

Finans Sektöründe Dijital Dönüşüm Uygulamaları ve Dolandırıcılık Tespiti **Digital Transformation Practices and Fraud Detection in the Finance Sector**

Habibe AKTAY¹

Y. Pınar SOYKUT SARICA²

Araştırma Makalesi/Research Article

Başvuru/Received: 30.03.2024; Revizyon/Revised: 19.10.2024; Kabul/Accepted: 22.10.2024

ÖZ

Teknolojik inovasyonlarda yaşanan gelişmeler ışığında rekabet şartları küresel düzeyde değişmiştir. Bu değişim ve dönüşümlerden finans sektörü de nasibini almıştır. Artan rekabet ile şirketlerin sürdürülebilir rekabet avantajı elde etmeleri, müşteri memnuniyeti sağlamaları ve pazar paylarını artırmalarının yolu tüm iş süreçlerini dijitalleştirmelerinden geçmektedir. Dolayısıyla örgütlerin manuel olarak yürüttükleri tüm iş sistemlerini bilişim sistem ve teknolojilerine entegre etmeleri gerekmektedir. Bu sayede örgütsel hedeflere ulaşma noktasında daha etkili ve verimli bir yol tercih edilmiş olacaktır. Tüm bunların sistem güvenliğinin sağlanarak yapılması gerekmektedir. Bu çalışmanın amacı mevcut literatür incelenerek finans sektöründe dijitalleşme olgusuna değinme ve dolandırıcılık tespitinde kullanılacak strateji ve algoritmalar hakkında uygulayıcılara ve teorisyenlere faydalı olacak kurumsal altyapı ve içgörü sağlamaktır. Araştırma kapsamında finansal hizmetlerde dijital dönüşümü sağlayan kavramların temel unsurları ve bileşenleri verilmiş olup, dolandırıcılık tespitinde kullanılan algoritmalar incelenmiştir. Bu çalışma sonucunda dijitalleşmenin finansal ve örgütsel süreçleri büyük oranda iyileştirdiği fakat dijital sistemlerin siber saldırıları da olanaklı kıldığı sonucuna ulaşılmıştır. Dolandırıcılık tespitinde veri madenciliği ve makine öğrenmesi algoritmalarının faydalı olduğu sonucuna ulaşılmıştır. Makine öğrenmesi algoritmaları arasında Sinir Ağları (Neural Networks), Rastgele Orman (Random Forest), Destek Vektör Makineleri [Support Vector Machines (SVM)] ve Gradyan Güçlendirme Ağaçları (Gradient Boosting Trees) algoritmalarının her biri doğruluk ve performans kriterleri açısından değerlendirildiklerinde yüksek performans gösterdikleri sonucuna ulaşılmıştır. Dolandırıcılık tespitinde algoritmalar ve farkındalık stratejilerinin uygulanmasının kurumlar lehine olduğu sonucu çıkarılmıştır.

Anahtar Kelimeler: Dijital Dönüşüm, Finans Sektörü, Siber Tehdit, Dolandırıcılık Tespiti

ABSTRACT

In the light of developments in technological innovations, competition conditions have changed at the global level. The finance sector has also been affected by these changes and transformations. With increasing competition, the way for companies to gain sustainable competitive advantage, ensure customer satisfaction and increase their market share is to digitalize all business processes. Therefore, organizations need to integrate all their manual business systems into information systems and technologies. In this way, a more effective and efficient way will be preferred to achieve organizational goals. All this should be done by ensuring system security. The purpose of this study is to provide institutional infrastructure and insights that will be useful for practitioners and theoreticians about the strategies and algorithms to be used in the digitalization phenomenon in the financial sector and fraud

¹ Işık Üniversitesi, Enformasyon Teknolojileri Bölümü, habibe.aktay@isikun.edu.tr, ORCID: 0000-0002-2917-6187

² Işık Üniversitesi, İşletme Bölümü, pınar.soykut@isikun.edu.tr, ORCID: 0000-0001-8349-607X

detection by examining the existing literature. Within the scope of the research, the basic elements and components of the concepts that enable digital transformation in financial services are given, and the algorithms used in fraud detection are examined. This study concludes that digitalization has greatly improved financial and organizational processes, but digital systems also enable cyber-attacks. Among the machine learning algorithms in fraud detection, Neural Networks, Random Forest, Support Vector Machines (SVM) and Gradient Boosting Trees algorithms have shown high performance when evaluated in terms of accuracy and performance criteria. The application of awareness strategies as well as algorithms in fraud detection is in favor of institutions.

Keywords: Digital Transformation, Financial Sector, Cyber Threat, Fraud Detection

1. Giriş

1900'lerin ikinci yarısında başlayan teknolojilerdeki yeni gelişmeler ile üretim sistemlerinde nesnelere interneti, büyük veri, yapay zekâ ve robotik kullanımlarının hayatımıza girmesi ile üretimde otomasyona gidilerek dijitalleşme süreci başlamıştır (Hepaktan ve Şimşek, 2022). Dijitalleşme çeşitli bilgilerin dijitalleştirilmesiyle güçlendirilen, manuel ve kâğıt tabanlı süreçlerin bir otomasyonu anlamını taşımaktadır. Bir organizasyonun dijitalleştirilmesi, işlerin daha hızlı, daha iyi ve daha ucuza yapılması noktasında büyük bir avantaj sağlamaktadır (Balasoto, 2024).

Dijitalleşme olgusu, teknolojik gelişmelerin çok hızlı bir şekilde gerçekleştiği son yıllarda çok popüler bir konu haline gelmiştir. Terim ortaya çıktığından ve tanımların çoğu dijitalleşmenin temel anlamıyla uyumlu olduğundan çeşitli tanımlarla olgu açıklanmaya çalışılmıştır. Dijitalleşme terimi ilk kez 1971'de *North American Review* tarafından "toplumun dijitalleşmesi" olarak yayınlanmıştır (Şükranlı, 2020: 5).

Dijitalleşme, herkesin erişebileceği geniş bir teknoloji yelpazesi sunmaktadır. Böylece kültürel, davranışsal, demografik ve yaşam döngüsü yönleri de dâhil olmak üzere en önemli değişikliklere katılmaktadır. Dijitalleşmenin bir sonucu olarak, e-ticaret, e-bankacılık, e-kitaplar, e-haberler, e-öğrenme terimleri ortaya çıkmıştır. (Mergel vd., 2019: 1).

Teknolojideki yeni gelişmeler ve teknolojik inovasyonlar finansal hizmetlerin dijitalleşmesine yardımcı olurken, tüketicilere, düzenleyicilere ve hizmet sağlayıcılara çeşitli fırsatlar sağlamakla birlikte zorlukları da beraberinde getirmektedir. Rekabette ve müşteri deneyiminde geri kalmak istemeyen finansal şirketlerin, süreçlerinde ve iş modellerinde dijital dönüşüm projeleri başlattıkları görülmektedir. Müşterilere daha iyi hizmet verebilmek için geliştirilen dijital dönüşüm uygulamalarının hayatımıza girmesi ile gizliliğin ve güvenliğin eskiye kıyasla daha önemli hale geldiği görülmektedir. Finansal hizmetlerdeki bu teknolojik yeniliklerin nasıl

çözümler sunduğunun ve hangi ekonomik ortamda kullanılması gerektiğinin tartışılması önem arz etmektedir.

Dijital dönüşümü başarılı bir şekilde yönetme ve bir işletmeyi veya sektörü tamamen dijital hale getirme konusunda daha fazla açıklamaya ihtiyaç bulunmaktadır. Dijital dönüşümün avantajları örgütlerin dikkatini çekmekte, bu nedenle örgütler dijital iş stratejileri oluşturarak rekabet avantajlarını artırmayı istemektedirler (Bharadwaj vd., 2013).

Günümüzde birçok kuruluş ve sektör dijitalleşme süreci başlatmış durumdadır. Finans sektörü de dijitalleşmeye geçen sektörlerden biridir. Dijitalleşme çeşitli avantajlar sağlasa da birçok riski beraberinde getirmiştir. Finans sektöründe alışılmış geleneksel sistemlerin yerine kullanılan yeni teknolojiler artan avantajlar sunmakla birlikte finansal suçlar için bazı riskler ve ön koşulları oluşturmaktadır. Artan siber saldırılarla ve dolandırıcılık girişimleriyle etkili bir biçimde mücadele edilebilmesi için süreçlerin ve teknolojilerin yakından takip edilmesi gerekliliği doğmuştur. Bu çalışma ile finans sektöründe dijital dönüşüm için gereken teknolojiler ve uygulama alanları incelenmiş olup, dijital dönüşüm ve etkileri analiz edilmiştir. Akabinde dijital dönüşüm teknolojileri ile ortaya çıkan güvenlik tehditlerine yakından bakılarak dolandırıcılık girişimlerine engel olmaya yönelik politikalara yer verilmiştir.

2. Finansal Hizmetlerde Dijital Dönüşümü Sağlayan Ana Teknolojiler

Başlarda yavaş ilerleyen teknolojik gelişmelerin çağımızda ivme kazandığı yani üssel bir seyir izlediği görülmektedir. Teknoloji arenasında yaşanan gelişmeler, finans sektöründeki dijital dönüşümler için önemli bir itici güç olmuştur. 1990'lı yılların sonundan bu yana, finansal kurumların çoğu internet bankacılığı hizmetlerini sunarak ürün cüzdanlarının bir bölümüne erişebilmekteler. Son yıllarda, bu platformların modernizasyonu yanında finansal kurumlar, mobil cihazlar aracılığıyla yeni erişim ve dağıtım kanalları geliştirmeye odaklanmış durumdadır. Böylece, sosyal ağlar tarafından sunulan kullanıcı deneyiminden ilham alınmasıyla akıllı telefonlar veya tabletler için yeni uygulamalar ortaya çıkmış olup, tüm işlevler sadece bir tık ile yapılabilir hale getirilerek optimize edilmiştir (Başer ve Akıncı, 2020: 872-873). Bankalar, benzer şekilde dijital cüzdanlar, NFC teknolojisi ödeme çözümleri veya bireyler arasında para transfer uygulamaları (P2P) gibi perakende ödemeler alanında da benzer şekilde yeni dijital ürünler geliştirmektedirler.

