İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

İstanbul Commerce University Journal of Science

http://dergipark.org.tr/ticaretfbd

Derleme Makale / Review Article

İŞLETMELER ARASI HETEROJEN VERİLERİN GİZLİLİĞİNİ KORUMAYA YÖNELİK ÖĞRENME MODEL ÇERÇEVESİ

A LEARNING MODEL FRAMEWORK FOR PRIVACY PRESERVATION OF HETEROGENEOUS DATA BETWEEN BUSINESSES

Arafat Salih AYDINER[1]

https://doi.org/10.55071/ticaretfbd.1762972

Sorumlu Yazar (Corresponding Author)	*Geliş Tarihi (Received)*	*Revizyon Tarihi (Revised)*	*Kabul Tarihi (Accepted)*
arafat.aydiner@medeniyet.edu.tr	*11.08.2025*	*04.11.2025*	*04.11.2025*

Öz

Yapay zekâ uygulamalarının hızla yaygınlaştığı bir çağda, veri kullanımının yaygınlaşması ve kişisel hakların korunmasının giderek zorlaşması, bu alanın doğası gereği dijital kişisel veri koruma tekniklerinin geliştirilmesinin önünü açmıştır. Bu çalışmada, kavramsal analiz kullanılarak literatürden kişisel verilerin korunmasına yönelik gizlilik koruma teknikleri çıkarılmıştır. Literatür analizinden 30 farklı makaleye dayanarak, aynı amaç için farklı verilerin eğitilmesine olanak tanıyan Federe Transfer Öğrenme yöntemini tanımlayan bir model önerisi geliştirilmiştir. Böylece çalışma, yerel verileri paylaşmadan çeşitli verilerin kullanılmasını sağlayarak ve ortak sorunların çözümü için gizlilik koruması ile karar alma desteği sağlayarak sahadaki pratik veri kullanım zorluklarını ele alan teorik ve pratik katkılar sağlayacaktır.

Anahtar Kelimeler: Veri gizliliği, gizlilik koruma teknikleri, federe öğrenme, federe transfer öğrenme, heterojen veriler.

Abstract

In the era of rapid artificial intelligence implementations, the proliferation of data use and the increasing difficulty of protecting personal rights, coupled with its inherent nature, have paved the way for the development of digital personal data protection techniques. In this study, privacy preservation techniques for protecting personal data were extracted from the literature using conceptual analysis. A model proposal was developed based on 30 different articles from the literature analysis, identifying the Federated Transfer Learning method, which enables training different data for the same purpose. Thus, the study will provide theoretical and practical contributions that address practical data usage challenges in the field by enabling the use of diverse data without sharing local data and providing privacy preservation with decision-making support for solving common problems.

Keywords: Data privacy, privacy preservation techniques, federated learning, federated transfer learning, heterogeneous data.

[1] İstanbul Medeniyet Üniversitesi, Siyasal Bilgiler Fakültesi, İşletme Bölümü, İstanbul, Türkiye.
arafat.aydiner@medeniyet.edu.tr.

1. GİRİŞ

Teknolojik ürünlerin artan kullanımı, dijitalleşmenin hızla yaygınlaşması, bununla beraber ortaya çıkan yeni teknolojilerin yoğun bir şekilde günlük hayatta kullanılması kişisel verilerin işlenmesine olanak tanımıştır. Biriken veri genişliği, çokluğu ve çeşitliliği ile artan suç eğilimleri ve yanlış kullanımlar, kişisel verilerin korunması için birçok ülkeyi ciddi önlemler almaya sevk etmiştir. Özellikle sağlık, ticaret, finans, devlet, siyaset, toplumsal, askeri gibi kritik alanlarda toplanan veriler, her türlü kişisel verinin özel nitelikli veri olarak tanımlanmasına yol açmıştır. Kişisel bilgilerin toplanması, bireysel gizliliği koruyacak ve veri kullanımını güvence altına alarak tekniklerin geliştirilmesini gerekli kılmıştır. Bu hassasiyet çerçevesinde çıkarılan kanunlar özellikle Türkiye'de verinin toplanması, saklanması ve kullanılmasının ancak ilgili kişinin açık rızası ile mümkün olabileceğini şeklinde düzenlenmiştir (Türkiye Büyük Millet Meclisi (T.B.M.M), 2016).

