Business Management*, 1-75. https://doi.org/10.1007/s10257-024-00688-w

Wolniak, R., & Grebski, W. (2023). The concept of diagnostic analytics. *Silesian University of Technology Scientific Papers. Organization and Management Series*, *175*, 650-669. http://dx.doi.org/10.29119/1641-3466.2023.175.41

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance. *MIS quarterly*, *39*(2), 497-518.

Yılmaz Börekçi, D., Büyüksaatçı Kiriş, S., & Batmaca, S. (2020). Analysis of enterprise resource planning (ERP) system workarounds with a resilience perspective. *Continuity & Resilience Review*, *2*(2), 131-148. https://doi.org/10.1108/CRR-06-2020-0022

Yılmaz, E. O. (2023). A scale development study for socio-technical pedagogical usability of mobile applications. *Malaysian Online Journal of Educational Technology*, *11*(1), 59-76. https://doi.org/10.52380/mojet.2023.11.1.469

Zaoui, F., & Souissi, N. (2020). Roadmap for digital transformation: A literature review. *Procedia Computer Science*, *175*, 621-628. https://doi.org/10.1016/j.procs.2020.07.090

Zhang, X. J. (2013). The Evolution of management Information Systems: a literature review. *Journal of Integrated Design and Process Science*, *17*(2), 59-88. https://doi.org/10.3233/jid-2013-0009

Yönetim Bilişim Sistemlerinde Güncel Konular

Editör:
Dr. Öğr. Üyesi Mehmet Fatih KARACA

ÖZGÜR YAYINLARI

ISBN 978-975-447-941-6