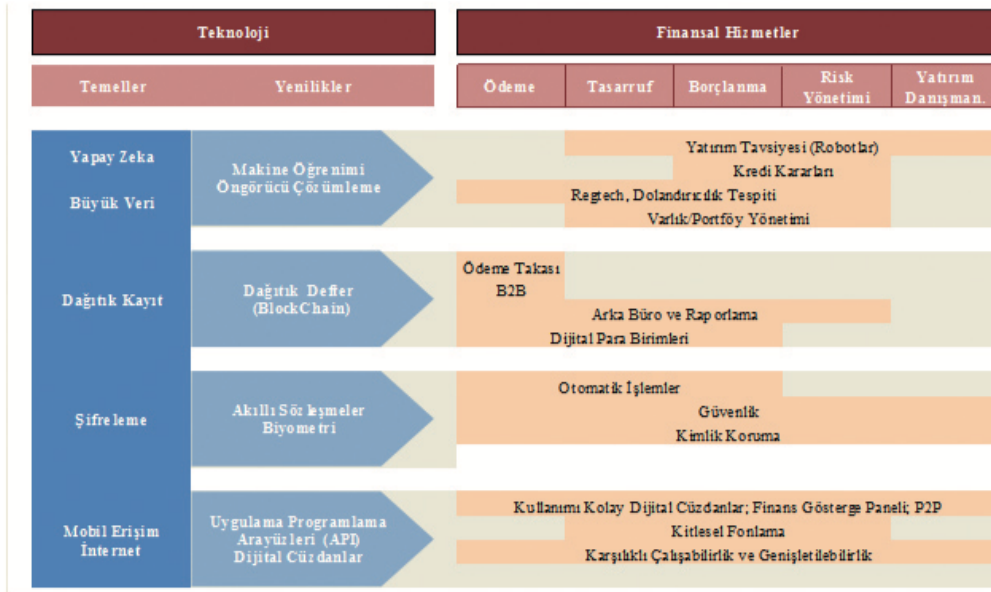
Rekabetin dijitalleşmesinin ilk aşamasında, örgütler normalde dijital gelişmeleri tek başına proje olarak görmekte ve çeşitli dağıtım kanallarını kısmen veya tamamen ayrı bir şekilde ele almaktadırlar. Her durumda yeni dijital kanalların ve ürünlerin yaratılması, yeni karmaşık sistemlerin hâlihazırda var olan altyapılarla bütünleştirilmesi ve tüm bunların teknolojik altyapıyla koordineli bir şekilde entegrasyonun yapılması gerekmektedir (Finaratz, 2023). Bankacılık dijital dönüşüm sürecinin ikinci aşaması, teknoloji platformunun yeniden biçimlendirilmesini gerçekleştirmek, yeni teknolojilerin uyumlu olmasını sağlayan daha modüler ve esnek bir altyapıya dönüştürmek ve daha hızlı yeni ürün geliştirerek sürdürülebilir rekabeti sağlamaktır.

Bankacılık teknolojisi altyapısının en belirgin özelliği, 1970'li yıllardan başlayarak 1990'lı yıllarda internetin ortaya çıkışı ile ortaya çıkan dağıtılmış sistemler ile yaşamak zorunda kaldıkları, yüksek güvenli sistemler ile donatılmış geniş, merkezi işlem platformlarının dâhil edilmesi eğiliminde olması olarak açıklanabilir. Bu nedenle, çeşitli ürün ve hizmetlerin tek başına ve verimsiz örtüşen yerlerde faaliyet gösterdiği, yerel, ulusal ve uluslar üstü otoritelerin dayattığı yasal gereksinimlere uyacak şekilde uyarlanması gereken karmaşık sistemler ortaya çıkmıştır (Fernando, 2018).

Öte yandan, yeni sayısal projeler için çeşitli kanallardan çok miktarda bilginin hızlı bir şekilde üretilmesi ve işlenmesi durumu söz konusudur. Bu noktada talepleri karşılayan çok kanallı, ultra uygun ve kullanıcı dostu deneyimler sunma yeteneğine sahip olmak kritik önem taşımaktadır. Bununla birlikte, hâlihazırda var olan altyapı, yeni teknolojilerin hızlı bütünleşmesi için veya işin hızlı değişen gereksinimleri ile hareket edebilmek için yeterince modüler değildir. Dolayısıyla, tüm teknoloji platformunun tamamen yenilenmesi çok mümkün değildir. Bu sebeple sıfırdan başlamak oldukça etkili olmaktadır. Bu aşamada, kurumlar dâhili kaynakların en iyi şekilde kullanılmasına olanak tanıyan bulut bilgi işlem teknolojisini benimsemeyi düşünmektedir. Buradaki amaç teknoloji havuzunun verimliliğini en üst düzeye çıkarmak ve tüm üretim sürecinde daha fazla esneklik sağlamaktır. Buluttaki dış kaynak kullanımı hizmetleri, sayısız sunucularda yer alan verilerin merkezileştirilmemesi ve uyumluluk sorunları nedeniyle finansal kurumlar için kullanımını pratik yapmasa da daha fazla fayda sağlamaktadır (Tayaksi vd., 2016: 71).

Şekil 1

Finansal hizmetlerde dijital dönüşümü sağlayan ana teknolojiler



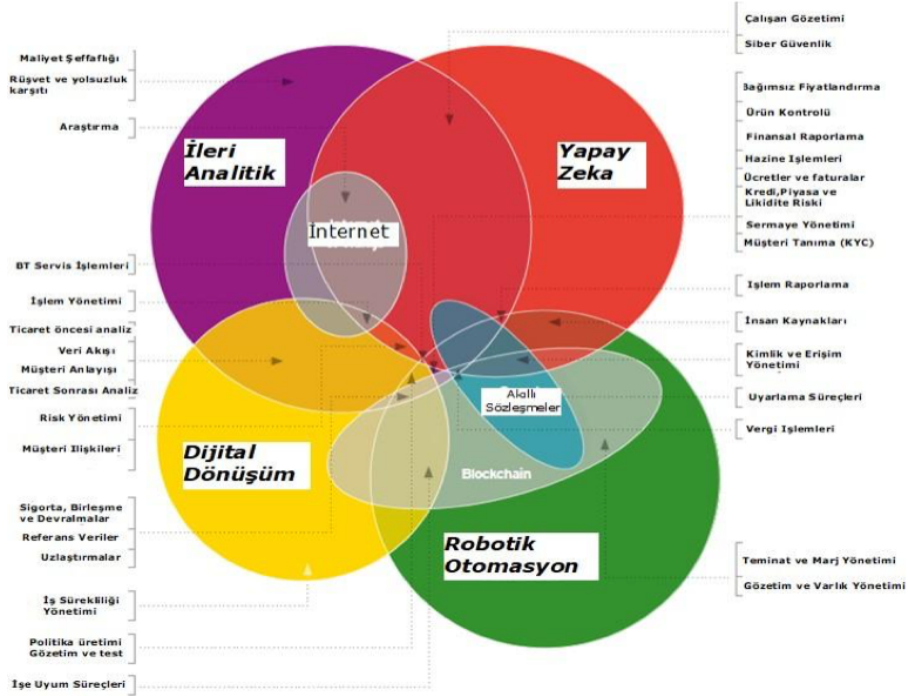
Kaynak: Deloitte, Connecting Global Fintech, 2017: 10

Finansal hizmetlerde kullanılan teknolojiler Şekil 1’de gösterilmiştir. Bu teknolojileri yapay zekâ, dağıtık kayıt, şifreleme ve mobil erişim internet teknolojileri olarak kategorize etmek mümkündür. Bu teknolojilerdeki yenilikler yapay zekâ ve büyük veri kullanılarak yatırım tavsiyesi, kredi kararları ve varlık portföy gibi finansal hizmetleri olanaklı kılmaktadır. Dağıtık kayıt teknolojisi dağıtık defter yeniliği ile ödeme takası, B2B, arka büro ve raporlama ve dijital para birimi hizmetlerini sağlamaktadır. Şifreleme teknolojisi otomatik işlemler, güvenlik ve kimlik koruma gibi finansal hizmetlerde etkili güvenlik hizmetini finansal hizmetlerle birlikte sağlamaktadır. Mobil erişim internet teknolojisi ise arayüzler ve dijital cüzdanlar vasıtasıyla kullanımı kolay dijital cüzdanlar, finans gösterge panelleri, kitlesel fonlama gibi finansal hizmetlerin kullanımını kolaylaştırmakta ve bunlara aracılık etmektedir.

Finansal hizmetlerde dijital dönüşümü sağlayan ana teknolojilere yakından bakıldığında yapay zekâ, büyük veri, dağıtık kayıt, şifreleme, mobil erişim ve internet gibi teknolojilerin finansal hizmetlerde daha çok öne çıkan dijital dönüşüm alanları olduğu görülmektedir. Şekil 2’de görüleceği üzere dijital dönüşüm yaratan teknolojilerle eşlenen yenilik kullanım durumlarının bazıları gösterilmiştir.

Şekil 2

Dijital dönüşüm yaratan teknolojilerle eşleşen yenilik kullanım durumları



Kaynak: EY-Capital Markets: Innovation and the FinTech Landscape, 2016: 31.

3. Dijital Dönüşüm ve Etkileri

Ekonomik büyüme ve yeni iş olanaklarının yaratılması işgücü açısından umut vaat ederken, giderek yaygınlaşan dijitalleşme ile düşük vasıflı işgücüne olan talebin azalacağı kaygısı yaratmaktadır. Bu nedenle, işgücünün ihtiyaç duyduğu yetkinliklere sahip olabilmesi için gerekli eğitimlerle desteklenmesi gerekmektedir. Kişilerin, gelecek yeni teknolojilere hazır hale getirilebilmesi için beceri ve yaratıcılıklarını ön plana çıkaran eğitim ve çalışma hayatı planlamasının yapılması gerekmektedir (Ortar ve Yeşiltaş 2021).

Dijitalleşmenin getirdiği avantaj ve dezavantajlar sırasıyla şunlardır (Bharadwaj vd., 2013):

Avantajları:

- Dijital çağ, verilerin merkezileştirilmesi ve erişilebilirliği özellikleri sayesinde her türlü bilgiyi parmak uçlarımıza getirmektedir.