Veri çokluğu her alanda kabiliyetlerin gelişmesini sağlarken, oluşturulan kanunlar kişisel bilgileri koruyan sıkı kurallar getirmiştir. Bu kurallar veri paylaşımını ve dijitalleşmede kişiye özel çözümlerin geliştirilmesini kısıtlamaktadır. Sağlık, finans, ticaret gibi alanlarda çıkan problemlere kişinin şahsi verisine kadar inerek bireysel çözümler bulunabilecekken, kişisel güvenliğin öncelikli olması, kişisel verilerin hukuki açıdan mülkiyet hakkı olarak kabul edilmesi, (T.B.M.M, 2016) kişisel problemlerin çözümünü engellemektedir. Bu nedenle veri paylaşımı yapılamadığında kurumlar arası ortak çalışma imkanları da kısıtlanmaktadır. Yapay zekâ üzerine yapılan çalışmalar, bu türden hukuki engellere takıldığından bireysel çözümlerin ve ortak iş birliklerinin oluşturulmasında engel teşkil etmektedir (Trinidad ve ark., 2010). Kişilik hakların korunması her ne kadar önemli ise, bilimsel alandaki gelişmelerin devamlılığını sağlamak, ortak ya da kişisel problemlere çözüm bulabilmek bir o kadar iş hayatı ve toplumsal açından önem arz etmektedir. Bundan dolayı kişisel veriyi korumak, toplanan, işlenen verilerle yapay zekâ (YZ) modellerinin güvenli bir şekilde geliştirilmesini sağlamak için bir denge kurmak önemlidir (Mitrou, 2018). Birçok sektörde kişilerin mahrem bilgilerinin toplanarak ilave efor olmadan yeniden kullanımı mümkündür (Chan ve ark., 2014). Fakat veri paylaşımı yapılırken kişisel verinin gizliliği açığa çıkabilir (Torkzadehmahani ve ark., 2021). Bu durumunda hem Kişisel Verileri Koruma Kanunu (KVKK) hem de Avrupa'daki "General Data Protection Regulation" (GDPR) kanunlarının düzenlemeleriyle karşılaşılmaktadır (European Parliament & Council of the European Union, 2016). İlaveten, dünyanın değişik yerlerinde, özellikle ticari işletmelerin Amerika Birleşik Devletleri, Çin'de yaptıkları veri ilintili faaliyetlerde kişisel verileri korumak için farklı versiyonlarda kural ve kanunlarla karşılaşmaktadırlar.

YZ ve makine öğrenmesi (MÖ) yöntemleri bilgisayarların veriyi kaynak olarak kullanabildiği, eğitilebilen yazılımsal teknolojilerdir. Verinin çokluğu, kalitesi ve niteliği, başarılı MÖ algoritmalarının en önemli şartlarındandır (Geron, 2017). YZ çağına girdiğimiz bu dönemde, değişik vasıfta olan verilerin sistemlerle, kurumlarla ve şahıslarla doğrudan paylaşılmadan, veri güvenliğini koruyarak kullanılabilirliğinin nasıl sağlanması gerektiği araştırma sorusu bu çalışmada belirlenmiştir. Gizliliği koruma prensibi için kullanılan birçok teknik arasında veri paylaşımı olmadan güvenliği sağlayan bir teknik önce çıkmaktadır. MÖ tekniği olarak ortaya çıkan federe öğrenme (FÖ) sayesinde, verileri merkezi bir sistemde toplamadan modeli eğiterek veri

gizliliğini sağlandığı görülmüştür (McMahan ve ark., 2017). Bu sayede yerel sistemlerdeki veriler güvende tutulmakta, ortak çalışma ile mevcut bir modelin geniş katılımcılarla eğitilebildiği görülmüştür. Bu çalışmanın temel amacı, yukarıda belirlenen araştırma sorusuna yanıt olarak farklı kuruluşların farklı yapıdaki verilerini model eğitimi için kullanarak iş birliği yapabileceği merkeziyetiz bir platform önerisidir. Bu kapsamda farklı MÖ modelleri incelenmiş ve bir çerçeve oluşturulmuştur. Bu modeller arasında hedef çerçevesinde en fazla FÖ modellerine odaklanılmıştır.

