

PARADOKS EKONOMİ, SOSYOLOJİ ve POLİTİKA DERGİSİ

PARADOKS Economics, Sociology and Policy Journal

Cilt/Vol: 21, Sayı/Issue: 1, Sayfa/Page: 62-86

Yıl: 2025

ISSN: 1305-7979



PARADOKS
Ekonomi, Sosyoloji ve Politika Dergisi



PARADOKS
Ekonomi, Sosyoloji ve Politika Dergisi

Editörler / Editors in Chief

Baş Editör

Prof. Dr. Elif KARAKURT TOSUN

Alan Editörü

Prof. Dr. Sema AY

Teknik Editör

Prof. Dr. Hilal YILDIRIR KESER

TARANDIĞIMIZ INDEXLER



Dergide yayınlanan yazılardaki görüşler ve bu konudaki sorumluluk yazarlarına aittir. Yayınlanan eserlerde yer alan tüm içerik kaynak gösterilmeden kullanılamaz.

All the opinions written in articles are under responsibilities of the authors. None of the contents published cannot be used without being cited.

Yayın ve Danışma Kurulu / Publishing and Advisory Committee

Prof. Dr. Sema AY (Uludağ Üniversitesi)
Prof. Dr. Veysel BOZKURT (İstanbul Üniversitesi)
Prof. Dr. Marijan CINGULA (University of Zagreb)
Prof. Dr. Recai ÇINAR (Gazi Üniversitesi)
Prof. Dr. Elif KARAKURT TOSUN
Prof. Dr. Aşkın KESER (Uludağ Üniversitesi)
Prof. Dr. Emine KOBAN (Gaziantep Üniversitesi)
Prof. Dr. Ferhat ÖZBEK (Gümüşhane Üniversitesi)
Prof. Dr. Senay YÜRÜR (Yalova Üniversitesi)
Assoc. Prof. Dr. Mariah EHMKE (University of Wyoming)
Doç. Dr. Zerrin FIRAT (Uludağ Üniversitesi)
Assoc. Prof. Dr. Ausra REPECKIENE (Kaunas University)
Assoc. Prof. Dr. Cecilia RABONTU (University “Constantin Brancusi” of TgJiu)
Prof. Dr. Hilal YILDIRIR KESER (Bursa Teknik Üniversitesi)
Dr. Murat GENÇ (Otago University)

Hakem Kurulu / Referee Committee

Prof. Dr. Hamza ATEŞ (Kocaeli Üniversitesi)
Prof. Dr. Veysel BOZKURT (İstanbul Üniversitesi)
Prof. Dr. Marijan CINGULA (University of Zagreb)
Prof. Dr. Recai ÇINAR (Gazi Üniversitesi)
Prof. Dr. Kemal DEĞER (Karadeniz Teknik Üniversitesi)
Prof. Dr. Mehmet Sami DENKER (Dumlupınar Üniversitesi)
Prof. Dr. Bülent GÜNŞOY (Anadolu Üniversitesi)
Prof. Dr. Ömer İŞCAN (Atatürk Üniversitesi)
Prof. Dr. Vedat KAYA (Atatürk Üniversitesi)
Prof. Dr. Sait KAYGUSUZ (Uludağ Üniversitesi)
Prof. Dr. Aşkın KESER (Uludağ Üniversitesi)
Prof. Dr. Emine KOBAN (Gaziantep Üniversitesi)
Prof. Dr. Ahmet MUTLU (Samsun Ondokuz Mayıs Üniversitesi)
Prof. Dr. Nilüfer NEGİZ (Süleyman Demirel Üniversitesi)
Prof. Dr. Serap PALAZ (Balıkesir Üniversitesi)
Prof. Dr. Ali Yaşar SARIBAY (Uludağ Üniversitesi)
Prof. Dr. Abdülkadir ŞENKAL (Kocaeli Üniversitesi)
Prof. Dr. Veli URHAN (Gazi Üniversitesi)
Prof. Dr. Sevtap ÜNAL (Atatürk Üniversitesi)
Prof. Dr. Sevda YAPRAKLI (Atatürk Üniversitesi)
Prof. Dr. Uğur YOZGAT (Marmara Üniversitesi)
Prof. Dr. Senay YÜRÜR (Yalova Üniversitesi)
Doç. Dr. Rasim AKPINAR (Manisa Celal Bayar Üniversitesi)
Doç. Dr. Gül ATANUR (Bursa Teknik Üniversitesi)
Doç. Dr. Tülin ASLAN (Uludağ Üniversitesi)
Doç. Dr. Arzu ÇAHANTİMUR (Uludağ Üniversitesi)
Doç. Dr. Ceyda ÖZSOY (Anadolu Üniversitesi)
Doç. Dr. Doğan BIÇKI (Muğla Üniversitesi)
Doç. Dr. Elif ÇOLAKOĞLU (Atatürk Üniversitesi)
Doç. Dr. Mithat Arman KARASU (Harran Üniversitesi)
Doç. Dr. Mustafa KOCAOĞLU (Konya Necmettin Erbakan Üniversitesi)
Doç. Dr. Ahmet MUTLU (Ondokuz Mayıs Üniversitesi)
Doç. Dr. Nilüfer NEGİZ (Süleyman Demirel Üniversitesi)
Doç. Dr. Veli Özer ÖZBEK (Dokuz Eylül Üniversitesi)
Doç. Dr. Ferhat ÖZBEK (Gümüşhane Üniversitesi)
Assoc. Prof. Dr. Cecilia RABONTU (University “Constantin Brancusi” of TgJiu)
Assoc. Prof. Dr. Ausra REPECKIENE (Kaunas University)

Doç. Dr. Gözde YILMAZ (Marmara Üniversitesi)
Doç. Dr. Aybeniz AKDENİZ AR (Balıkesir Üniversitesi)
Dr. Öğr. Üyesi Cantürk CANER (Dumlupınar Üniversitesi)
Dr. Öğr. Üyesi Işın KIRIŞKAN (Giresun Üniversitesi)
Dr. Öğr. Üyesi Burcu ÖNGEN BİLİR (Bursa Teknik Üniversitesi)
Dr. Öğr. Üyesi Ersoy SOYDAN (Kastamonu Üniversitesi)
Dr. Öğr. Üyesi Oğuzhan ÖZALPIN (Isparta Uygulamalı Bilimler Üniversitesi)
Dr. Murat GENÇ (Otago University)
Dr. Enes Battal KESKİN (Uludağ Üniversitesi)



Paradoks Ekonomi Sosyoloji ve Politika Dergisi

Yıl: 2025, Cilt/Vol: 21, Sayı/Issue: 1

HAKEM KURULU

Prof. Dr. Gökçe Çiçek CEYHUN	BURSA TEKNİK ÜNİVERSİTESİ
Prof. Dr. Halit Burç AKA	TEKİRDAĞ NAMIK KEMAL ÜNİVERSİTESİ
Prof. Dr. Funda YİRMİBEŞOĞLU	İSTANBUL TEKNİK ÜNİVERSİTESİ
Doç. Dr. Esra ÇIKMAZ	GAZİANTEP ÜNİVERSİTESİ
Doç. Dr. Yaprak ÖZEL	İSTANBUL NİŞANTAŞI ÜNİVERSİTESİ
Doç. Dr. Gülşen ÇETİN AYDIN	KARAMANOĞLU MEHMETBEY ÜNİVERSİTESİ
Doç. Dr. Mehmet Fatih ÇÖMLEKÇİ	KIRKLARELİ ÜNİVERSİTESİ
Dr. Öğr. Üyesi Gökmen DURMUŞ	GAZİANTEP ÜNİVERSİTESİ
Dr. Öğr. Üyesi Ercan İNCE	İĞDIR ÜNİVERSİTESİ
Dr. Öğr. Üyesi Gülayşe ÜLGEN TÜREDİ	KIRKLARELİ ÜNİVERSİTESİ
Dr. Öğr. Üyesi Bilge ÇAĞATAY	FENERBAHÇE ÜNİVERSİTESİ

İŞLETMELERDE, HİLE TESPİTİ VE ÖNLENMESİ SÜREÇLERİNDE YAPAY ZEKÂ UYGULAMALARIYLA VERİMLİLİĞİN ARTIRILMASI

Mehmet ERKAN

*Prof. Dr., İstanbul Gedik Üniversitesi, İktisadi, İdari ve Sosyal Bilimler Fakültesi,
İşletme Bölümü*

ORCID: 0009-0007-9578-9292

mehmet.erkkan@gedik.edu.tr

İsmail ÖZDEMİR

*Dr. Öğr. Üyesi., İstanbul Gedik Üniversitesi, Gedik Meslek Yüksekokulu,
İnsan Kaynakları Yönetimi Programı*

ORCID: 0000-0001-6478-9168

iozdemir@gedik.edu.tr

Ahmet ERKASAP

*Dr. Öğr. Üyesi., İstanbul Gedik Üniversitesi, İktisadi, İdari ve Sosyal Bilimler Fakültesi,
Yönetim Bilişim Sistemleri Programı*

ORCID: 0000-0002-6239-1700

ahmet.erkasap@gedik.edu.tr

ÖZET

Finansal hilelerin tespit ve önlenmesinde yapay zekâ uygulamalarının rolü giderek önem kazanmaktadır. Geleneksel denetim yöntemlerinin sofistike hile tekniklerini tespit etmede yetersiz kaldığı günümüz iş dünyasında, yapay zekâ teknolojisi, büyük veri setlerini analiz ederek anormallikleri tespit etme, öngörücü analizlerle gelecekteki hileli işlemleri tahmin etme ve gerçek zamanlı izleme gibi yeteneklerle öne çıkmaktadır. Bu yetenekler, işletmelerde operasyonel maliyetleri azaltma ve yanlış pozitif sonuçları minimize etme avantajları sunmaktadır. Ancak, yapay zekânın veri kalitesi, model açıklanabilirliği ve düzenleyici gereklilikler gibi zorluklarla karşı karşıya kaldığı da unutulmamalıdır. Bu nedenle, işletmelerin hileye karşı etkin bir savunma oluşturmak için klasik yöntemleri yapay zekâ teknolojisi ile entegre bir şekilde kullanmaları gerekmektedir.