- Dijitalleşme sayesinde insanlar birbirlerine anında ve birçok farklı formatta mesaj gönderebilmektedirler. Dolayısıyla dijitalleşme olgusu, iletişim yeteneğimizi de çağın dinamiklerine uygun olarak değiştirmiş ve dönüştürmüştür.
- Dijitalleşme sayesinde yeni fikirler geniş alanlara kolaylıkla ve hızlı bir şekilde iletilebilmekte ve kitleler tarafından benimsenebilmektedir.
- Dijitalleşmeyle yaygınlaşan internet teknolojileri uzaktan çalışmaya izin vermekte; bu sayede yeni fırsatlara ulaşım kolaylaşmaktadır. Mekândan bağımsız çalışma rutinleri ve şekilleriyle maliyetler düşmekte ve verimlilik artmaktadır.
- Son olarak, dijitalleşmeyle rekabet şartları değişmiş ve tüketicilerin artık seçim yapabilecekleri çok daha fazla seçenek ortaya çıkmıştır. Bu da tüketicilerin bir markaya bağlı kalma zorunluluğunu ortadan kaldırdığından pozitif bir gelişme olarak kabul edilebilir.

Dezavantajları:

- Finansal varlıklar ve kişisel bilgiler üzerindeki kontrolün merkezileştirilmesi, tüm yumurtaların tek bir sepete konduğu anlamına gelmektedir. Teknoloji insan hatasını ortadan kaldırırken, başarısızlıktan muaf değildir, bu nedenle %100 güvenilir olmayan bir şeye güvenmek, varlıkların kontrolünü kaybetme riskini doğurmaktadır. Kontrolü devretmek aynı zamanda yıkıcı potansiyeli bilinmeyen bilgisayar korsanları gibi dijital suçlara da davetiye çıkarmaktadır.
- İletişim kolaylığı, gerçek hayattaki sosyal beceriler üzerinde olumsuz bir etkiye sahip olabilmekte ve topluluğun gücünü zayıflatabilmektedir.
- Bilgiye kolay erişim, örneğin sağlık durumları için bireylerin kendi kendilerine teşhis koymaları gibi durumlar, dijitalleşmenin kötüye kullanılma olasılığını artırmakta ve manipülatif amaçlarla kullanılacak yanlış bilgilerin yayılmasına izin vermektedir.

Dijitalleşme neredeyse her endüstriyi etkilemekte ve iş yapış biçimlerini değiştirmektedir. Ancak dijitalleşme çağıyla en çok dönüşen sektörlerden ikisi telekomünikasyon ve bankacılık / finansal hizmetler sektörüdür. Dijitalleşme sayesinde örgütler bazı avantajlara sahip olmaktadır. Bunlar aşağıdaki gibi listelenebilmektedir (Digital Europe, 2020: 29).

Dijital Çağ için Dönüşüm Gündemi Digital Europe'un 2020 vizyonuna göre:

- Üretkenliği artırmak,
- Rekabet gücünü artırmak,
- Müşterilere daha iyi fiyatlarla ve daha yüksek kalite düzeyinde daha fazla kişisel ürün sunmak,
- Çalışanların üretkenliğini artırmak ve hareketsizlik sürelerini en aza indirmek,
- Ürün geliştirme maliyetlerini düşürmek ve pazara yeni bir ürün sunmak için gereken süreyi kısaltmak,
- Müşteriler arasında daha fazla güven kazanmak ve böylece müşteri tabanını büyütmek.

4. Dijital Dönüşümü Sağlayan Teknolojiler

4.1. Büyük Veri ve Büyük Veri Analitiği

Büyük veri, yüksek hacim, hız, çeşitlilik ve doğruluk ile karakterize edilen ve değer çıkarımı için özel analitik yöntemler gerektiren geniş bilgi varlıklarını ifade eder. Büyük veri internetin yaygınlaşmasıyla kullanımı yaygınlaşan ve önemi artan bir kavramdır. Bu kavram internet üzerinden özellikle mobil uygulamaların artması ile sosyal platformlardan toplanan fotoğraf, bloglar, mesajlar ve videoların paylaşılması ile artan veriyi ifade etmek için kullanılmaktadır. Büyük Veri kavramı teknolojinin hızla ilerlemesi ve internete bağlı dijital cihazların çoğalması sebebiyle kümülatif olarak biriken geniş ve karmaşık veri setlerini ifade etmek için kullanılmaktadır (Harding ve Hersh, 2018; Oancea, 2024).

Finansal uygulamalardaki işlemlerin güvenlik nedeni ile belli bir süre saklanması ve müşteri deneyimlerini incelemek için kayıt altına alınması da verilerdeki artışların nedenleri olarak gösterilebilmektedir. Bu verilerin çok büyük yer kaplaması nedeni ile geleneksel saklama yöntemleri bu durumda yeterli olmamaktadır. Bu nedenle ilgili veriler ilişkisel veri tabanlarında tutulmamaktadır (MIS, 2014: 173-174). Daha hızlı ve doğru kararlar vermek isteyen birçok örgütün, bireyin ve ekonomik birimlerin veriye ulaşma ihtiyacının arttığı görülmektedir. Büyük Veri, rekabette üstünlüğünü kaybetmek istemeyen finans şirketleri için büyük imkânlar sunması nedeni ile çok büyük bir önem arz etmektedir. Büyük veri bileşenlerini üç ana grupta toplamak mümkündür. Bunlar süreç, yönetim ve veri bileşenleridir (Vassakis vd., 2018; Wang vd., 2016).

- Süreç bileşenleri: Veri toplama ve depolama, veri madenciliği ve temizleme, veri toplama ve entegrasyon, mantıksal çözümlenme ve modelleme, veri yorumlama olarak listelenmektedir.
- Yönetim Bileşenleri: Gizlilik, güvenlik, veri yönetimi, veri ve bilgi paylaşımı, maliyet/operasyonel giderler, veri sahipliği olarak listelenmektedir.
- Veri Bileşenleri: Veri büyüklüğü (*volume*), verinin hızı (*velocity*), veri çeşitliliği (*variety*), veri doğrulama (*veracity*), veri görselleştirme (*visualization*), veri değeri (*value*) olarak listelenmektedir.

Finans sektöründeki rekabetin artması ile şirketlerin müşterilerin davranışlarına ve ihtiyaçlarına göre akıllı ürünler sunma ihtiyacı doğmuştur. Dolayısıyla finansal kurumlarda bu büyük verilerin analiz edilmesi ve bunlardan rekabette öne çıkaracak stratejiler geliştirilmesi ihtiyacı ortaya çıkmıştır. Klasik yöntemler ile bu büyük verilerin analiz edilememesi dolayısıyla yeni metotların ve yaklaşımların kullanılması gündeme gelmiştir.

4.2. Yapay Zekâ ve Makine Öğrenmesi

Yapay zekâ “Artificial Intelligence: AI” teriminin bir tercümesidir. Yapay zekâyla, teknolojidaki gelişmeler ile makinelerin akıllı hale getirilmesi hedeflenmiştir. Bununla birlikte, insan gibi öğrenebilen, çevresini algılayabilen ve kararlarını önceden belirlenmiş hedeflere göre verebilen makineler geliştirmek mümkün hale gelmiştir (Hassani vd., 2020: 148).

Pazar payını muhafaza etmek ve genişletmek isteyen şirketlerin yapay zekânın gelişimine destek verdikleri görülmektedir. Yapay zekâ ile en iyi müşteri deneyiminin sunulabileceği, gerekli yetkinliklerin daha hızlı kazanılacağı, geleceğe daha hazır olunacağı ve rekabet üstünlüğü ele geçirileceği düşünülmektedir. Büyük verilerin kullanılmasıyla ve kullanılan yeni algoritmik yaklaşımlarla dünyanın önemli problemlerini çözmeye çaba gösteren ekiplerin sayısının giderek arttığı görülmektedir. Dijital dönüşüm süreçlerinde yapay zekâ ve makine öğreniminin önemi her geçen gün artmaktadır. Nesnelerin interneti, bulut bilişimi ve büyük veri alanındaki teknolojik gelişmelerden yararlanılarak süreçlerin ve iş modellerinin akıllı hale getirildiği görülmektedir (World Economic Forum, 2024).

Yukarıdaki açıklamalardan anlaşılacağı üzere yapay zekâ, kalıcı, paylaşılabilir, daha erişilebilir, tutarlı ve belgeli bir zekâ türüne işaret etmektedir. Doğal zekâ ise yaratıcıdır, tecrübeyi kullanmaktadır. Yapay zekâ, bilgisayara iletilen bilgilerle sınırlı iken; bu nedenle

yaratıcılığı, deneyimlerden yararlanma ve çözüm üretme yeteneği insanlara kıyasla şu anda daha kısıtlı olsa da aşağıda tartışılan birçok alanda kullanılmakta ve kullanımı hızla artmaktadır (Adalı, 2017: 9-11).

Makine öğrenmesi, belirli bir amaç için büyük verilerin işlenmesi ve başarılı bir şekilde anlamlandırılması ile bilgisayarların bundan çıkarım yapması ve konuyu öğrenmesi olarak ifade edilmektedir (Sinap, 2024). Makine öğrenimi, bilgisayarlara açık bir şekilde programlanmadan öğrenme yeteneği kazandıran bir yapay zekâ türüdür. Makine öğrenmesi, değişen şartlarda bile verilerin adlandırılabilmesi amacıyla bilgisayar programlarının geliştirilmesine odaklanmaktadır. Bugün, makine öğrenmesinin geleceği tahmin etmek için kullanılabileceği öngörülmektedir. Otomatik para çekme makinesinde nakdin en iyi şekilde kullanımını sağlamak buna verilecek güzel bir örnektir. Ayrıca mevcut hava durumu verileri ve geçmiş verilerin incelenmesi ile hava tahmini uygulamalarında bu veriler işlenebilmekte ve gelecekteki hava koşulları hakkında bir gelecek tahmin modeli yapılabilmektedir (Valenta vd., 2023: 211).

4.3. İnsan Gibi Düşünen ve Hareket Eden Sistemler

İnsan gibi düşünen ve hareket eden sistemlerle insan gibi öğrenen ve zekâsını geliştirebilen bilgisayarların yaratılması amaçlanmaktadır. Bu sayede birçok sektörde insana ihtiyaç duyulmadan hizmet verilmesinin mümkün olacağı düşünülmektedir. Örneğin kendi kendine 7 gün 24 saat durmaksızın üretim yapan fabrikalar ortaya çıkarma, şoförsüz araçlarla insanların zamandan tasarruf etmelerini sağlama, ameliyatlarda doktorların yerine görev yapacak robotlar üretme, finans sektöründe müşterilere çağrı merkezinde insansız hizmet verme gibi çalışmalar, bunlardan bazıları olarak düşünülmektedir (Öz, 2022).