Çalışmada, özel nitelikli verilerin paylaşımına gerek kalmadan tüm paydaşların iş birliği yapmasına olanak tanıyan federe makine öğrenmesi tekniği ele alınmıştır. Bu teknik, doğrudan açık veriyi paylaşmak yerine öğrenilmiş modellerin paylaşımını sağlar. Ayrıca diğer tekniklere göre avantajları, mimari modeli değerlendirilerek farklı veriler için alternatif model önerilmiştir. Bu sayede kurumlar farklı veri içeriklerini FÖ ve Federe Transfer (FT) Öğrenme yaklaşımlarıyla geliştirdikleri modelleri paylaşabilecek ve diğer kuruluşların farklı verilerden oluşan modellerini de kullanacaktır. Böylelikle FT öğrenme dinamik kabiliyetler teorisi perspektifiyle değerlendirildiğinde, veri kullanımı bağlamında ortaya çıkacak fırsatları algılama, yakalama ve bunları pratik kullanılabilir hale dönüştürüldüğü görülecektir. Bu çalışmanın önemi, FT öğrenmeyle kurgulanan modeller, kuruluşların farklı veriler üzerinden sürdürülebilir ve güvenilir bir çerçevede iş birliği yapabilmesini sağlayacak, açık veri felsefesiyle gizliliği koruyarak ortak sorunlara çözüm imkânı sağlayacaktır. Bu sayede yapılan çalışmalar tekrar kullanılabilir olacak ve limitli kaynaklarla yürütülen çalışmalar daha geniş kitleler tarafından ele alınarak karar vericiler için doğru sonuç üretmek mümkün olacaktır. Sonuç olarak araştırma-geliştirme (ARGE), verilerin maskelenmesi ve korunması için ayrılan bütçe, zaman ve emek daha verimli bir şekilde kullanılmış olacaktır. Verimliliğin sağlanmasının yanı sıra kişinin en hassas verisi olabilecek kişisel verinin mahremiyeti de gizliliği koruma tekniği olan FT öğrenme sayesinde güvence altına alınmış olacaktır.

Çalışmanın bundan sonraki içeriğinde konu ile alakalı literatür taraması gerçekleştirilmiş, araştırmanın temel sorusu oluşturularak model önerisi ortaya konmuştur. Müteakiben araştırmanın metodu, son olarak da sonuç ve etkileri tartışılarak çalışma sonuçlandırılmıştır.

2. YÖNTEM

Bu çalışmada betimleyici (narratif) literatür taraması yöntemi tercih edilmiş, metinsel veriler analiz edilerek araştırma sorusunun cevabına ulaşacak çerçeve model geliştirilmiştir. Betimleyici literatür tarama yöntemin amacı, araştırmamızdaki sorunları, zayıflıkları ve tartışmaları ortaya çıkararak veri güvenliği ve mahremiyeti açısından teknolojik çözümlerin tespitini sağlamak, aralarında veri paylaşımı yapılmadan heterojen ortamlarda çözüm sağlayan çerçeve modeline ulaşmaktır (Baumeister & Leary, 1997). İlgilendiğimiz ana çerçeve YZ için kavram gizliliği ve mahremiyeti koruma, korumayı sağlayabilecek teknolojik çözümlerdir. Bu genel çerçeve üzerinden detaylı bir şekilde veri paylaşmadan model eğiten MÖ çözümleri ve heterojen özellikteki verilerin veri paylaşımsız olarak YZ modellerinde eğitilmesi betimleyici yöntemle analiz edilmiştir. Araştırmada kullanılan terimler; gizliliği koruma, veri gizliliği, veri mahremiyeti, YZ ve veri mahremiyet, gizliliğini korumak

ve teknolojik çözümler, heterojen özellikteki veri, güvenliği koruma modelleri, MÖ'de kullanılan modeller ve öğrenme yöntemleri, transfer öğrenme, federe öğrenme olarak belirlenmiştir. Bu temalar doğrultusunda Google Scholar üzerinden yapılan taramada Web of Science veri tabanına ait SSCI, SCI indeksleri, ayrıca Scopus ve TRDizin veri tabanları kullanılmıştır. Bu kapsamda 51 makale incelenmiştir. Ancak, belirlenen temalar dışında kalan terimler, işletme, yönetim bilişim sistemleri, bilgisayar bilimleri ve mühendisliği alanlarının dışındaki sonuçlar elenmiş, böylece 51 sonuç 30 makaleye indirgenmiştir. Temaların makale konularıyla eşleşmeleri aşağıdaki Tablo 1'de verilmektedir.