Anahtar Kelimeler: Yapay Zekâ, Hile, Hile Denetimi, İşletme, Verimlilik.

Jel Sınıflandırması: M40, M10, D20

INCREASING EFFICIENCY WITH ARTIFICIAL INTELLIGENCE APPLICATIONS IN FRAUD DETECTION AND PREVENTION PROCESSES IN ENTERPRISES

Mehmet ERKAN

*Prof. Dr., Istanbul Gedik University, Faculty of Economics, Administrative and Social
Sciences, Department of Business Administration*

ORCID: 0009-0007-9578-9292

mehmet.erkkan@gedik.edu.tr

İsmail ÖZDEMİR

*Assist. Prof. Dr., Istanbul Gedik University, Gedik Vocational School,
Department of Human Resources Management*

ORCID: 0000-0001-6478-9168

iozdemir@gedik.edu.tr

Ahmet ERKASAP

*Assist. Prof. Dr., Istanbul Gedik University, Faculty of Economics, Administrative and
Social Sciences, Department of Management Information Systems*

ORCID: 0000-0002-6239-1700

ahmet.erkasap@gedik.edu.tr

ABSTRACT

The role of artificial intelligence applications in the detection and prevention of financial fraud is becoming increasingly important. In today's business world where traditional audit methods are insufficient to detect sophisticated fraud techniques, artificial intelligence technology stands out with capabilities such as detecting anomalies by analysing large data sets, predicting future fraudulent transactions with predictive analyses and real-time monitoring. These capabilities offer the advantages of reducing operational costs and minimising false positives. However, it should be noted that artificial intelligence faces challenges such as data quality, model explainability and regulatory requirements. Therefore, businesses need to use classical methods integrated with artificial intelligence technology to create an effective defence against fraud.

Key Words: *Artificial Intelligence, Fraud, Fraud Audit, Business, Efficiency.*

Jel Classification: M40, M10, D20

1. GİRİŞ

Varlık hırsızlığı ve finansal hileler, işletmelerin karşı karşıya kaldığı en önemli risklerden ikisidir. İşletmeler tarafından ciddiyle tedbir alınması gereken bu iki yasa dışı durum arasındaki temel farklar, bunların tespit edilme ve önlenmesine yönelik yöntemlerden kaynaklanmaktadır. Günümüzde işletmelerde hilenin tespit edilmesi ve önlemesi için teknolojiye dayalı çeşitli yöntemler kullanılmaktadır. Bu teknoloji yoğun yöntemler, etkin bir hile denetiminin yanında verimliliğin artırılmasına, maliyetlerin düşürülmesine ve muhtemelen rekabet avantajı elde edilmesine de önemli katkılar sağlamaktadır.

Özellikle hızlı gelişen yapay zekâ teknolojileri, işletmelerde hilenin tespiti ve önlenmesinde çok önemli fonksiyonlar üslenmiş ve üstlenmektedir. Yapay zeka teknolojilerinin, gelişmiş algoritmalar ve makine öğrenimi teknikleri kullanılmak suretiyle sunmuş olduğu, büyük hacimli verileri analiz etmek, kalıpları belirlemek, anormallikleri tespit etmek ve şüpheli faaliyetleri gerçek zamanlı olarak belirlemek gibi olanaklar, hilenin mali kayıplara yol açmadan önce etkili bir şekilde tespit edebilmesi ve önleyebilmesini mümkün kılmaktadır.

Güncel araştırmalar, finansal kurumların yapay zekâ harcamalarının 2027 yılına kadar 97 milyar dolara çıkmasının beklendiğini ve finansal sektörün %29,6'lık bileşik yıllık büyüme oranı (CAGR) ile yapay zekâ yatırımında en hızlı büyüyen sektör olduğunu göstermektedir (Vuković et al., 2025). Bu exponansiyel büyüme, JPMorgan ve Morgan Stanley gibi önde gelen finansal firmaları kendi yapay zekâ altyapılarını kurmaya yöneltmiş ve teknolojinin dönüştürücü potansiyelini kabul ettirmiştir.

Yapay zekanın hile tespiti ve önlenmesine yönelik etkinliği artırarak zaman ve kaynaklardan tasarruf edebilmesine katkı sağlamaktadır. Günümüzde, artık işletmeler, hile tespitinde yapay zekâdan yararlanarak finansal işlemlerdeki kalıpları ve anormallikleri etkili bir şekilde belirleyebilmekte, bu da dolandırıcılık faaliyetlerinin zamanında tespit edilmesini sağlamaktadır. Bunun yanında, yapay zekâ, gelecekteki ticari eğilimleri tahminlemekte ve suç işleme niyetinde olanların güvenlik açıklarından yararlanmasını önlemek için sağlam bir güvenlik sistemi kurmaya da yardımcı olmaktadır (Vuković et al., 2025).

Özellikle 2019-2024 yılları arasında yapılan sistematik literatür incelemeleri, organizasyonların yıllık gelirlerinin %5'ini hileye kaybettiğini ve bu durumun trilyonlarca dolarlık bir kayba denk geldiğini ortaya koymaktadır (Chen et al., 2025). Bu çalışmanın amacı, işletmelerdeki finansal hilelerin yapay zekâ ile tespit edilmesi ve önlenmesine ilişkin

uygulamaları ortaya koymak ve güncel literatür bulgularını entegre ederek bu alandaki gelişmeleri kapsamlı bir şekilde değerlendirmektir.

Daha önceki yıllarda yapılan ve literatürde yer alan çalışmalar Makine Öğrenimi Tekniklerinin Karşılaştırmalı Analizi şeklinde olmuştur. Bu çalışmalarda finansal hile tespitinde makine öğrenimi tekniklerinin kullanımında önemli trendleri ortaya koymaktadır (Hernandez Aros vd., 2024).

Yakın geçmişte ve günümüzde yapılan çalışmalar ise, finansal hile tespitinde derin öğrenme tekniklerinin gelişiminde önemli trendleri ortaya koymaktadır (Chen vd., 2025). Bu çalışmalarda; CNN, LSTM ve Transformer modelleri gibi çeşitli derin öğrenme modellerinin etkinliği kanıtlanmış, kredi kartı işlemleri, sigorta talepleri ve finansal tablo denetimleri ana uygulama alanları olarak öne çıkmış ve veri gizliliği çerçevelerinin etkisi ve özellik mühendisliği ile veri ön işleme alanındaki gelişmeler önemli temalar olarak belirlenmiştir. Literatürde yer alan bu konulara; Çin, Hindistan, Suudi Arabistan ve Kanada önde gelen katkı sağlayan ülkeler olarak öne çıkmaktadır. Latin Amerika ülkelerinin bu alanda sınırlı sayıda yayını bulunmaktadır. Araştırmalarda yer alan metodolojik yaklaşımlar; Denetimli öğrenme yaklaşımları, denetimsiz, derin öğrenme, pekiştirmeli ve yarı-denetimli yaklaşımlara kıyasla en yaygın kullanılan yöntem olarak tespit edilmiştir.

Son dönemde hile tespiti ve önlenmesine yönelik çalışmalarda, Blockchain ve Gizlilik Koruyucu Teknolojiler öne çıkmaktadır. Blockchain entegrasyonu ve Principal Component Analysis (PCA) gibi gizlilik koruyucu tekniklerin finansal hile tespitinde artan önemi her geçen zaman daha da belirgin olarak ortaya çıkmaktadır (Chen vd., 2025). Bu teknolojiler hem güvenliği artırmakta hem de düzenleyici gerekliliklere uyumu kolaylaştırmaktadır.

Blockchain Entegrasyonu, Blockchain teknolojisi, işlem kayıtlarının değiştirilemezliğini sağlayarak hile önleme konusunda önemli avantajlar sunmaktadır. Özellikle çoklu taraf işlemlerinde şeffaflık ve güvenilirlik sağlamaktadır.

Gizlilik Koruyucu Tekniklerden, GDPR ve CCPA gibi veri koruma düzenlemelerine uyum sağlamak için geliştirilmiş teknikler, kişisel verilerin korunmasını sağlarken etkili hile tespitine olanak tanımaktadır.