4.4. Uzman Sistemler

İnsan gibi düşünen ve davranan sistemlerin geliştirilmesi ile bir uzmanın vereceği kararları verebilecek sistemlerin üretilmesinin mümkün hale geldiği görülmektedir. Yakından bakıldığında uzman sistemlerin finans, trafik, sigortacılık ve tıpta kullanıldığı ve çözümler geliştirildiği görülmektedir. Amaç daha sağlıklı ve doğru kararların verilmesini sağlamak olarak ifade edilebilmektedir (Çakar vd., 1997: 34).

4.5. Doğal Dil İşleme

İnsanların konuştuklarını anlayıp, sorularına doğru cevaplar verebilen sistemlerin geliştirilmesi ile otomatik yanıt veren sistemlerinin birçok sektörde kullanılmaya başlandığı görülmektedir. Bu sistem ile diller arası çevirinin yapılabildiği ve önemli bir noktaya geldiği bilinmektedir. Bu yöntemin bankacılık ve turizm hizmetlerinde kullanılmaya başlandığı görülmektedir (Mah, 2022: 74).

4.6. Robotlar

Robot teknolojisindeki gelişmelerin son yıllarda önemli bir noktaya geldiği görülmektedir. Özellikle güvenlik (askeri, polis, vb.) ve üretim sektörlerinde çok önemli görevler alacağı düşünülen robotlar işlevselliği açısından üç kısma ayrılmaktadır (Gürgüze ve Türkoğlu, 2019: 54-55):

Programlı robotlar programlar yardımı ile hareketlerini öğrenen robotlardır. Robotların üzerinden kullanılmak için özel dillerin oluşturulduğu görülmektedir. Bu programlar sayesinde hareket komutlarını yerine getirmektedirler. Karşılaşılabilecek durumlara yönelik verilecek tepkiler bu programlar içinde belirlenir. Daha çok üretim sektörlerinde bu tip robotların kullanıldığı görülmektedir. Montaj işlemleri buna örnek verilebilir (Gürgüze ve Türkoğlu, 2019: 54-55).

Öğretebilen robotlar ise programlar ile yapılması mümkün olmayan bir profesyonel tarafından eğitilerek üretilen robotlardır. Robot, öğrenim aşamasında tüm hareketleri hafızasına alarak kendisi yinelemektedir. Bu tip robotlara örnek olarak araç üretimi ve araç boyama verilebilir.

Akıllı robotlar ise programlama ve yapay zekâ kullanımı ile çevresi ile etkileşime girerek davranışlarını ve hareketlerini belirleyebilmektedirler. Bu yönüyle akıllı robotlar insana benzetilirler. İnsanlar gibi yürüyebilen ve konuşabilen bu robotların sürücüsüz araçlarda, insansız uçaklarda ve askeri amaçlarla kullanıldıkları görülmektedir (Di Palo, 2017: 3).

4.7. Görüntü İşleme

Kameradan gelen görüntülerin tanınması ve işlenmesi için geliştirilen makineler görüntü işlemeye imkân vermiştir. Hangi amaçla kullanılacağına bakılarak özelleştirmeler yapılmaktadır. Yapay zekâ ile kullanımı halinde birçok alanda kullanımının önü açılmaktadır. Yakından baktığımızda otoyol ve köprü kullanımlarında ücretlerin tahsil edilmesinde, otoparklarda plakanın tanınması ve giriş çıkış saatlerine göre ücretlerin otomatik tahsil

edilmesinde, trafikte yapılan yanlış kullanımların tespitinde ve herhangi bir suça karışan kişilerin tespitinde kullanıldıkları görülmektedir (Valenta vd., 2023: 210).

4.8. Blok Zincir ve Şifreleme

Küreselleşmenin hızlanması ve dijitalleşmenin her alanda yaygınlaşması ile değerli olarak görülen bilginin paylaşımı, aktarılması, depolanması ve etkin bir biçimde kullanımında güvenli araçlara olan ihtiyaç da gün geçtikçe artmıştır. Bu doğrultuda hukuki olarak güvenceye alınacak bir düzenlemeyle kullanılan blok zincir teknolojisi hem ulusal hem de uluslararası boyutta bankacılık ve finans sektörlerinde faydalar sağlayacaktır. Fakat şu an için gerek yapısal gerek teknik özelliklerinden dolayı özellikle kamu kesiminde blok zincir teknolojisine geçişte piyasaların hızı ve kurumların aynı paralelde gitmeleri beklenmemekle birlikte gelişme göstermeye de devam etmektedir (Syamsuddin vd., 2024: 6-7).

Özellikle son yıllarda hızlı bir şekilde yaygınlaştığı ve kabul gördüğü düşünülen blok zincir teknolojisi esasında bir nevi veri tabanıdır. Bu veri tabanı tek bir merkezde bulunmamakla birlikte dağınık bir şekilde kurgulanışı özelliğinden dolayı üzerinde kolay değişiklik yapılabilmesine karşın korumalı ve yenilikçi bir yapıya sahiptir. Merkezi bir kuruma bağlı olmaksızın tüm kullanıcılarına işlemlerini kontrol edebilme imkânı sağlamaktadır. Kullanılan kriptografi teknolojisi sayesinde sistemin güvenilirliğinin artması, işlemlerin blok zincir üzerinden yürütülmesi sebebiyle özellikle işletmeler açısından sürecin hızlanması ve maliyetlerin düşmesi, çalışanların verilere gerçek zamanlı olarak ulaşabilmesi sayesinde üretkenliği artırması, e-ticarette firmalar ve müşterilere şeffaflık, hız ve güvenilirlik sağlaması sistemin en temel faydalarındandır (Habib vd., 2023: 41).

Maliyetinin düşük olma ihtimali ve verimliliğe olan etkisi nedeniyle banka ve finans sektörlerinde birçok yöneticinin blok zincir teknolojisine çekmeye devam etmektedir.

İstanbul Feasibility Study tarafından 2009 yılında dünyadaki sekiz büyük yatırım kuruluşu üzerinde yapılan bir araştırma sonucunda blok zincir teknolojisinin kontrol edilebilirlik ve şeffaflık özelliği sayesinde kanuni ve hukuki gereklere uyma konusundaki giderleri %30-50 oranında azalttığı bulgusuna ulaşılmıştır. Ayrıca iç kontrole imkân vermesi, veri kalitesinin yüksek olması sebebiyle finansal raporlama maliyetlerini %70 oranında azalttığı ve ticari ve merkezi işlem giderlerini %50 oranında azalttığı sonucuna ulaşılmıştır.

Blok zincir teknolojisinin finansal sektörlere olumlu ve olumsuz etkileri bulunmaktadır. Pandey (2024) tek bir merkeze bağlı olmaksızın, dijital kayıtların tutulabildiği, verileri dağıtılmış veri tabanları vasıtasıyla paylaşma fırsatı sunan blok zincir teknolojisine karşı ilginin her geçen gün arttığını ifade etmektedir. Fakat her ne kadar oldukça güvenli olduğu düşünülse de çalışmak isteyen kişi ve kurumlar tarafından bu sisteme oldukça dikkatli yaklaşıldığının altını çizen Pandey, bu durumu 2008-2009 dönemi krizinde o dönem bankacılık ve finans sektörü sisteminin yetersizliğinin ortaya çıkmasıyla açıklamıştır. Ayrıca Pandey, günümüzde özellikle merkez bankaları ödeme sistemleri için önemli devlet politikalarını bu sebepten ötürü benimsediklerini vurgulamıştır.

Ödeme sistemlerinin etkinliği, maliyetinin düşüklüğü, aktarma yollarının uygunluğu için gereken altyapının temin edilmesi, gelişen teknolojik yapı ve talepleri karşılayabilmek, güvenliğin sağlanması, yasal ve finansal riskleri iyi yönetebilmek ve özellikle güvenlik ve gizlilik son yıllarda önemi artan konulardır. Blok zincir teknolojisinin maliyetleri azaltabilme ve özellikle ödemeler konusunda finansal kurumların aracı fonksiyonunu durdurabilme yeteneği oldukça dikkat çekicidir. Blok zincir teknolojisinin umut vadetmesi ile bugün pek çok büyük çaplı banka iş birliklerine katılmaya başlamıştır (Holotiuk, Pisani ve Moonmann, 2017: 916).

Finansal sektörlerde olduğu kadar finansal olmayan pek çok alanda da uygulama fırsatı sunan blok zincir teknolojisi bugün geleneksel sistemlere yönelik bir tehdit olarak görülmemektedir. Özellikle 2017 yılında değerini önemli bir biçimde artıran kripto para birimleri için Avrupa Merkez Bankası Başkanı Mario Draghi, henüz gerçek ekonomiyle olan ilişkisinin çok da güçlü olduğunu söylemenin mümkün olmadığını ifade etmiştir. Fakat gelecekte kripto para birimlerinin oluşturabileceği riskler açısından uluslararası düzeyde daha etkin bir düzenlemeye ihtiyaç duyulacağı üzerinde durulmaktadır (Blockchain Türkiye, 2019).

Avrupa Ödemeler Konseyi tarafından gerçekleştirilen, “Ödemelerde Blok Zincirinin Etkileri” çalışmasında katılımcıların %90’ı 2025 yılına kadar ödemeler konusunda blok zincir teknolojisinin önemli bir etkisinin olacağını ifade etmişlerdir. Bu konuya olumlu bakan kesim içerisinde %36’lık bir bölüm ise özellikle bazı niş alanlarda veya sadece ödeme alanlarında bu etkinin görülebileceğini ifade etmişlerdir. %30’luk bir bölüm blok zincir sisteminin ödemeler için yenilikçi bir yol olacağını ifade etmektedirler. %24 oranında bir kısım ise blok zincir sisteminin tüm ödemeler konusunda etkili olacağını düşünmektedir (Casanova, 2016).

Blok zincir sisteminin gelişimini ve sistemin düzenlenmesinde etkili olabilecek kilit etkenleri çevresel etkenler; yasal düzenlemeler, piyasa koşulları ve uygulamaları; teknolojik etkenler, teknolojinin mevcut sistemlerle uyumu ve çalışabilirliği; mali etkenler maliyeti azaltma potansiyeli, projeler, pazar potansiyeli olarak sıralamak mümkündür (Orji vd., 2020: 5-6).