Tablo 1. Tema ve Makale Eşleşmesi

Temalar	Makale Konuları
Gizliliği koruma / Veri gizliliği / Veri mahremiyeti	Veri Koruma, Gizlilik Teorisi, Bilgi Gizliliği, Bilgi Etiği, Bilgi İşlem Yönetimi
YZ AND veri mahremiyeti	Gizlilik Koruma Makine Öğrenmesi, Büyük Veri Mahremiyeti
Gizliliğini korumak AND teknolojik çözümler	Diferansiyel Gizlilik, Homomorfik Şifreleme, Blokzinciri, Servis olarak Gizlilik
Heterojen özellikteki veri / Heterojen özellikteki veri AND güvenlik koruma modelleri	Federe Öğrenme, Federe Transfer Öğrenme, Hiyerarşik Federe Öğrenme
MÖ modelleri AND öğrenme yöntemleri	Gizlilik Koruma Makine Öğrenmesi (MÖ odaklı)
Transfer öğrenme	Federe Transfer Öğrenme, Transfer Learning tabanlı modeller
Federe öğrenme AND Transfer öğrenme	Federe Öğrenme, Federe Transfer Öğrenme, Hiyerarşik Federe Öğrenme

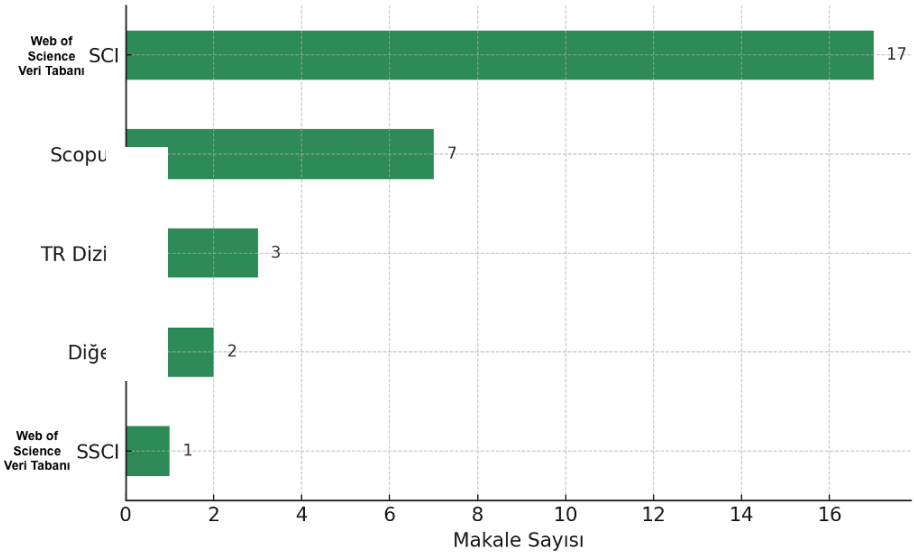
Yapılan eleme sonrası, temaların makalelerle eşleştirilmesiyle çalışmamızda incelenen makale konuları, adetleri ve çalışma içerisindeki yüzdelik olarak ağırlıkları tespit edilip Tablo 2' de paylaşılmıştır.

Tablo 2. İncelenen Makale Konu ve Adetleri

Makale Konusu	Çalışmada Kullanılan Adet	Yüzdelik %
Federe Öğrenme	7	23,3
Federe Transfer Öğrenme	4	13,3
Veri Koruma	3	10
Gizlilik Koruma Makine Öğrenmesi	2	6,7
Diferansiyel Gizlilik	2	6,7
Blokzinciri	2	6,7

Hiyerarşik Federe Öğrenme	2	6,7
Gizlilik Teorisi	2	6,7
Homomorfik Şifreleme	1	3,3
Bilgi Gizliliği	1	3,3
Servis olarak Gizlilik	1	3,3
Bilgi Etiği	1	3,3
Bilgi İşlem Yönetimi	1	3,3
Büyük Veri Mahremiyeti	1	3,3

İncelenen her bir makale veri tabanları açısından da değerlendirilip Şekil 1'de detayları verilmiş, ayrıca Tablo 3' de makale konularının yıllara göre dağılımı ve adetleri tablolaştırılmıştır.