2. İŞLETMELERDEKİ DOLANDIRICILIK

İşletmelerde sıkça karşılaşılan varlık hırsızlığı ve finansal hileler hem finansal hem de işletmelerde itibar kayıplarına yol açabilen ciddi sorunlardır. Bu iki yaşa dışı işlem arasındaki

temel farklar, tespit ve önlenmesine ilişkin yöntemlerden kaynaklanmaktadır. Varlık hırsızlığı, işletmenin fiziksel varlıklarının (nakit, stok, demirbaş vb.) veya dijital varlıkların yetkisiz kişilerce izinsiz olarak alınması veya kullanılmasıyla, finansal hileler ise işletme yönetiminin ya da çalışanlarının mali tablolarında kasıtlı olarak yanlış bilgi verilmesi, gelirlerin veya giderlerin manipüle edilmesi gibi işletmenin mali durumunu olduğundan farklı gösterilmesi ile ortaya çıkmaktadır (Vuković vd., 2025).

İşletmelerdeki finansal hilelerin genellikle dört ana kategoride değerlendirilmesi söz konusu olabilmektedir. İlki gelir Manipülasyonudur. Gelirlerin yanlış beyan edilmesi, öne çekilmesi veya ertelenmesidir. Bu durum, özellikle halka açık şirketlerde yaygın olarak görülmekte ve yatırımcıları yanıltmaya yönelik olarak kullanılmaktadır. İkincisi maliyet ve gider manipülasyonudur. Bu hile şeklinde, giderler gizlenir veya yanlış sınıflandırılmaktadır. Özellikle büyük ölçekli projelerde ve karmaşık muhasebe yapılarında tespit edilmesi zor olan bu hile türü, işletmenin karlılığını olduğundan yüksek göstermek amacıyla kullanılmaktadır. Üçüncüsü ise varlık ve yükümlülük manipülasyonudur. Bu hile şeklinde ise varlıklar şişirilmekte veya yükümlülükler eksik gösterilmektedir. PricewaterhouseCoopers'ın 2022 raporuna göre, dünya çapında şirketlerin %56'sı bir tür hileye maruz kalmıştır. Latin Amerika'da ise şirketlerin %32'si hile sorunu yaşamıştır (Vuković vd., 2025). Bu istatistikler, yapılan araştırma bulgularıyla da örtüşmektedir; ankete katılan yöneticilerin %83'ü son 12 ayda siber saldırılara hedef olduklarını, %71'i ise bir tür iç veya dış hileyle karşılaştıklarını bildirmiştir. Son olarak da para aklama ve güncel hile tekniklerinden bahsedilebilir. Para aklama, yasadışı paranın kökenini gizleyerek yasal görünmesini sağlayan karmaşık bir süreçtir. Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) tahminlerine göre, para aklama dünya ekonomisinin %2,1-4'ünü oluşturmaktadır (Gadimov ve Birihanu, 2025). Bu süreç tipik olarak üç aşamada gerçekleşmektedir. Bu aşamalar; Yerleştirme (Placement): Yasadışı fonların finansal sisteme fiziksel olarak sokulması, Katmanlama (Layering): Paranın izinin karmaştırılması için çoklu finansal işlemler ve Entegrasyon (Integration): Aklanmış fonların yasal ekonomiye geri sokulmasından oluşmaktadır.

Sonuç olarak, işletmelerde hilelerin tespiti, geleneksel denetim yöntemleriyle zor olmaktadır. Bu durum hile yapma iradesini taşıyan kişileri cesaretlendirmektedir. Ancak, yapay zekâ destekli teknolojilerinden yararlanılarak yapılan denetimler, çok daha etkin denetim süreçlerinin gerçekleştirilmesini sağlamaktadır. Bu nedenledir ki, yapay zekanın bu maksatla kullanılması, her geçen gün daha artma potansiyeline sahiptir.

3. İŞLETMELERDE KLASİK YÖNTEMLERLE HİLE TESPİTİ VE ÖNLENMESİ

İşletmelerde hile tespiti ve önlenmesi uzun yıllardır geleneksel denetim yöntemlerine dayanmaktadır. Bu yöntemler, işletmelerin finansal ve operasyonel süreçlerini inceleyerek, olası hileli işlemleri tespit etmeye ve önlemeye yönelik bir dizi teknik ve prosedürü içermektedir. Geleneksel denetim, genellikle iç ve dış denetim süreçleri aracılığıyla gerçekleştirilmektedir.

İç denetim, işletme içindeki çeşitli departmanların ve süreçlerin performansını ve uyumluluğunu değerlendirmek amacıyla yapılan bağımsız bir incelemedir. İç denetim, potansiyel hilelerin tespit edilmesi ve önlenmesi için kritik bir rol oynamaktadır. Denetçiler, muhasebe kayıtları, envanter yönetimi ve nakit akışları gibi alanlarda sistematik incelemeler yaparak, finansal verilerdeki olası anormallikleri ve hileli işlemleri ortaya çıkarmaya çalışmaktadırlar. Bu süreçte, iç denetçilerin bağımsızlığı ve objektifliği büyük önem taşımaktadır (Bhimani vd., 2012).

Dış denetim ise, bağımsız denetim firmaları tarafından yürütülen bir süreç olup, işletmenin finansal tablolarının doğruluğunu ve güvenilirliğini değerlendirmeyi amaçlamaktadır. Bu denetimler, genellikle yasal gereklilikler doğrultusunda yapılır ve işletmenin mali durumunu bağımsız bir perspektiften analiz etmeyi amaçlamaktadır. Dış denetim sürecinde, hileli faaliyetlerin belirlenmesi amacıyla finansal veriler ve belgeler titizlikle incelenir. Ancak, dış denetimin sınırlı bir zaman diliminde gerçekleştiriliyor olması, hileli faaliyetlerin tam olarak tespit edilmesini zorlaştırabilmektedir (Xu vd., 2023).

Geleneksel hile tespiti yöntemleri arasında yer alan bir diğer yaklaşım, kapsamlı kontrol listeleri ve prosedürlerdir. İşletmeler, hile risklerini minimize etmek için belirli görevlerin ayrılması (segregation of duties), yetki sınırlarının belirlenmesi ve onay süreçlerinin düzenlenmesi gibi uygulamaları içermektedir. Örneğin, satın alma işlemleri için onay süreçleri, muhasebe kayıtlarının çift kontrol edilmesi gibi uygulamalar yaygındır. Bu yöntemler, hile risklerini minimize etmek için geliştirilmiştir ve çalışanların yetkilerini kötüye kullanmasını engellemeyi amaçlamaktadır (Benedek vd., 2023).

Klasik hile tespit yöntemlerinden bir diğeri olan analitik incelemeler de finansal verilerin incelenmesinde önemli bir yere sahiptir. Bu yöntem, işletmenin finansal performansının, önceki dönem verileri ve benzer işletmelerle karşılaştırılması yoluyla anormalliklerin tespit edilmesini amaçlamaktadır. Özellikle gelir ve giderlerdeki beklenmedik ani değişiklikler, hesap hataları veya diğer olağandışı işlemler, potansiyel hile belirtileri olarak değerlendirilmektedir (Day ve Schoemaker, 2016).

İşletmelerde hilenin önlenmesi, çalışanları hileye karşı bilinçlendirmek ve eğitmekle de sağlanabilmektedir. Bu yöntem, en etkili yöntemlerden birisidir. Çalışan eğitimleriyle, potansiyel hile türleri, bu hilelerin nasıl tespit edileceği ve şüpheli durumlar karşısında izlenecek prosedürler konusunda bilgilendirilmektedirler. Bu tür eğitimlerle, çalışanların hileli faaliyetlere karşı daha dikkatli olmalarını sağladığı gibi hile yapmaktan kaçınmalarını, diğer çalışanların da hileli faaliyetlerini daha kolay fark edebilmelerini ve de hileye karşı mücadelede proaktif rol almalarını sağlamaktadır (Aziz ve Andriansyah 2023).

4. KLASİK YÖNTEMLERİN DEĞERLENDİRİLMESİ

Klasik yöntemlerin hile tespiti ve önlenmesi konusunda sağladığı fayda ve sakıncalar yer almaktadır. Bu fayda ve sakıncaların ele alınarak incelenmesi, yapay zekâ destekli hile denetimi ve uygulamalarının gelişiminin hangi yöne evrileceğini değerlendirmek açısından bir perspektif yaratacaktır.

Klasik denetim yöntemleri, faydalarının en önemlisi, işletmelerin finansal ve operasyonel süreçlerini düzenli bir şekilde incelemek için sistematik bir yapı sunmasıdır. Bu yapı sayesinde işletmeler, finansal verilerini düzenli olarak kontrol edebilir ve olası hilelerin tespiti için standart prosedürler geliştirebilmektedirler (Bhimani vd., 2012).

Klasik yöntemlerin diğer bir faydası da çoğu yasal düzenleme ve muhasebe standartları ile uyumlu olmasıdır. Bu durum, denetimlerin yasal zorunluluklar çerçevesinde yapılmasını sağlarken, işletmelerin yasal yükümlülüklerini yerine getirmelerine de yardımcı olmaktadır (Xu vd., 2023).

Klasik yöntemler yoğun farkındalık ve eğitim programlarına dayanmaktadır. Çalışan eğitimleri ve bilgilendirme programları, klasik yöntemlerin bir parçası olarak, işletme içindeki hile farkındalığını artırmakta ve hileli faaliyetlerin erken tespitini ve önlenmesi sağlamaktadır (Aziz ve Andriansyah, 2023).