Blok zincir teknolojisinin olası faydalarını şu şekilde sıralamak mümkündür: Finansal alanda özellikle kritik konumda bulunan gruplara etki ettiğinden bu durumu finansal hizmetlere katkıyı da artırabilmektedir. Aracı kurumların etkisizleştirilmesi ile yeni hizmet ve değişimler direkt olarak blok zincir yapısı üzerinde oluşturulabilmektedir. Değer değişimindeki çeşitlilik sebebiyle ticari özellikteki nitelikli varlıkların sayısı artırılabilir. Özellikle gelişmekte olan piyasalarda mülkiyet kayıtlarını ve başka türlü şeyleri de ticarete kullanabilme imkânı sağlanabilmektedir. Gerçekleştirilen tüm işlemleri depolayabilme özelliği şeffaflığı da desteklemektedir.

Blok zinciri sistemi ülkeler için fırsatlar sunabildiği gibi zorlukları da mevcuttur. Şu anki haliyle geleneksel sistemler gibi bir merkez bankası tarafından denetlenemiyor olması daha az kontrol edilmesi olarak da düşünülebilir. Bu sebeple para politikalarının özellikle merkez bankaları tarafından tekrar kontrol edilmesi gerekebilir. Ayrıca blok zincir sistemi üzerindeki işlemlerden alınabilecek vergiler de buna imkân sağlayacaktır.

Blok zinciri için finans uygulamaları hemen hemen her türlü işlem için geçerlidir. Bu örnekler, dünyanın dört bir yanındaki şirketlerde pilotluk yapmakta veya üretime geçmektedir. Deloitte'un "Finans İçin Blok Zincir 2018" raporuna göre finans üzerinde blok zincir sisteminin etkilerini alacak ve borçlar için kendi kendini doğrulayan alt defterleri, nakit ödeme ve ödeme için uyumluluk sağlama, gelir döngüsü yönetimi, ticaret finansı, çalışma sermayesi ve nakit döngüsü iyileştirme, dolandırıcılık ve risk tespiti, garanti tahakkukları ve yönetimi ve sermaye planlaması ve performans yönetimi olarak sıralamak mümkündür.

5. Dünyada ve Türkiye’de Finansal Hizmetlerde Dijitalleşme Verileri

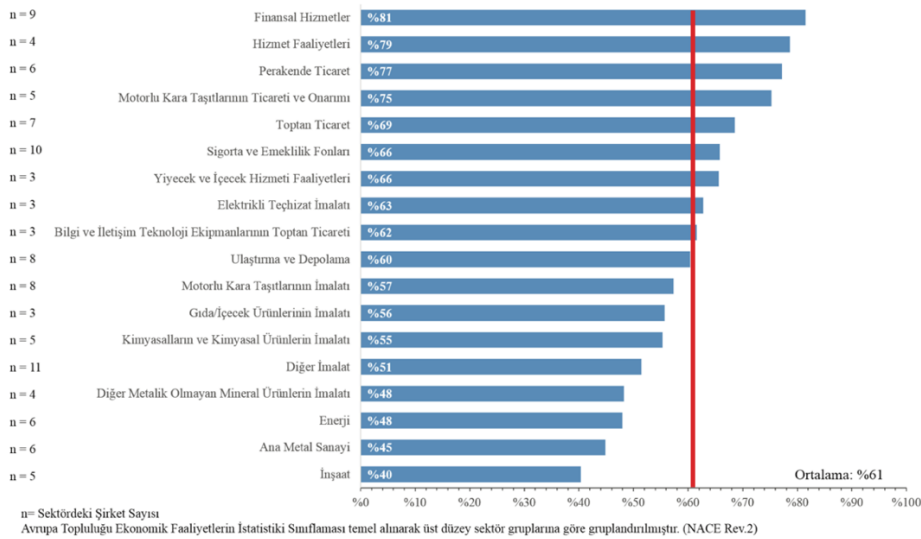
Fintek firmalarının ortaya çıkması ile teknolojiye yapılan yatırımlarda da artışlar olduğu görülmektedir. Özellikle son yıllarda finansal kurumlar ile Fintek ekosistemi arasındaki iş birliklerinin artması sayısız fırsatların oluşmasına neden olmuştur. Finansal kurumların Fintek firmaları ile iş birlikleri yaparak inovasyon eksikliklerini kapatmaya çalıştıkları görülmektedir. Finans kurumlarına rakip olmak yerine onların ürünlerindeki eksikleri gidermeye yönelik

çözümler geliştiren ve kazan-kazan düşüncesiyle hareket eden Fintek’lerin sayısı günden güne artmaktadır (Sezal, 2020: 234).

İnternet erişiminin artması ile teknolojik gelişmelerin hızlandığı görülmektedir. İnternet kullanımının yaygınlaşması dijital dönüşüm süreçlerine önemli katkılar sağlamaktadır. Daha fazla internet erişimi, dünya çapında bilgi üretiminde ve tüketiminde bir patlamaya yol açmaktadır. Bu nedenle rekabeti ve girişi teşvik eden düzenlemeler, dijital fırsatları artıran beceriler, yetkin ve sorumlu ajanslar teknolojinin tamamlayıcısı olarak kabul edilmektedir.

Şekil 3

Sektörlerin Dijitalleşme Endeksi Puanları



Kaynak: Accenture Türkiye Dijitalleşme Endeksi 2016 Raporu

Accenture Dijitalleşme Endeksi (2016) sonuçları sektörlerin dijitalleşme endekslerini göstermektedir. Şekil 3’te gösterildiği gibi, Türkiye’nin 2016’daki Dijitalleşme Endeksi puanı %61’dir. 18 sektör grubunu değerlendiren bu çalışmada, dijital puanı en yüksek sektör %81 ile finansal hizmetler olarak gösterilmiştir. Finansal hizmetleri %79 dijitalleşme oranı ile hizmet faaliyetlerinin takip ettiği Şekil 3’te görülmektedir. En az dijitalleşme oranı %40 ile inşaat sektöründe gösterilmiştir.

6. Dijital Dönüşüm Yaratan Teknolojilerle Birlikte Ortaya Çıkan Güvenlik Sorunları

Şirketlerin ürünlerini ve süreçlerini dijitalleştirilmesi ile ürünün kullanımının ve erişiminin kolaylaşması işlem hacimlerini yükseltmektedir. Bu da beraberinde dolandırıcılık riskinin

artmasına neden olmaktadır. Dijital dönüşüm ile çıkacak zafiyetlerin önlenmesi, siber güvenliği çok daha önemli bir noktaya getirmektedir. Devletlerin ve şirketlerin bünyesinde siber güvenlik bölümleri oluşturulmalı ve bu bölümde çalışanlar eğitimlerle desteklenmelidir. Güvenlik için gerekli yatırım bütçeleri ayrılmalı ve Ar-Ge çalışmaları desteklenerek gerekli altyapılar sağlanmalıdır (Yenice, 2023).

6.1. Siber Tehdit

Bireysel ve örgütsel verilerin gizliliğini yasa dışı bir şekilde aşarak bu verilere erişmek veya var olan sistemi veya verileri tahrip etmek amacıyla gerçekleştirilen her türlü siber saldırı ve/veya saldırı girişimi siber tehdit olarak adlandırılır. Bu tehditlere sunucu web servis hizmetlerini durdurma, virüs yolu ile sisteme erişme ya da trojenler örnek olarak verilebilirler (Şahinaslan, 2003). Özetle sanal ortamda, bireysel ve kurumsal verilerin herhangi birine dönük güvenliği zedeleyen tüm siber saldırılar, “siber tehdit” şeklinde tanımlanmaktadır. Siber tehditler, bir kişi veya kuruluş tarafından başka bir kişinin veya kuruluşun bilgi sistemine girmeye yönelik kötü niyetli, kasıtlı girişimlerdir. Bilgisayar korsanı, genellikle kurbanın ağını bozarak kâr elde etmeye çalışır. Saldırganlar, kurumsal sistemlerdeki güvenlik açıklarından yararlanmaya çalışır ve bu da siber suçlarda yıllık artışa neden olmaktadır (Akşam, 2020).

Siber alandaki tehditler ile bilinen tehditlerin arasında pek çok farklar vardır. Bunların özünde, kuşkusuz tehditlerin daha önce fark edilmesinin olanak ve kıstaslarının çok az olması vardır. Çağımızda internetin yaygınlaşması ve hızlanması ile birlikte siber tehditler de süratli bir biçimde yayılmaktadır. Farklılıklardan biri de yüklenen ve neden olunan maliyetler bakımından gerçekleşmektedir. Siber ortamda bir saldırıda bulunmak üzere ucuz araçlar bile etkili olabilir iken, bu araçlarla saldırıya uğrayan taraf bakımından çok yüksek bedeller söz konusu olmaktadır. Örneğin, bir devlet ya da kurumun sistemine sızmak suretiyle yapılabilecek en basit bir iş duraksaması da milyon dolarlar ile ölçülebilecek zararlara neden olmaktadır. Ya da bir devletin yaptığı tercihlere müdahalede bulunulduğunda tartışmalı bir politik kargaşa çıkmaktadır (Kiraz, 2021:75).

Siber araçlar ile gerçekleştirilen saldırıların ülkeler, finans kuruluşları ve kişiler üzerinde yıkıcı etkileri olabileceği bilinmektedir. Özellikle askeri savunma sistemlerinin, kişisel bilgilerin ve finans hizmetlerinin neredeyse büyük oranda internet ve bilgisayar sistemine bağlı olması konunun önemini artırmaktadır. Çünkü internet ağları üstünden ulaşılan söz konusu bilgiler, kısa zaman içinde herkese duyurulmakta, kopyalanmakta ve değiştirilmektedir. Tüm bu tehditleri yönlendiren korsanlar devlet, kurum ve firmaların yok olmasını sağlamanın yerine

yalnızca algı oluşturmaya çalışabilmekte veya pek çok amaca dönük eş zamanlı ve yok edici neticelere neden olabilecek saldırılar da yapabilmektedirler. Bu tip saldırılar ülkelerin, kamu kurumlarının ve özel işletmelerin fonksiyonlarını işlemez hale getirerek kargaşa oluşmasına neden olmaktadır. Böyle saldırılara karşı yeteri kadar siber güvenlik donanımı ve altyapısı bulunmayan devletler ya da firmalar çok ciddi neticelerle karşılaşmak zorunda kalmaktadır. Sürekli gelişmekte olan tehditler ile gelen yeni çalışma ortamları ve güvenlik sorunları, kurum ve şirketlerin IT alanlarına ve siber güvenliğe yoğunlaşmalarına neden olmaktadır (Bolat, 2020:16-17).

6.2. Finansal Hizmetlerde Yapılan Hırsızlık ve Dolandırıcılık Eylemleri

Finansal hizmetlerin dijitalleşmesiyle kullanılan sistemlerin dolandırıcılık eylemine açık kapı bırakması oldukça olasıdır. Dijitalleşme ile dolandırıcılık yöntemleri de dijitalleşmiştir. Bu yöntemlere karşı bazı önlemler mevcuttur. Bireysel düzeyde ve örgütsel düzeyde bu önlemleri uygulamak bireyleri ve kurumları koruyabilmektedir. Her teknoloji suistimali de beraberinde getirmektedir. Dolayısıyla dolandırıcılık tespitinde yol alabilmek için öncelikle dolandırıcılık türlerine aşina olmak gerekir.

Bankacılık hizmetlerinin internet ve mobil üzerinden sunulmasının yaygınlaşması ile müşteriler dolandırıcıların hedefi haline gelmektedir. Bankaların, verdikleri elektronik bankacılık hizmetlerinde oluşabilecek risklerin kontrolü konusunda uzmanlaşması ve güvenlik alt yapılarına yaptığı yatırımlar ile riskleri azalttığı görülmektedir. Özellikle müşterilerin her noktada konuyla ilgili bilgilendirmeleri müşterilerin bilinç düzeylerini artırmakta ve dolandırıcılık eylemlerinin önlenmesinde önemli rol oynamaktadır. Ayrıca denetleyici otoritelere alınan etkili tedbirler gerçekleşen saldırı ve tehditlerin başarı oranını da düşürmektedir. Bankaların elektronik bankacılık hizmetlerini sunarken karşılaştıkları riskler, internet ve mobil bankacılık, kredi kartı ve ATM hizmetleri üzerinde yoğunlaşmaktadır (Aliyeva, 2016).

6.3. E-Dolandırıcılık

E-Dolandırıcılık, Truva atı denilen programlarla internet bankacılığı kullanan müşterilerin internete girişte kullandıkları kullanıcı/kimlik bilgilerinin elde edilmesi yoludur. Kötü niyetli bir yazılım olarak adlandırılan bu sistemin adli iş modeli yapılanması son derece karışıktır. Amaç kullanıcıları gerçek siteye girdiğine ikna ederek kullanıcı ve şifre bilgilerinin çalınmasıdır. Elde edilen bu bilgilerle kullanıcıların hesaplarının boşaltılması

hedeflenmektedir. Ayrıca kullanıcıların kimlik ve hassas bilgileri ele geçirilerek başkalarına satılmaktadır. Bu durumda yasal takip başlatılsa dahi virüsü kimin yazdığının tespiti zordur (Yılmaz, 2016).

6.4. ATM Dolandırıcılığı ve Kart Bilgilerinin Kopyalanması

ATM dolandırıcılığı haberlerine sık sık medyada yer verilmektedir. ATM cihazlarında yer alan kartların bilgilerinin kopyalanması suretiyle ATM cihazlarında hesapların boşaltılması suçudur. Teknik olarak bu yöntemle kart okuma yuvasına yerleştirilen bir aparatla kart bilgileri kopyalanmaktadır (Elçiboğa, 2018).

6.5. Kredi Kartı Dolandırıcılığı

Dolandırıcılar, kart bilgilerini ele geçirmek için kart sahiplerini ikna ederek kurdukları sahte siteler üzerinden işlem yapmalarını sağlamaktadır. Örneğin, 2011 yılı Şubat ayında kredi kartı dolandırıcıları yurtdışında Cocos adasından ücretsiz bir domain alınarak <http://www.ekstreogrenme.co.cc> internet sitesini oluşturmuşlardır. Kurguda, kredi kartı sahiplerinin 7 gün 24 saat kredi kartı borçlarını öğrenebilmeleri amacıyla Türkiye Bankalar Birliği'nin 4982 sayılı Bilgi Edinme Hakkı Kanununa atıfla bu hizmeti verdiği izlenimi oluşturulmuştur. İnternet sitesinin oluşturulmasında TBB'nin amblem ve kurumsal renkleri kullanılmaya çalışılarak kredi kartı kullanıcılarının şüphelenmemeleri sağlanmıştır. Bu yöntemle kredi kartı sahiplerinden banka, kredi kart sahibinin adı, kart numarası, kart türü, son kullanma tarihi, güvenlik kodu, kart şifresi, T.C. kimlik numarası, anne kızlık soyadı, doğum tarihi, müşteri numarası, GSM numaraları istenmiştir. Sahte TBB internet sitesi vasıtasıyla dolandırıcıların elde ettikleri bilgiler uluslararası dolandırıcılık çeteleri tarafından kullanılmış, binlerce vatandaş mağdur olmuştur (Altuğ, 2021).

7. Dolandırıcılık Tespitinde Kullanılabilecek Stratejiler ve Bazı Algoritmalar

Dolandırıcılık tespitinde ilk adım bilinçli farkındalık kazanmaktır. Bu da gerçekle sahte olanın ayırdına varabilme içgörüsü gerektirir. Bireylerin bilinçlendirilmesi ve dolandırıcılık yöntemlerinin tanıtılması dolandırıcılık önlemede ilk sırada yer almaktadır. Örgütler, çalışanlarını dolandırıcılık yöntemleri konusunda eğitmeli ve bilişim sistemlerindeki açıkları onarma noktasında hızlı reaksiyon alabilmelidirler. Bireylerin sosyal mühendislik yolu ile bilgilerinin toplanması en sık rastlanan dolandırıcılık yöntemidir. Bireyler bankacılık işlemleri veya diğer dijital araçları kullanarak işlem yaparlarken, kurumların site uzantılarına dikkat

etmeliler, e-posta ile tanımadıkları kişilerden kendilerine gönderilen linkleri tıklamamalı, kişisel verileri içeren formları doldurmamalıdır.

Bireysel ve örgütsel düzeyde farkındalık dolandırıcılık önlemede büyük fayda sağlamaktadır. Lakin bireyleri aşan düzeyde siber saldırıların gerçekleşmesi halinde, örgütlerin siber savunma kalkanları oluşturmaları elzemdir. Bu noktada dolandırıcılık tespitinde bazı makine öğrenmesi algoritmaları kullanılarak güvenlik sağlanabilir. Bu algoritmalarından dolandırıcılık tespitinde en sık kullanılanlar makine öğrenmesi ve veri madenciliği algoritmalarıdır. Veri madenciliği algoritmaları ile verilerde gizlenen bilgiler ortaya çıkarılabilmektedir. Bunlar en temel olarak doğrulamaya dayalı algoritmalar ve keşfe dayalı algoritmalar olarak iki kategoriye ayrılırlar. Bu algoritmalarından en çok kullanılanları hipotez testi, sınıflama algoritması, ilişkilendirme algoritması, kümeleme algoritması olarak sıralanmaktadır (Simoudis, 1996).

Makine öğrenmesi algoritmaları, farklı bağlamlarda etkinlik gösteren çeşitli yöntemlerle finansal dolandırıcılığın tespit edilmesinde çok hayati bir rol oynamaktadır. Temel algoritmalar arasında Sinir Ağları (*Neural Networks*), Rastgele Orman (*Random Forest*), Destek Vektör Makineleri (*Support Vector Machines - SVM*) ve Gradyan Güçlendirme Ağaçları (*Gradient Boosting Trees*) yer almaktadır. Bu algoritmaların her biri doğruluk ve performans kriterleri açısından değerlendirildiklerinde yüksek performans göstermektedirler (Obeng vd., 2024; Bello vd., 2004; Sharma vd., 2024).

Dolandırıcılık tespiti ve önlenmesinde kullanılan algoritmalarından Sinir Ağları %97,5 doğruluk oranı ile zirvede yer almaktadır (Xu, 2024). Sinir Ağları gerçek zamanlı işlemlerde oldukça etkili sonuçlar vermektedirler, dolandırıcılık faaliyetlerinin tespit süresini kısalttıklarından önemli bir önleme aracı olarak kullanılabilirler (Bello vd., 2024; Sharma vd., 2024).

Rastgele Orman (*Random Forest*) %96,3'lük doğruluk oranı ile dolandırıcılık tespitinde etkili sonuçlar vermektedir (Xu, 2024). Bu algoritma kredi kartı ve banka dolandırıcılığı dahil olmak üzere birçok dolandırıcılık türü tespitinde kullanılmaktadır (Han, 2024; Mohaimin vd., 2024).

Destek Vektör Makineleri (SVM) sıklıkla hileli işlemleri normal işlemlerden ayırt etmede kullanılmaktadır. Bu algoritmanın en güçlü yönü mükemmel olan karmaşık karar sınırları oluşturmasıdır. Bu algoritma çeşitli alanlarda kullanılmaktadır. Sağlık ve otomobil sigortası işlemleri sırasında gerçekleşme olasılığı olan dolandırıcılık eylemlerini saptamada oldukça iyidir (Han, 2024; Ranisavargaonkar vd., 2024).

Gradyan Güçlendirme Ağaçları kredi riski değerlendirmesinde %90,5 doğrulukla başarıyla kullanılmıştır (Xu, 2024). Bu algoritma topluluk öğrenme yaklaşımını baz aldığından ötürü genel tespit ve doğruluk oranını artırmaya yardımcı olmaktadır (Bello vd., 2024). Dolandırıcılık tespitinde kullanılan bu algoritmalar etkili sonuçlar vermesine rağmen, verilerin dengesizliği ve yorumlanmasında yaşanan sıkıntılar finansal dolandırıcılık konusunda endişe yaratan konular olarak bireylerin ve örgütlerin yaşamında önemli yer edinmeye devam edecektir. Dolayısıyla bu sorunları etkili bir şekilde değerlendirmek ve dolandırıcılık eylemlerinin önüne geçmek için kullanılan algoritmaların sürdürülebilirliği ve geliştirilmesi elzemdir. Bu da sürekli araştırma ve geliştirme faaliyetlerinin kurumların ve bireylerin hayatında yer edinmesi ile mümkün olabilir.