Klasik yöntemlerin sakıncalarına gelince, en başta bu yöntemlerin büyük ölçüde manuel süreçlere dayanması ifade edilebilir. Manuel olarak ortaya konulan çabalar, karmaşık ve sofistike hile tekniklerini tespit etmekte yetersiz kalabilmekte ve uygulanması zaman alıcı ve maliyetli olmaktadır. Ayrıca, denetim süreçlerinin sürekli değil de belirli aralıklarla gerçekleştirilmesi, hileli faaliyetlerin zamanında tespit edilememesine neden olmaktadır. Bu durum, özellikle büyük işletmelerde, denetim süreçlerinin verimliliğini azaltmakta ve hilelerin tespitinde gecikmelere yol açabilmektedir (Benedek vd., 2023). Bu sınırlılıklar, günümüzde yapay zekâ destekli denetim yöntemlerine olan ihtiyacı artırmıştır (Buyuktepe vd.,2023).

Geleneksel yöntemler, genellikle basit ve doğrudan hileleri tespit etmekte etkilidir ve finansal verilerdeki manipölasyonlar, bu yöntemlerle her zaman başarılı bir şekilde ortaya çıkarılamamaktadır (Day ve Schoemaker, 2016). Klasik denetimlerin periyodik olarak yapılması, işletmelerde sürekli bir hile tespit sistemi kurmayı zorlaştırmaktadır. Bu durum, hileli faaliyetlerin denetim dönemleri dışında gerçekleşmesine ve tespit edilmesinde gecikmelere neden olabilmektedir. Süreklilik ve gerçek zamanlı izleme eksikliği, hilecilerin denetim boşluklarından yararlanmalarına olanak tanımaktadır (Buyuktepe vd.,2023).

Klasik yöntemlerle yapılan denetimlerde, yanlış pozitif (hile olarak işaretlenen meşru işlemler) ve yanlış negatif (hileli işlemlerin tespit edilememesi) oranlarının yüksek olması, denetim süreçlerinin etkinliğini zayıflatmaktadır. Bu durum hem gereksiz incelemelere zaman ayrılmasına hem de gerçek hilelerin gözden kaçmasına yol açabilmektedir (Kaggwa vd., 2024). Güncel araştırmalar, geleneksel kural tabanlı anti-para aklama (AML) sistemlerinin %98'in üzerinde yanlış pozitif ürettiğini göstermektedir (Gadimov ve Birihanu, 2025). Bu durum, finansal kurumlar için önemli operasyonel maliyetlere yol açmakta ve gerçek para aklama vakalarının tespit edilememesi ciddi düzenleyici uyumluluk riskleri oluşturmaktadır.

Klasik yöntemler, hızlı teknolojik gelişmelere uyum sağlamakta zorlanmaktadır. Bu, mevcut olan uygulamaları önceleme ve devam etirme güdüsünden öte, etik ve mevzuata dayalı sorunlardan da kaynaklanmaktadır. Diğer yandan klasik yöntemler, büyük veri analitiği, yapay zekâ gibi modern teknolojileri kullanmadığı için, büyük ölçekli ve karmaşık veri setleriyle çalışmakta yetersiz kalabilmektedir (Kaggwa vd., 2024).

5. YAPAY ZEKÂ İLE HİLE ÖNLEME UYGULAMALARININ GETİRDİĞİ YENİLİKLER

İşletmelerdeki hile tespiti ve önlenmesinde yapay zekânın kullanımı, hilenin erken tespit edilerek gerekli tedbirleri alınması suretiyle, işletmelerin hileden kaynaklanan mali kayıpların en aza inmesi sağlanabilmektedir. Son dönemlerde işletmelerde hızla artan yapay zekâ uygulamalarının hile önleme stratejilerine entegrasyonu birlikte finansal hilelerle mücadelede oldukça etkili olduğu kanıtlanmıştır. İşletmeler, biyolojik özellikler ve gelişmiş yapay zekâ algoritmalarının bir kombinasyonunu kullanarak, biyolojik sahtekârlığı (biological fraud) önlemek için anormal işlemleri etkili bir şekilde değerlendirmekte ve sürekli olarak izlemektedirler. Bunu başarmak için işletmelerin etik açıdan, finansal teknolojinin bağımsızlığını ve kontrol edilebilirliğini sağlamalı, bu alandaki yenilik ve araştırmaları

destekleyerek yapay zekâ uygulamalarının yazılım ve donanım ortamı titizlikle takip etmelidir (Day ve Schoemaker,2016).

Yapay zekânın işletmelerdeki varlık ticareti, varlık yönetimi ve bankacılık gibi finansal hizmetlere dâhil edilmesiyle hileli işlemlerin tespiti ve önlenmesinde ciddi mesafeler alınmıştır. Güncel araştırmalar, yapay zekanın finansal hile tespitinde devrim yarattığını ve bankacılık, sigorta ve sağlık sektörleri dahil olmak üzere çeşitli sektörlerde daha doğru, ölçeklenebilir ve uyarlanabilir sistemler sağladığını göstermektedir (Adhikari vd., 2024).

Yapay zekâ ile hileli işlemleri tespit etmek işletmelere önemli katkılar sağlamaktadır. Günümüz işletmelerinin büyük ve karmaşık yapısı, hile yapma potansiyeline sahip klişeleri cesaretlendirmekte ve işletmeler hile yoluyla önemli gelir kaybına uğramaktadırlar. Bu nedenle, işletmelerde hileli işlemlerden kaynaklanan gelir kaybının tespit edilmesi ve önlemlerin alınması giderek daha önemli hale gelmektedir. İşletmeler hile kaynaklı olası zararların önüne geçebilmek için çeşitli hile tespit sistemleri kullanmaktadır. Yapay zekâ uygulamalarında, işletmelerde hileli finansal işlemlerin tespit edilmesine ve engellemesine olanak tanıyan bir dizi süreç ve analiz tanımlanmıştır. Yapay Zekâ uygulamaları, hileli işlemleri tespit etmek, hileli işlemlerle ilgili kalıpları, anormallikleri ve davranışları belirlemek için makine öğrenimi algoritmalarından ve veri analizi tekniklerinden yararlanmaktadır. Böylece büyük veri analizi yaparak milyonlarca finansal işlemi hızlı bir şekilde tarayabilmesi ve potansiyel anormallikleri belirlemesi söz konusu olacaktır. Bunun için kullanıcı davranışlarını sürekli takip ederek, içeriden gelen tehditler ve hileli faaliyetlerin erken aşamada ortaya çıkarılması mümkün olacaktır. Bu tür uygulamalar, tipik bir çalışanın normalden sapma eğilimlerini öğrenerek, anormal durumları belirleyip işletme yetkililerine rapor edebilmektedir (Hernandez Aros vd., 2024).

Yapay zekâ, özellikle büyük veri setlerini analiz etme, anormallikleri tespit etme ve tahminlerde bulunma yetenekleri sayesinde finansal raporlama hilelerinin belirlenmesinde etkili bir araçtır (Day ve Schoemaker,2016). Yapay zekanın bu alanda kullanımına yönelik başlıca yaklaşımlar yer almaktadır. Bu yaklaşımları üç başlık altında toplanabilir:

- **Makine Öğrenimi (Machine Learning):** Makine öğrenimi algoritmaları, geçmiş verileri analiz ederek, finansal raporlardaki olası hileli davranışları belirlemektedir. Bu algoritmalar, özellikle denetim geçmişi olan şirketlerin verilerini kullanarak, hileli ve hilesiz durumları öğrenir ve gelecekteki raporlamalarda anormallikleri tespit edebilir. Güncel literatür incelemesi, denetimli öğrenme yaklaşımlarının finansal hile tespitinde en yaygın kullanılan yöntem olduğunu göstermektedir (Hernandez Aros vd., 2024).

- Doğal Dil İşleme (Natural Language Processing - NLP): NLP, finansal raporlardaki metinleri analiz ederek, tutarsızlıkları ve şüpheli ifadeleri belirlemektedir. Özellikle denetim raporları ve yönetim açıklamaları gibi metinsel verilerde kullanılarak, dolandırıcılık belirtilerini ortaya çıkarabilmektedir.
- Anomali Tespiti: YZ tabanlı anomali tespit sistemleri, finansal verilerdeki alışılmadık ve beklenmedik kalıpları belirlemektedir. Bu sistemler, normal davranıştan sapmaları tespit ederek, olası hileleri işaretlemektedirler. Yapay zekâ sadece hileleri tespit etmenin ötesinde, aynı zamanda önlenmesine de yardımcı olmaktadır.

Derin öğrenme, makine öğreniminin bir dalı olarak, günümüz teknolojik gelişmelerinin ve yeniliklerinin temel teknolojisidir. Derin öğrenme tabanlı yaklaşımlar, kredi kartı işlemleri gibi büyük veri setlerindeki karmaşık kalıpları analiz etmek ve tespit etmek için kullanılan en gelişmiş yöntemlerdir (Mienye ve Jere, 2024). Ancak, literatürdeki çoğu kredi kartı hile modeli geleneksel makine öğrenimi algoritmalarına dayanmaktadır ve son zamanlarda derin öğrenme tekniklerinin bu alanda artan kullanımı gözlenmektedir.