8. Sonuç ve Öneriler

Bu çalışmada dijital dönüşüm kavramı ele alınmış ve işletmelerde dijital dönüşüm kavramının bileşenleri bu alandaki çalışmalar ile vurgulanmıştır. Günümüzde bilgi teknolojisi çeşitli alanlarda uygulanmaktadır. Bu doğrultuda son yıllarda işletmelerin teknik altyapılarını değiştirmeye çalışarak iş modellerinden organizasyon yapılarına kadar pek çok alanda dijitalleşme sürecine dikkat etmeye başladıkları görülmektedir. İşletme açısından bu kavramlarla başa çıkmak için doğru yöntemi benimsemenin önemi yadsınamaz. Bununla birlikte şirketlerin dijitalleşme sürecinde tek bir kavramdan çok birçok kavramla karşı karşıya kaldıkları görülmektedir. Buna yönelik olarak, şirketler mevcut durumu analiz etmeli ve tüm iş süreçlerini veya geleceğe yönelik planlarını kapsayan bir dönüşüm stratejisi geliştirmelidir. Bu ancak şirketler farklı dijital kavramları iş modellerine ne zaman ve nasıl birleştireceklerini anladıklarında ve kısacası bu alanda gerekli bilgiye sahip olduklarında mümkündür. Bu sebeple dijital dönüşümle ilgili her bileşenin gereksinimlerine odaklanarak dijital dönüşüm stratejileri oluşturmak ve bunları iş süreçlerine uyarlamak faydalı olabilmektedir. Blok zincir teknolojisinin kullanımları teşvik edilerek merkezi kayıt kuruluşlarına ihtiyaç duyulmadan daha güvenli ve kritik kayıtların tutulması sağlanmalıdır. Blok zincir altyapıları sayesinde kamu ve finansal şirketlerin kritik hizmetlerini elektronik ortamlardan güvenli ve hızlı bir şekilde verilmesi sağlanmalıdır. Bu teknolojinin yaygınlaşması ile kamu ve finans şirketlerinde verimlilik artırılmalıdır.

Dijital dönüşüm sürecinde ortaya çıkan yeni teknolojilerde yapay zekâ, büyük veri, blok zincir teknolojisi ve makine öğrenimi öne çıkmaktadır. Dijital dönüşüm, strateji gerektiren uzun bir süreçtir. Süreç içerisinde iş modellerinin, altyapı teknolojilerinin, ürünler ve hizmetlerin

değişmesi beklenmektedir. Bu değişim ve dönüşümler bazı güvenlik açıklarını da beraberinde getirmektedir. Dolandırıcılığı önlemek ve dijitalleşmeden maksimum verim alabilmek için örgütlerin bireysel ve örgütsel farkındalığı artırmaları gerekmektedir. Bunun yanı sıra siber tehditlere karşı yine teknolojiyi kullanarak mücadele vermeliler. Bu teknolojiler çok çeşitli olmakla birlikte, finans alanında dolandırıcılık önlemede en etkili tekniklerden biri veri madenciliği algoritmaları ve makine öğrenmesi algoritmalarıdır. Bu algoritmalar kullanılarak finans sektöründe dolandırıcılık tespiti yapılarak olası zararların üstesinden gelinebilir. Hâlihazırda var olan literatürden hareketle dolandırıcılık tespitinde etkili olduğu düşünülen ve desteklenen algoritmaları şu şekilde sıralayabiliriz: Sinir Ağları (*Neural Networks*), Rastgele Orman (*Random Forest*), Destek Vektör Makineleri (*Support Vector Machines - SVM*) ve Gradyan Güçlendirme Ağaçları (*Gradient Boosting Trees*). Veri madenciliği algoritmaları ise verilerde gizlenen bilgileri ortaya çıkarabilmektedir. Bunlar en temel olarak doğrulamaya dayalı algoritmalar ve keşfe dayalı algoritmalar olarak iki kategoriye ayrılırlar. Hem veri madenciliği algoritmaları hem de makine öğrenmesi algoritmalarının her biri doğruluk ve performans kriterleri açısından değerlendirildiklerinde yüksek performans göstermektedirler (Obeng vd., 2024; Bello vd., 2004; Sharma vd., 2024; Xu vd., 2024; Han, 2024; Ranisavargaonkar vd., 2024; Simoudis, 1996).

Sonuç olarak, dijitalleşme birçok ana teknoloji ekseninde gerçekleşmektedir. Bu teknolojilerin işletmelerde ve finans sektöründe kullanımı sürdürülebilir rekabet avantajı geliştirilmesi noktasında örgütlere faydalı olmaktadır. Fakat bu işin karanlık bir tarafı vardır. Bu da bu sistemlerin siber saldırılarla erişime açılma olasılığıdır. Bu noktada ilk olarak işletmelerin ve finansal hizmetlerden faydalanan bireylerin dolandırıcılık eylemleri konusunda bilgilendirilmeleri ve bilinçli farkındalık kazanmaları elzemdir. Örgütlerin dolandırıcılığa karşı strateji geliştirmeleri gerekmektedir. Bu önlem ve farkındalıklara ilaveten kurumların finansal hizmetlerdeki dolandırıcılık eylemlerini saptamak maksadıyla veri madenciliği ve makine öğrenmesi algoritmalarından kendi durumlarına uygun olanı kullanmaları güvenlik açısından gereklidir. Hem bilinçli farkındalık hem de algoritmik kalkanlarla dolandırıcılık tespiti ve önlenmesi noktasında önemli adımlar atılabilir.

Bu çalışmada, dijital dönüşüm kavramının temel unsurları ve bileşenleri incelenmiştir. Bunun yanı sıra dolandırıcılık tespitinde kullanılan doğruluk derecesi yüksek makine öğrenmesi ve veri madenciliği algoritmalarına değinilmiştir. Dijitalleşme sürecinde ortaya çıkan siber saldırılarla ve dolandırıcılıkla mücadelede yine teknolojik araçların kullanımının önemi bu çalışmada vurgulanmıştır. Dolandırıcılık tespitinde dijital araçlarla birlikte bilinçli farkındalık

ile sosyal mühendislik ve diğer dolandırıcılık tekniklerinin önlenmesinin mümkün olduğu vurgulanmıştır. Çalışmanın, dijital dönüşüm sürecinde ortaya çıkan kavramlar ve bu kavramları incelemeyi amaçlayan kişiler için başlangıç rehberi/yol haritası olarak literatüre katkı sağlaması beklenmektedir.

Kaynakça

- Accenture. (2016). Türkiye Dijitalleşme Endeksi, https://www.accenture.com/t20170202T045842Z__w_/tr-en/_acnmedia/PDF-42/Accenture-HBR-Rapor-Vodafone.pdf.
- Adalı, E. (2017). Yapay Zekâ. İTÜ Vakfı Dergisi, 75, s. 8-13.
- Aliyeva, B. (2016). “Bankacılık sisteminde internetin olumlu ve olumsuz yönleri”, İnönü Üniversitesi Uluslararası Sosyal Bilimler Dergisi, 5(1): 237-252.
- Akşam, 2020. “Siber güvenlik tehditleri nelerdir? Tehdit türleri ve siber saldırıların önlenmesi nasıl olur?”, Akşam, <https://www.aksam.com.tr/teknoloji/siber-guvenlik-tehditleri-nelerdir-siber-guvenlik-konusunda-nelere-dikkat-edilmeli/haber-1137402>. (Erişim tarihi: 20 Mart 2024).
- Altuğ, Ş. (2021). “Banka veya kredi kartlarının kötüye kullanılması”, Uyuşmazlık Mahkemesi Dergisi, 17: 1-44.
- Arner, Douglas W., Janos Barberis, ve Ross P. Buckley (2017). “FinTech, RegTech and the Reconceptualization of Financial Regulation.” *Northwestern Journal of International Law and Business*.
- Balasoto, C. (2024). “The Importance of Digitalization in Business in Today’s Digital World”, LinkedIn, 3 Ocak. <https://www.linkedin.com/pulse/importance-digitalization-business-todays-digital-world-balasoto-7chuc> (Erişim tarihi: 10 Şubat 2023).
- Başer, E. & Akıncı, S. (2020). “Kullanıcı Deneyimi ve Kişiselleştirme Bağlamında Bir Dijital Platform İncelemesi” *Selçuk İletişim Dergisi*, 13(2): 866-897.
- Bello., H., O., Courage, I., Toluwalase, V., Iyelolu. (2024). 2. Implementing machine learning algorithms to detect and prevent financial fraud in real-time. *Computer science & IT research journal*, doi: 10.51594/csitrj.v5i7.1274
- Bharadwaj A., El Sawy O., Pavlou P.A. & Venkatram N. (2013). *Digital Business Strategy: Toward a Next Generation of Insights*. *MIS Quarterly*, 37(2): 471-482.
- Blockchain Use Cases, “What are the Benefits of Blockchain in Finance?” <https://consensus.io/blockchain-use-cases/finance>. (Erişim tarihi: 20 Mart 2024).
- Blockchain Türkiye, 2019. “Avrupa Merkez Bankası yetkilisinden açıklama: Kripto masalı sona erdi”, Blockchain Türkiye, 8 Ocak. <https://bctr.org/avrupa-merkez-bankasi-yetkilisinden-aciklama-kripto-masali-sona-erdi-7215/> (Erişim tarihi: 20 Mart 2024).
- Bolat, C. (2020). “Siber saldırılara karşı meşru müdafaa hakkının uluslararası hukuk açısından incelenmesi”, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı Tezi.

- Casanova, Kylene (2016). “90% say blockchain will significantly impact EU payments by 2025 – EPC poll” Cash and Treasury Management File, 10 Ağustos. <https://ctmfile.com/story/90-say-blockchain-will-significantly-impact-eu-payments-by-2025-epc-poll> (Erişim tarihi: 20 Mart 2024).
- Çakar, Tarık; Çil, İbrahim ve Kurt, Akif, (1997). “Uzman sistemlerin tasarımı, geliştirilmesi ve bilgi mühendisliğinin rolü”, Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 1: 33-40. <https://dergipark.org.tr/tr/download/article-file/193047>
- Deloitte, (2017). Connecting global fintech: Intern hub review 2017, <https://www2.deloitte.com/tr/en/pages/finance/articles/atale-of-44-cities-global-FinTech-hub-federation-gfhfconnecting-global-Fintech-hub-report.html>.
- Di Palo, N. (2017). “Teachable robots are the new programmable robots, How the paradigm is shifting from programming to teaching machines”, Medium, 28 Kasım. <https://www.linkedin.com/pulse/smart-robots-convergence-ai-robotics-baleshwar-yadav> (Erişim tarihi: 20 Mart 2024).
- Digital Europe (2020). “Dijital Çağ İçin Dönüşüm Gündemi” Digital Europe’un 2020 Vizyonu.
- Elçiboğa, K. (2018). “Kartlı Ödeme Dolandırıcılık Türleri, Risk ve Mali Sorumlulukları”, FinTechTime, 17 Şubat. <https://fintechtime.com/2018/02/kartli-odeme-dolandiricilik-turleri-risk-ve-mali-sorumluluklari/>.(Erişim tarihi: 20 Mart 2024).
- England, J. (2022). “Technology in Fintech and the story of Online Banking”, FinTech, 08 June. <https://fintechmagazine.com/banking/fintech-timelines-and-the-story-of-online-banking> (Erişim tarihi: 20 Mart 2024).
- EY-Capital Markets (2016). “Innovation and the FinTech Landscape, How collaboration with FinTech can transform investment banking” https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-capital-markets-innovation-and-the-fintech-landscape.pdf (Erişim tarihi: 20 Mart 2024).
- Fernado, C. (2018). “Evolution of distributed systems”, LinkedIn, 24 Mart. <https://www.linkedin.com/pulse/evolution-distributed-systems-chanaka-fernando> (Erişim tarihi: 10 Şubat 2023).
- Finartz 2023. “E-Para Kuruluşları için Dijital Cüzdanlar”, Finartz, 25 Ağustos. <https://tr.linkedin.com/pulse/e-para-kurulu%C5%9Flar%C4%B1-finartz> (Erişim tarihi: 10 Şubat 2023).
- Gürgüze, G. & Türkoğlu, İ. (2019). “Kullanım Alanlarına Göre Robot Sistemlerinin Sınıflandırılması” Fırat Üniversitesi Müh. Bil. Dergisi, 31(1): 53-66.
- Google trends. (2018). Bigdata. google.com, <https://trends.google.com/trends/explore?date=all&q=big%20data>
- Han Y. (2024). 3. An Investigation of Machine Learning Applications in the Financial Fraud Detection. *Advances in Economics, Management and Political Sciences*, doi: 10.54254/2754-1169/98/2024ox0125
- Harding, M., Hersh, J. Big Data in Economics. IZA World of Labor (2018). 451 doi: 10.15185/izawol.451

- Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., ve Ishfaq, M. (2024). "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing", *Future Internet*, 14(11): 41
- Hassani, H.; Silva, Emmanuel S.; Unger, S.; Taj M., Maedeh; Mac F., Stephen 2020 "Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future?" *AI Basel 1 (2)*: 143-155.
- Hepaktan, C.E., Şimşek, D. (2022). "Industry 4.0 and The Future of The Labor Market". *İzmir Sosyal Bilimler Dergisi*, 4(2), 80-88.
- Holotiuk, F., Pisani, F., Moormann, J. (2017) The Impact of Blockchain Technology on Business Models in the Payments Industry, in Leimeister, J.M.; Brenner, W. (Hrsg.): *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, St. Gallen, S. 912-926
- Istanbul Feasibility Study IFC (2009), Deloitte Consultancy on behalf of The Banks Association of Turkey. <https://www.tbb.org.tr/english/raporing.pdf>
- Kiraz, O. Z. (2021). "Siber Güvenlik Bağlamında Yeni Tehdit Algılamalarının Türkiye'nin Güvenlik Politikalarına Etkileri", *Journal of Management Theory and Practices Research*, 2(2): 69-88.
- Mah, P. M. (2022). "Analysis of artificial intelligence and natural language processing significance as expert systems support for e-health using pre-train deep learning models," *Acadlore Trans. Mach. Learn.*, 1 (2): 68-80. <https://doi.org/10.56578/ataiml010201>
- Mergel, I.; Edelman, N.; ve Haug, N. (2019) "Defining digital transformation: Results from expert interviews", *Government Information Quarterly*, 36, (4): 1-16.
- MIS (2014). "The role of big data for ICT monitoring and for development", (ed.) *Measuring the Information Society Report 2014 (173-205)*. ITU Yayınları https://www.itu.int/en/ITU-D/Statistics/Documents/bigdata/MIS2014_Chapter5.pdf
- Mohaimin, M. R., Sumsuzoha, M., Pabel, M. A. H., & Nasrullah, F. (2024). Detecting Financial Fraud Using Anomaly Detection Techniques: A Comparative Study of Machine Learning Algorithms. *Journal of Computer Science and Technology Studies*, 6(3), 01-14.
- Oancea, B. (2024). Big data in economics. arXiv preprint arXiv:2406.11913. doi: 10.48550/arxiv.2406.11913
- Obeng, S., Iyelolu, T. V., Akinsulire, A. A., & Idemudia, C. (2024). Utilizing machine learning algorithms to prevent financial fraud and ensure transaction security. *World Journal of Advanced Research and Reviews*, 23(1), 1972-1980. doi: 10.30574/wjarr.2024.23.1.2185
- Orji, Ifeyinwa Juliet; Kusi-Sarpong, Simonov; Huang, Shuangfa; Vazquez-Brust, Diego (2020) "Evaluating the factors that influence blockchain adoption in the freight logistics industry", *Logistics and transportation review*, 141: 1-26.
- Ortar, Okşan ve Yeşiltaş, Candan (2021). "Ekonomideki Dijital Dönüşüm ve İstihdam Üzerindeki Etkisi". *Working Paper Series Dergisi*, 2(1), 43-52. <http://workingpaperseries.ticaret.edu.tr/index.php/wps/article/view/36> (Erişim tarihi: 15 Mart 2021)
- Öz, Esra 2022. "Yapay zekâ ile insan gibi düşünen, duygulanan ve karar verebilen robotlar geliyor", *Independent Türkiye*, 18 Mart.

- <https://www.indyturk.com/node/486106/bi%CC%87li%CC%87m/yapay-zeka-ile-insan-gibi-d%C3%BC%C5%9F%C3%BCnen-duygulanan-ve-karar-verebilen-robotlar-geliyor>. (Erişim tarihi: 20 Mart 2024).
- Quinn, S. ve Roberds, W. (2008). “The Evolution of the Check as a Means of Payment: A Historical Survey.” *Economic Review*, 93(4).
- Pandey, V. (2024). “Blockchain Revolution: Rethinking Finance and Banking” LinkedIn, 23 Şubat. https://www.linkedin.com/pulse/blockchain-revolution-rethinking-finance-banking-dr-vivek-pandey-jzomf?trk=article-ssr-frontend-pulse_more-articles_related-content-card (Erişim tarihi: 20 Mart 2024).
- Ranisavargaonkar. S. S., Vaishnavi, J., Kishore, M. (2024). 5. Machine Learning Approaches for Credit Card Fraud Detection. *International Journal of Advanced Research in Science, Communication and Technology*, doi: 10.48175/ijarsct-17896
- Sezal, L. (2020). “Fintek Hizmetlerinin Finans Sektörüne Etkileri ve Sağlanan Devlet Teşvikleri” *Ekonomi İşletme Maliye Araştırmaları Dergisi*, 2(3): 233-248.
- Sinap, V. (2024). Comparative analysis of machine learning techniques for credit card fraud detection: Dealing with imbalanced datasets. *Turkish Journal of Engineering*, 8(2), 196-208. <https://doi.org/10.31127/tuje.1386127>
- Simoudis, E., (1996). Reality check for data mining, In *IEEE Expert: Intelligent Systems and Their Applications*, (5): 26-33.
- Sharma, R., & Sharma, A. (2024). Combatting Digital Financial Fraud through Strategic Deep Learning Approaches. In *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)*: 824-828. IEEE. doi: 10.1109/icscss60660.2024.10625249
- Start Smarter Editorial Team 2024. “The advantages and disadvantages of digitalisation” *Start Smarter* <https://startsmarter.co.uk/the-advantages-and-disadvantages-of-digitalisation/> (Erişim tarihi: 10 Şubat 2023).
- Syamsuddin; S.; Yusrizal ; D., Tuti; Fatmawati, E. (2024). “Utilizing Blockchain Technology in Global Supply Chain Management: An Exploration of Scalable Information Systems” *EAI endorsed transactions on scalable information systems*, 11 (1): 1-12.
- Şahinaslan Ö. (2003). *Siber Saldırılarına Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma*. Doktora, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne
- Şükranlı, D. (2020). *The Effect Of Company’s Level of Digitalization on Employee Satisfaction and Productivity*. Master’s Thesis, The Republic of Turkey Bahçeşehir University Graduate School of Social Sciences Master of Business Administration Program, İstanbul.
- Tayaksi, ; A. ve Kazançoğlu (2016) “Bulut Üretim: İşlemler Yönetiminde Yeni Bir Bulut Bilişim Modeli”, *Ege Akademik Bakış* 16, 71-83.
- Valente, Jorge; Anónio, João; M., Carlos; Jardim, S. (2023). “Developments in Image Processing Using Deep Learning and Reinforcement Learning”, *Basel*, 9(10): 207-230.
- Vassakis, K., Petrakis, E., Kopanakis, I. (2018). “Big Data Analytics: Applications, Prospects and Cahllenges”, *Mobil Big Data, Lecture Notes on Data Engineering and*

- Communications Technologies 10, ISBN 978-3-319-67925-9 (eBook), Springer International Publishing AG 2018, s. 3-20.
- Wang, Y., Kung, L., Byrd, T.A., (2016). Big Data Analytics: Understanding Its Capabilities and Potential Benefits for Healthcare Organizations. *Technological Forecasting And Social Change*. 126 (1), 3-13.
- World Bank (2016). World Development Report 2016: Digital Dividends, 17 Mayıs, <http://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf>.
- World Economic Forum (2016). The Fourth Industrial Revolution: What It Means, How To Respond, <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>
- World Economic Forum (2024) “How 6 mid-market companies are using AI to scale”, Artificial Intellegence, <https://www.weforum.org/agenda/2024/01/5-ways-ai-can-help-mid-market-companies-grow-faster/>
- Xu. T. (2024). 1. Fraud Detection in Credit Risk Assessment Using Supervised Learning Algorithms. doi: 10.54097/qw9j1892
- Yenice, H. B. (2023). “Siber Güvenlik: Önemi, Fırsatları ve Zorlukları”, *Turkom*, 19 Ekim, <https://tr.linkedin.com/pulse/siber-g%C3%BCvenlik-%C3%B6nemi-f%C4%B1rsatlar%C4%B1-ve-zorluklar%C4%B1-turcomofficial>. (Erişim tarihi: 20 Mart 2024).
- Yılmaz, A. Tuğsan (2016). “İnternet Bankacılığı ile Yapılan Dolandırıcılık”, *Fikri Sinai Haklar ve Bilişim Hukuku*, 12 Mayıs. <https://www.tugsanyilmaz.av.tr/fikri-haklar-ve-bilisim-hukuku/internet-bankaciligi-ile-yapilan-dolandiricilik>. (Erişim tarihi: 20 Mart 2024).