Kredi kartı işlemlerindeki hızlı teknolojik gelişmeler ve elektronik hizmetlerin kolaylığı nedeniyle kredi kartı işlemleri artmıştır (Mienye ve Jere, 2024). Buna bağlı olarak hem finansal kurumlar hem de müşteriler için önemli bir endişe haline gelen kredi kartı hileleri gibi güvenlik sorunlarında da artış yaşanmıştır. Nielsen raporuna göre, 2019, 2020 ve 2021 yıllarında kredi kartı hilelerinden kaynaklanan kayıplar sırasıyla yaklaşık 28.65, 28.50 ve 32,34 milyar dolar olmuştur (Mienye ve Jere, 2024). Küresel olarak kredi kartı hile kayıpları son on yılda üç katına çıkmış, 2011'de 9,84 milyar dolardan 2021'de 32,34 milyar dolara yükselmiştir. Bu dramatik artış, daha sofistike ve etkili hile tespit yöntemlerine olan ihtiyacı vurgulamaktadır. Derin Öğrenme Mimarileri bu maksatla kullanılan ve önemli fırsatlar sunan derin öğrenme tabanlı yapılardır. Bu yapıları ele üç farklı şekilde inceleyebiliriz.

Tekrarlayan Sinir Ağları (RNN) ve Varyantları: RNN ve varyantları olan LSTM (Long Short-Term Memory) ve GRU (Gated Recurrent Unit), sıralı verileri öğrenme ve zamansal ilişkileri tespit etme yetenekleri nedeniyle kredi kartı işlemlerini modelleme ve analiz etmek için en yaygın kullanılan derin öğrenme tabanlı ağlardır (Mienye ve Jere, 2024).

LSTM ağı, bir dizideki uzun vadeli bağımlılıkları öğrenmek için kullanışlıdır. Önceki zaman adımlarından gelen bilgileri hatırlayabilmesi ve yeni girdiler işlenirken bu bilgileri seçici olarak unutulabilmesi veya güncelleyebilmesi nedeniyle güçlüdür. LSTM gibi GRU da kapılama mekanizması sayesinde önceki zaman adımlarından gelen verileri seçici olarak güncelleyebilir

veya unutulabilir, bu da onu zaman serisi modellemesi için uygun hale getirmektedir (Mienye ve Jere, 2024).

Konvolüsyonel Sinir Ağları (CNN): CNN'ler, özellikle görüntü işleme alanında başarılı olmalarına rağmen, finansal veri analizinde de etkili sonuçlar vermektedir. Finansal işlem verilerinin görsel temsillerini analiz ederek, gizli kalıpları ve anormallikleri tespit edebilmektedir.

Transformer Modelleri: Son yıllarda, doğal dil işleme alanında devrim yaratan Transformer mimarileri, finansal hile tespitinde de umut verici sonuçlar göstermektedir. Bu modeller, uzun mesafeli bağımlılıkları yakalama konusunda üstün performans sergilemektedir.

Güncel araştırmalar, gerçek zamanlı şüpheli işlem tespiti için gelişmiş çerçeveler önermektedir. Bu sistemler, finansal kurumların para aklama ve finansal suçlarla etkili bir şekilde mücadele etmesini sağlamaktadır. Önerilen modeller iki temel yaklaşım içermektedir: iliki, Docker konteyner tabanlı dağıtık bilişim mimarisi, esneklik, taşınabilirlik yetenekleri ve özelleştirmeyi artırmak için kullanılmaktadır. İkincisi ise, Autoencoder Yöntemidir. Bu yöntem, şüpheli tespit modülü, autoencoder yöntemini kullanarak sistemde herhangi bir şüpheli aktivite olup olmadığını belirlemek için yeniden yapılandırma hatasını (reconstruction error) kullanmaktadır (Gadimov ve Birihanu, 2025).

Derin öğrenme modellerinin performansını değerlendirmek için çeşitli metrikler kullanılmaktadır. Güncel literatür incelemesi, en yaygın kullanılan performans metriklerinin Accuracy (Doğruluk), Precision (Kesinlik), F1 Score, Recall (Duyarlılık) ve AUC-ROC olduğunu göstermektedir (Hernandez Aros vd., 2024; Chen vd., 2025).

Bu metriklerin her biri, farklı açılardan model performansını değerlendirmekte ve özellikle dengesiz veri setlerinde (imbalanced datasets) kritik önem taşımaktadır. Finansal hile tespitinde, hileli işlemlerin toplam işlemlere oranının çok düşük olması nedeniyle dengesiz veri setleri yaygın bir sorundur.

6. YAPAY ZEKÂ DESTEKLİ HİLE TESPİTİNDE GÜNCEL TRENTLER, GELİŞMELER KAPSAMINDA FAYDA, YAŞANAN ZORLUK VE SINIRLILIKLAR

Geleneksel hileli işlemlerin tespiti ve önlenmesi yöntemleri, karmaşık ve hızla gelişen hırsızlık planlarının belirlenmesinde ve azaltılmasında genellikle yetersiz kalmaktadır. Yapay zekâ, analistlere göre gerçek zamanlı içgörülere erişim sağlayarak dönüştürücü bir fırsat sunmaktadır. Geleneksel hile tespit süreçleri, genellikle veri işleme ve analizinde gecikmeler

hile önleme kararlarının alınma hızını bir hayli yavaşlatmaktadır (Bhimani vd.,2012). Yapay zekâ hile tespitinin doğruluğunu ve verimliliğini artırmak için sahip olduğu teknolojik üstünlük nedeniyle geleneksel yöntemlerden farklılık gösterir. Bu nedenle yapay zekânın, günümüzde hileli işlemlerle mücadelede güçlü bir araç olarak ortaya çıktığı aşikardır. Yapay zekânın, veri analizi ve örüntü tanıma yeteneklerinin her geçen gün gelişmesi, hile önemli fırsatlar sunmaktadır. Ancak, başarılı uygulama, bu teknolojiyle ilgili doğal zorlukların var olduğunun net bir şekilde anlaşılmasını gerektirir (Gaikwad,2020).

Yapay zekâ, özellikle makine öğrenimi, hile tespiti ve önlenmesi için dönüştürücü bir yaklaşım sunmaktadır. Yapay zekâ bir işletmede gerçekleştirilen işlemlerin geçmişini ve cihaz bilgilerini kapsayan geniş veri kümelerini analiz ederek, insan analistlerin gözlerinden kaçabilecek karmaşık kalıpları ve anormallikleri belirleyebilir (Kaggwa vd.,2024). Bu işlemler işletmelere şunları yapabilme yeteneği kazandırır:

Veri Analizi ve Örüntü Tanıma ile Hileli Davranış risklerini azaltır. Yapay zekâ sistemleri, özellikle makine öğrenimi algoritmalarını kullanarak büyük veri kümelerini insanlardan çok daha hızlı işleme konusunda uzmandır. Yapay zekanın örüntü tanıma yetenekleri dolandırıcılık tespitinde çok önemli bir rol oynamaktadır. Makine öğrenimi algoritmaları, dolandırıcılık faaliyetleriyle ilişkili düzensizlikleri veya kalıpları belirlemek için geçmiş verilerden öğrenebilir. Bu proaktif yaklaşım, kuruluşların önleyici tedbirler uygulamasına ve iç kontrollerini güçlendirmesine olanak tanır. Yapay zekâ, örüntü tanımadan yararlanarak daha sağlam ve dirençli bir finansal ekosisteme katkıda bulunur ve hileli davranışlarla ilişkili riskleri en aza indirir (Hassan vd., 2023).

Yapay Zekâ uygulamaları, hileyi tespitte yüksek doğruluk sağlamaktadır. Yapay zekâ algoritmaları, işlem geçmişini, coğrafi konum verilerini ve cihaz bilgilerini kapsayan geniş veri kümelerini analiz ederek belirlenmiş temel çizgilerden ince sapmaları tanımlamada mükemmeldir. Yapay zekâ destekli sistemler, hileli faaliyetleri daha büyük bir hassasiyetle tespit edilmesini sağlamaktadır. Bu ise hileli işlemlerden dolayı olası mali kayıplarda önemli bir azalmaya neden olmaktadır (Longbing,2021).

Yapay zekâ uygulamalarının hile denetimi süreçlerinde yarattığı en önemli sonuçlardan biri de operasyonel maliyetleri azaltmasıdır. Yapay zekâ, hileli işlemlerin tespitini otomatikleştirerek, manuel incelemeler ve soruşturmalara ilişkili operasyonel maliyetlerin azaltılmasına neden olurken işletme kaynaklarının daha verimli bir şekilde kullanılmasına olanak tanımaktadır. Bu kaynaklar daha sonra insan müdahalesi gerektiren diğer karmaşık görevler için kullanılabilir.

Yapay zekâ, işlemlerin gerçek zamanlı olarak izlemesine ve müdahale edilmesine olanak sağlamaktadır. Yapay zekâ ile gerçek zamanlı işlemleri izleme ve veri işleme sayesinde verileri sınıflandırmak, depolamak ve görselleştirmek daha kolay hale gelmektedir. Aynı zamanda anlık veri işleme, aykırı değerlerin ve veri anormalliklerinin anında düzeltici eylem için işaretlenmesine yardımcı olarak dolandırıcılık tespitini ve çözümünü hızlandırmaktadır. Bu proaktif yaklaşım, hileli işlemlerin tamamlanmasını önleyerek mali kayıpları önemli ölçüde en aza indirmektedir (Longbing,2021).

Yapay zekâ anormallikleri tespit ederek, hile denetimini kolaylaştırmaktadır. Yapay zekâ sistemleri, işletmelerdeki verilerin çoğunluğundan önemli ölçüde farklılık göstererek şüphe uyandıran veri noktalarını, olayları veya gözlemleri tanımlamayı içeren anormallikleri anında tespit etmektedir. Bu nedenle yapay zekâ algoritmaları, işletmelerdeki bir veri kümesinde normal davranışın nasıl olması gerektiği ve bu normdan önemli ölçüde sapan aykırı değerleri veya anormallikleri belirlemek için eğitilmektedirler. Hileli işlemler genellikle aykırı değerler veya işlem verilerinde anormallikler olarak ortaya çıktığından, anormallik tespiti hile tespitinde temel öneme sahiptir.

Yapay zekanın bir diğer yarattığı fayda ise; hileli işlemlerle ilgili tahminlerde bulunmayı sağlamasıdır. Tahmine dayalı analitik, işletmede gerçekleşen geçmiş verileri kullanarak gelecekteki olası hileli işlemlerle ilgili tahminlerde bulunmaya dönük bir yaklaşımdır. Diğer bir ifadeyle yapay zekâ modelleri işletmelerdeki hile işlemlerin tespitinde, gelecekteki bir işlemin hileli olma olasılığını tahmin etmek için geçmişteki hile amaçlı olan ve olmayan işlemlerin veri kümeleri üzerinde eğitilmektedir (Kaggwa vd.,2024). Bu da hilenin önceden tespit edilmesi ve sonrasında bu işlemlerin durdurularak maddi kayıpların en aza indirilmesinde yardımcı olacaktır. Bu maksatla, hile tespitinde; lojistik regresyon, karar ağaçları, rastgele ormanlar ve gradyan artırma makineleri gibi teknikler yaygın olarak kullanılmaktadır. Tahmine dayalı analitik uygulamalar, müşteri davranışları, pazar eğilimleri ve ortaya çıkan fırsatlar hakkında işletmelere içgörü kazanabilmektedir. Yapay zekanın bu stratejik kullanımı iş genişletme, ürün geliştirme veya pazara giriş gibi bilinçli önerilerde bulunmasını sağlamaktadır. İşletmeler, yapay zekâ tarafından üretilen içgörülerden yararlanarak kendilerini pazar trendlerinden yararlanmak ve sürdürülebilir büyümeyi sağlamak için konumlandırabilmektedir (Uwaoma vd.,2024).

Yapay zekâ, hile denetiminde uyarlanabilirlik ve ölçeklenebilirlik sağlamaktadır. İşletmelerde gerçekleşen tüm hileli faaliyetler mali kayıplara neden olduğu gibi itibarına da zarar verir. İşletmelerde kullanılan genellikle kural tabanlı ve statik olan geleneksel hile tespit yöntemleri, dolandırıcıların giderek daha sofistike hale gelen taktiklerine ayak uydurmakta

zorlanmaktadır. Çok katmanlı sinir ağlarını içeren makine öğreniminin bir alt kümesi olan derin öğrenme ise, karmaşık hile şekillerini önceden tespit etmede özellikle ustadır. Konvolüsyonel sinir ağları ve tekrarlayan sinir ağları, geleneksel tespit yöntemleri tarafından görülmeyen hileli işlemleri belirlemek için sırasıyla görüntüler ve sıralı veriler gibi yapılandırılmamış verileri işlemektedir (Dileep,2023).

Yapay zekâ modelleri doğası gereği statik kuralların aksine dinamiktir. Yapay zekâ, yeni tür hile faaliyetleri ve taktikleriyle karşılaştıkça bu deneyimlerden öğrenerek modellerini bu yeni gelişmelere göre adapte eder, böylece yeni dolandırıcılık taktikleri ortaya çıktıkça bunları anında belirlemektedir. Bu uyarlanabilirlik, dolandırıcılar yeni planlar geliştirdikçe yapay zekâ sistemleri de tespit yöntemlerini proaktif bir şekilde ayarlayarak dolandırıcılardan bir adım önde kalmalarını sağlamaktadır(Dileep,2023). Aynı zamanda yapay zekâ sistemleri, büyük veri kümelerini yönetecek şekilde zahmetsizce ölçeklenebilir; bu da onları yüksek hacimli işlemleri işleyen büyük kuruluşlar için ideal kılmaktadır (Longbing,2021).

Yapay zekâ hile denetiminde hız ve verimlilik sağlamaktadır. Yapay zekâ destekli hile tespit sistemleri 7/24 çalışarak işlemleri ve etkinlikleri gerçek zamanlı olarak analiz etmektedir. Bu yetenek, hileli işlemleri tespit etmek ve bunlara yanıt vermek için gereken süreyi önemli ölçüde azaltarak potansiyel kayıpları en aza indirmektedir. Aynı zamanda yapay zekâ, insan kaynaklarında orantısız bir artışa gerek kalmadan hilenin tespit süreçlerinin verimliliğini artırarak çok büyük miktarda veri ve işlemi yönetebilmektedir.

Yapay zekâ destekli hile denetimi, yanlış pozitiflerin azaltılmasını sağlamaktadır. Yanlış-pozitif (false-positive) kavramı bir hesaplama, saptama veya algılama hatasıdır. Yanlış-pozitif bir durum meydana geldiğinde gerçek bir işlem, yanlış alarm verilerek şüpheli olarak tanımlanmaktadır. Hileli işlemleri tespit ederken bir işlemin gerçek mi yoksa şüpheli mi olduğuna karar vermek, analistler için büyük bir zaman kaybına neden olur. Geleneksel yöntemlerde yanlış-pozitifler ihtimali, işletmelerdeki işlem sayısının çok fazla olmasından dolayı zaman kaybına neden olmakta ve gerçek hileli işlemlerin tespit edilme hızını yavaşlatmaktadır.

Yapay zekâ makine öğrenmesi modelleri kullanılarak hileyi tespit edip hızlı önlem alarak mali kayıpları en aza indirir. Ancak hile tespit programlarında çok sayıda kuralın kullanılması, yüksek sayıda yanlış-pozitif sonuç vermesine neden olabilmektedir. Böylece birçok gerçek mali işlemlerin hile şüphesiyle engellenebileceği anlamına gelmektedir. Bu durumda normal bir işlem hileli işlem olarak nitelendirilebilir ve incelendiğinde herhangi bir

hilenin olmadığı ortaya çıktığında, bunu tespit etmek hile analistlerinin harcadıkları süre gereksiz zaman kaybıdır.

6.1. Hile Tespitinde Yapay Zekâ Kullanımının Zorlukları ve Sınırlılıkları

Yapay zekâ işletmelere muazzam fırsatlar sunarken, başarılı bir uygulama için birtakım zorlukları ve sınırlılıkları da beraberinde ortaya çıkarır. Bu zorlukların bilincinde olmak, yapay zekaya dayalı hile denetimi uygulamalarının kullanım etkinliğinin artırılmasında önemli katkı sağlar.

Yapay zekâ uygulamalarının finansal hile tespitindeki en önemli zorluklarından biri veri kalitesidir. Etik kaygılar, algoritmik önyargı, veri gizliliği sorunları ve sistem güvenlik açıkları gibi zorluklar yaygın benimsemeyi engellemektedir (Adhikari vd., 2024). Küçük organizasyonlarda ölçeklenebilirlik sorunları, AI'nın potansiyelinden tam olarak yararlanmayı engellemektedir. Bir işletmede, hileli işlemlerle karşılaşıldığında, hile tespitindeki önyargılı veya dengesiz veri kümeleri, belirli dolandırıcılık türlerini tespit etmekte başarısız olmasına neden olmaktadır (Tewari, 2023). Finansal hile tespitinde en yaygın karşılaşılan teknik zorluklardan biri dengesiz veri setleridir. Hileli işlemlerin toplam işlemlere oranının çok düşük olması (%1'den az), geleneksel makine öğrenimi algoritmalarının performansını olumsuz etkilemektedir. Bu durum, özellikle yanlış negatif oranlarının yüksek olmasına ve gerçek hilelerin gözden kaçmasına neden olmaktadır.

Gelişen Dolandırıcılık Taktiklerine Adapte Olmak, işletmeler açısından zorluklar barındırmaktadır. Günümüzün devrim niteliğindeki teknolojisi olan yapay zekayı dolandırıcılık tespitinde kullanan işletmeler, dolandırıcılığın tespitinde kullanılan geleneksel yöntemlere göre daha iyi sonuçlar elde etmektedirler. Yapay zekâ programları sayesinde işletmelerin farklı durum ve teknolojilere uyum sağlaması, yeni yöntem ve teknolojiler geliştiren dolandırıcılarla mücadele etmesi önemlidir. İşletmeler yapay zekâ ile her gün gerçekleşen milyonlarca hesap işlemi izleyerek olası hileli işlemlere karşı gerekli tüm aksiyonları alabilmektedirler.

Yapay zekâ, zamanla işletmenin belirlediği özel kurallar çerçevesinde çalışarak kontrol edilmesi gereken beklenmedik hareketleri de tespit edebilmektedir. Bu nedenle dolandırıcılar, tespit edilmekten kaçınmak için yaratıcı olmaya ve yeni teknikler geliştirmeye çalışırlar. Yapay zekâ destekli hileli işlemleri tespit araçları, işletmelerin dolandırıcılık grafiği, skorlama ve gelişmiş filtreleme gibi bazı önlemleri almalarını da kolaylaştırmaktadır. Yapay zekâ, şüpheli işlemleri izlerken aynı zamanda şüpheli işlemleri aynı anda gerçekleşen diğer işlemlerle karşılaştırarak yeni dolandırıcılık planlarını da tespit edebilmektedir. Yapay zekâ, keşfettiği

yeni dolandırıcılık tekniklerini dolandırıcılık tespit programlarına kolaylıkla dahil edebilmekte ve bunları bir strateji olarak kullanabilmektedir (Sukanya ve David, 2021). Ancak, yapay zekâ uygulamalarının güncel ve gelişen dolandırıcılık faaliyetlerinde etkin olarak kullanılmasını sağlayacak şekilde yeni gelişen durumlara uyarlamak gerekir. Yapay zekâ modellerinin, adaptasyonu işletmeler için zorlayıcı bir durumdur.

Hem yanlış pozitifleri (sahtekârlık olarak işaretlenen meşru işlemler) hem de yanlış negatifleri (sahtekârlık işlemlerinin tespit edilmemesi) en aza indirmek için yapay zekâ modellerinin hassasiyetini dengelemek, işletmeler açısından önemli bir zorluktur. Her ikisinin de yüksek oranlarda olması dolandırıcılık tespit sistemlerinin etkinliğini zayıflatan bir durumdur (Longbing, 2021).

Yapay zekanın model açıklanabilirliği ve şeffaflığı yeterli olmayabilir. Yapay zekâ modellerinin karmaşıklığı, özellikle de derin öğrenme algoritmaları, karar verme süreçlerini anlaşılabilir hale getirebilir. Bu açıklanabilirlik eksikliği, insan gözetimini engeller ve bir işlemin neden hileli olarak işaretlendiğini anlamayı zorlaştırabilir.

Şeffaflık, insan gözetimi ve yanlış pozitiflerin en aza indirilmesi için çok önemlidir. Kararlarının arkasında net gerekçeler sağlayan daha şeffaf yapay zekâ modelleri geliştirmeye yönelik araştırmalar, güveni artırmak ve hileli işlemlerin tespitinde yapay zekânın sorumlu bir şekilde kullanılmasını sağlamak için çok önemlidir. İşletmeler, yorumlanabilir yapay zekâ modellerini uygulamaya öncelik vermeli veya model kararlarını açıklamak için mekanizmalar geliştirmelidir.

İşletmelerdeki verilerin ve işlem hacimlerinin büyümesine göre ölçeklenebilen ve aynı zamanda mevcut sistem ve süreçlerle sorunsuz bir şekilde entegre olabilen yapay zekâ çözümlerinin uygulanması, teknik ve operasyonel açıdan zor bir durumdur.

Veri gizliliğini, tüketicinin korunmasını ve yapay zekâ etiği ile ilgili düzenlemeler sürekli olarak gelişmektedir. Dolandırıcılık tespiti için yapay zekâdan yararlanırken uyumluluğun sağlanması dikkatli planlama ve yürütme gerektirir. İşletmeler, yasal sonuçlardan kaçınmak için yapay zekâ destekli dolandırıcılık tespit sistemlerinin bu düzenlemelere uygun olmasını sağlamalıdır. Gelişen veri gizliliği düzenlemelerine uyumu sağlamak için hukuk ve uyumluluk ekipleriyle yakın iş birliği şarttır.

Düzenleyiciler, karmaşık AI sistemlerinin altında yatan mekanizmaları anlamakta önemli zorluklarla karşılaşmakta ve bu durum etkili gözetim oluşturma çabalarını karmaşıktırmaktadır (Vuković vd., 2025). Benzer şekilde, tüketiciler karar verme süreçlerinde AI tarafından üretilen çıktıların arkasındaki mantığı çözmekte zorlanmaktadır.

Bu zorluklar, AI modellerinde şeffaflığı ve yorumlanabilirliği önceliklendiren Açıklanabilir Yapay Zekâ (XAI) kavramının ortaya çıkmasına yol açmıştır. AI teknolojisindeki hızlı gelişim hızı, düzenleyici çerçevelerin sürekli güncellenmesi gerektiği anlamına gelmekte ve bu durum düzenleyici kurumlara önemli maliyetler yüklemektedir.

Yapay zekâ destekli hileli işlemlerin tespitindeki veri kalitesi, uyarlanabilirlik ve mevzuata uygunluk gibi zorluklarla karşılaşılması olasıdır, ancak bu zorluklar aşılamaz değildir. Yapay zekanın geliştirilmiş hileli işlemleri tespit yetenekleri ve maliyet azaltma gibi sunduğu fırsatlar, dolandırıcılığı önleme stratejilerini dönüştürme potansiyelini ifade etmektedir. Bu zorluklarla başarılı bir şekilde başa çıkmak, veri kalitesine yatırım yapmayı, model açıklanabilirliğine odaklanmayı ve düzenleyici değişikliklere ayak uydurmayı içeren düşünceli bir yaklaşımı gerektirirken, tüm bunları sahtekârlıkla etkili bir şekilde mücadele etmek için yapay zekânın benzersiz güçlü yönlerinden yararlanmayı gerektirir.

7. SONUÇ

Bu çalışma, işletmelerde hile tespiti ve önlenmesi süreçlerinde yapay zekâ uygulamalarının rolünü kapsamlı bir şekilde incelemiş ve güncel literatür bulgularını entegre ederek bu alandaki gelişmeleri değerlendirmiştir. Araştırma sonuçları, yapay zekâ teknolojilerinin finansal hile tespitinde devrim niteliğinde değişiklikler yarattığını ve geleneksel yöntemlere kıyasla önemli avantajlar sağladığını göstermektedir.

Teknolojik Dönüşüme maksadıyla, finansal kurumların yapay zekâ harcamalarının 2027 yılına kadar 97 milyar dolara çıkması beklenmekte ve finansal sektör %29,6'lık oranla yapay zekâ yatırımında en hızlı büyüyen sektör konumundadır (Vuković vd., 2025). Bu exponansiyel büyüme, teknolojinin dönüştürücü potansiyelini açıkça ortaya koymaktadır.

Derin öğrenme teknikleri, özellikle LSTM, GRU ve CNN mimarileri, geleneksel kural tabanlı sistemlere kıyasla gerçek zamanlı hile tespitini ve gelişen hile kalıplarına uyarlanabilirliğini önemli ölçüde iyileştirmekte ve önemli ölçüde performans üstünlüğü sağlamaktadır (Adhikari vd., 2024; Mienye ve Jere, 2024). Kredi kartı hile kayıplarının son on yılda üç katına çıkması (2011: 9,84 milyar dolar, 2021: 32,34 milyar dolar) bu teknolojilere olan ihtiyacı daha da artırmaktadır.

Autoencoder yöntemi ve Docker konteyner tabanlı dağıtık bilişim mimarisi kullanılarak geliştirilen gerçek zamanlı tespit sistemleri, finansal kurumların para aklama ve finansal suçlarla etkili mücadele etmesini sağlamaktadır (Gadimov ve Birihanu, 2025). Bu sistemler,

yeniden yapılandırma hatası (reconstruction error) kullanarak şüpheli aktiviteleri başarıyla tespit edebilmektedir.

Klasik denetim yöntemlerinin %98'in üzerinde yanlış pozitif üretmesi (Gadimov ve Birihanu, 2025), manuel süreçlere dayalı olması ve periyodik denetim yapısı gibi sınırlılıkları, yapay zekâ destekli sistemlerin üstünlüğünü açıkça ortaya koymaktadır. Yapay zekâ sistemleri büyük veri setlerini gerçek zamanlı analiz edebilme, karmaşık kalıpları ve anormallikleri tespit etme, sürekli öğrenme ve adaptasyon kapasitesi ve düşük yanlış pozitif oranları gibi avantajlar sağlamaktadır.

Hibrit yaklaşım benimsenmesi bu alanda yürütülecek çalışmalara önemi üstünlükler sağlamaktadır. İşletmelerin, klasik denetim yöntemlerini tamamen terk etmek yerine, bunları yapay zekâ teknolojileri ile entegre eden hibrit bir yaklaşım benimsemeleri önemlidir. Bu yaklaşım hem insan uzmanlığından hem de teknolojik yeteneklerden maksimum fayda sağlayacaktır. Özellikle küçük ve orta ölçekli işletmeler için, yapay zekâ sistemlerinin aşamalı olarak uygulanmalıdır. İlk aşamada basit anomali tespit sistemleri ile başlanarak, zamanla daha karmaşık derin öğrenme modelleri entegre edilebilir.

Veri Kalitesi ve Yönetimi uygulamalardan elde edilecek sonuçların doğruluğu açısından önemlidir. Yapay zekâ sistemlerinin başarısı büyük ölçüde veri kalitesine bağlı olduğundan, işletmelerin veri toplama, temizleme ve yönetim süreçlerine özel önem vermeleri gerekmektedir.

Düzenleyici otoritelerin, finansal hizmetlerde kullanılan yapay zekâ sistemleri için açıklanabilirlik standartları geliştirmesi önerilmektedir. Bu standartlar hem şeffaflığı artıracak hem de hesap verebilirliği sağlayacaktır.

Finansal suçların küresel doğası göz önüne alındığında, yapay zekâ tabanlı hile tespit sistemleri için uluslararası standartların geliştirilmesi ve koordinasyonun artırılması gerekmektedir.

Sonuç olarak; finansal hilelerin tespit ve önlenmesinde yapay zekâ uygulamaları, işletmeler için kritik bir rekabet avantajı haline gelmiştir. Geleneksel yöntemlerin sınırlılıklarını aşan bu teknolojiler, gerçek zamanlı tespit, yüksek doğruluk oranları ve sürekli öğrenme kapasitesi ile finansal güvenliği yeni bir seviyeye taşımaktadır. Ancak, bu teknolojilerin başarılı uygulanması için veri kalitesi, model açıklanabilirliği, etik kullanım ve düzenleyici uyumluluk gibi konulara özel dikkat gösterilmelidir. İşletmelerin, teknolojik yenilikleri benimserken insan faktörünü de göz ardı etmemeleri ve hibrit yaklaşımlar geliştirmeleri önemlidir.

Gelecekte, yapay zekâ teknolojilerinin daha da gelişmesi ve yaygınlaşması ile birlikte, finansal hile tespiti alanında daha etkili, verimli ve güvenilir sistemlerin ortaya çıkması beklenmektedir. Bu süreçte, akademik araştırmalar, endüstriyel uygulamalar ve düzenleyici çerçevelerin uyumlu bir şekilde geliştirilmesi, sürdürülebilir ve sorumlu bir dijital dönüşümün anahtarı olacaktır.

Gelecek bu konuya yönelik yapılacak çalışmalarda, Veri gizliliğini koruyarak çoklu kurumlar arası iş birliğini sağlayan federatif öğrenme (federated learning) yaklaşımlarının finansal hile tespitindeki potansiyeli araştırılmalıdır. Bunun yanında, Sürekli öğrenen ve kendini güncelleyen adaptif hile tespit sistemlerinin geliştirilmesi önemli bir araştırma alanıdır.

YAZARLARIN KATKISI

Bu çalışmanın giriş ve sonuç kısmı Ahmet ERKASAP, ikinci, üçüncü ve dördüncü kısmı Mehmet Erkan, beşinci ve altıncı kısmı İsmail Özdemir tarafından yapılmıştır.

ÇIKAR ÇATIŞMASI BEYANI

Herhangi bir kurum, kuruluş, kişi ile mali çıkar çatışması yoktur ve yazarlar arasında çıkar çatışması bulunmamaktadır.

KAYNAKÇA

- Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*, 13(01), 1457–1472. <https://doi.org/10.30574/ijsra.2024.13.1.1860>
- Adeyelu, O., Ugochukwu, C., & Shonibare, M. (2024). The impact of artificial intelligence on accounting practices: Advancements, challenges, and opportunities. *International Journal of Management & Entrepreneurship Research*, 6, 1200–1210. <https://doi.org/10.51594/ijmer.v6i4.1031>
- Aziz, L., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132. Retrieved from https://www.researchgate.net/publication/373489510_The_Role_Artificial_Intelligence_in_Modern_Banking_An_Exploration_of_AI-Driven_Approaches_for_Enhanced_Fraud_Prevention_Risk_Management_and_Regulatory_Compliance
- Benedek, B., & Balint, Z. N. (2023). Traditional versus AI-based fraud detection: Cost efficiency in the field of automobile insurance. *Financial and Economic Review*, 22(2), 77–98. <https://doi.org/10.33893/fer.22.2.77>
- Bhimani, A., Horngren, C., Foster, G., & Datar, S. (2012). *Management and cost accounting* (6th ed.). Financial Times Prentice Hall. Retrieved from https://opac.atmaluhur.ac.id/uploaded_files/temporary/DigitalCollection/YWRjNmRIZmFiZjgxMzZiMzUzZDM1M2I4MmQ3ZGNmZjNIM2U2YmI2MQ==.pdf
- Bi-Cun, X., Yaonan, W., Xiuwu, L., & Kaidong, W. (2023). Efficient fraud detection using deep boosting decision trees. *arXiv preprint arXiv:2302.05918*. <https://doi.org/10.48550/arXiv.2302.05918>
- Botond, B., & Zsolt, N. (2023). Traditional versus AI-based fraud detection: Cost efficiency in the field of automobile insurance. *Financial and Economic Review*, 22(2), 77–98. <https://doi.org/10.33893/fer.22.2.77>
- Buyuktepe, O., Catal, C., Kar, G. B., Yamine, M., Hans, & Gavai, A. (2023). Food fraud detection using explainable artificial intelligence. *Expert Systems*. <https://doi.org/10.1111/exsy.13387>
- Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. *arXiv preprint arXiv:2502.00201*. <https://arxiv.org/html/2502.00201v1>
- Cagatay, C., Gorkem, K., Yamine, B., & Anand, G. (2023). Food fraud detection using explainable artificial intelligence. *Expert Systems*. <https://doi.org/10.1111/exsy.13387>

- Day, G. S., & Schoemaker, P. (2016). Adapting to fast-changing markets and technologies. *California Management Review*, 58(4), 59–77. <https://doi.org/10.1525/cmr.2016.58.4.59>
- Dileep, A. K., Amma, K. S., Gujja, S., Ganesh, D., & Hariharan, S. (2023). Financial fraud detection using deep learning techniques. In 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1–6). <https://doi.org/10.1109/ICDCECE57866.2023.10150467>
- Farman, M., & Abbas, A. (2023). Artificial intelligence for fraud detection and prevention. Retrieved from https://www.researchgate.net/publication/375671860_Artificial_Intelligence_for_fraud_detection_and_prevention
- Formica AI. (2021, July 13). Yapay zeka ile dolandırıcılık tespitinde 4 önemli fayda. LinkedIn. Retrieved from <https://www.linkedin.com/pulse/yapay-zeka-ile-doland%C4%B1r%C4%B1c%C4%B1l%C4%B1k-tespitinde-4-%C3%B6nemli-fayda-/?originalSubdomain=tr>
- Gadimov, E., & Birihanu, E. (2025). Real-time suspicious detection framework for financial data streams. *International Journal of Information Technology*. <https://doi.org/10.1007/s41870-025-02529-6>
- Gaikwad, S. (2020). AI in fraud detection: Benefits, challenges and uses. GetApp UK.
- Ginni, A., & Ruchika, B. (2023). Detection and analysis of fraud phone calls using artificial intelligence. In REEDCON (pp. 592–595). <https://doi.org/10.1109/REEDCON57544.2023.10150631>
- Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132.
- Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodriguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, Article 1130. <https://doi.org/10.1057/s41599-024-03606-0>
- Kaggwa, S., Eleogu, T., Okonkwo, F., Farayola, O., Uwaoma, P., & Akinoso, A. (2024). AI in decision making: Transforming business strategies. *International Journal of Research and Scientific Innovation*, 10(12), 423–444. <https://doi.org/10.51244/IJRSI.2023.1012032>
- Longbing, C. (2021). AI in finance: Challenges, techniques and opportunities. arXiv preprint arXiv:2107.09051. <https://doi.org/10.48550/arXiv.2107.09051>
- Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*, 12. <https://doi.org/10.1109/ACCESS.2024.3424170>

- Ruhanen, S. (2023). Contemporary advancements in financial technology and adoption (Bachelor's thesis, University of Twente). Retrieved from https://essay.utwente.nl/95295/1/Ruhanen_BA_BMS.pdf
- Sukanya, A., & David, J. (2021, June 22). AI in fraud detection: Benefits, challenges and uses. GetApp UK.
- Tewari, N. (2023). Artificial intelligence in finance and industry: Opportunities and challenges. In *Decision Strategies and Artificial Intelligence Navigating the Business Landscape*. <https://doi.org/10.59646/edbookc5/009>
- Uwaoma, P. U., Eleogu, T. F., Okonkwo, F., Farayola, O. A., Kaggwa, S., & Akinoso, A. (2024). AI's role in sustainable business practices and environmental management. *International Journal of Research and Scientific Innovation*, 10(12), 359–379.
- Xu, B., Wang, Y., Liao, X., & Wang, K. (2023). Efficient fraud detection using deep boosting decision trees. arXiv preprint [arXiv:2302.05918](https://doi.org/10.48550/arXiv.2302.05918). <https://doi.org/10.48550/arXiv.2302.05918>
- Yusuf, I., İlker, K., & Jale, S. (2023). Detection of fraudulent transactions using artificial neural networks and decision tree methods. *Business and Management Studies: An International Journal*, 11(2), 451–467. <https://doi.org/10.15295/bmij.v11i2.2200>
- Vuković, D. B., Dekpo-Adza, S., & Matović, S. (2025). AI integration in financial services: A systematic review of trends and regulatory challenges. *Humanities and Social Sciences Communications*, 12, Article 562. <https://doi.org/10.1057/s41599-025-04850-8>