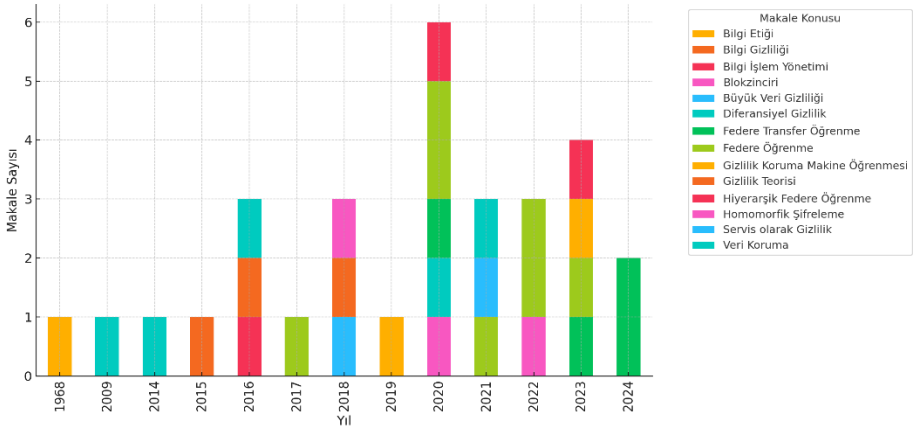


Şekil 1. Makalelerin Veri Tabanlarına Göre Dağılımı

Tablo 3. Yıllara Göre Temaların Dağılımı

Yıl	Temalar	Adet
1968	Bilgi Etiği	1
2009	Veri Koruma	1
2014	Diferansiyel Gizlilik	1
2015	Bilgi Gizliliği	1
2016	Veri Koruma	1
2016	Bilgi İşlem Yönetimi	1
2016	Gizlilik Teorisi	1
2017	Federe Öğrenme	1
2018	Büyük Veri Mahremiyeti	1
2018	Homomorfik Şifreleme	1

2018	Gizlilik Teorisi	1
2019	Gizlilik Koruma Makine Öğrenmesi	1
2020	Blokzinciri	1
2020	Diferansiyel Gizlilik	1
2020	Federe Öğrenme	2
2020	Federe Transfer Öğrenme	1
2020	Hiyerarşik Federe Öğrenme	1
2021	Veri Koruma	1
2021	Federe Öğrenme	1
2021	Servis olarak Gizlilik	1
2022	Blokzinciri	1
2022	Federe Öğrenme	2
2023	Federe Öğrenme	1
2023	Federe Transfer Öğrenme	1
2023	Hiyerarşik Federe Öğrenme	1
2023	Gizlilik Koruma Makine Öğrenmesi	1
2024	Federe Transfer Öğrenme	2



Şekil 2. Yıllara Göre Makale Konularının Dağılımı

Çalışmamızın incelenen makalelerinin yıllara göre konu bazlı dağılımı incelendiğinde bilgi güvenliği ve etiğinin yıllar öncesine dayanan bir sorun olduğu ve bu sorunun teorik yaklaşımlarının kurulduğu görülmektedir. Veri ve bilginin korunmasına dair çalışmaların 2018 yılında artık teknolojik koruma yöntemlerine evrildiği anlaşılmaktadır. 2020 sonrası sistemlerin ve verilerin karmaşıklaşması, YZ kullanımının artması MÖ tekniklerinin daha fazla veri ile buluşması FÖ tekniklerinin çalışılmaya başladığını göstermektedir. Bu da artık verinin gizliliğini koruyarak daha fazla kitlelere ulaştırılmak istenmesinin göstergesidir. Son yıllara gelindiğinde ise çalışmamızın temelini oluşturan farklı veri türlerinin MÖ modellerinde kullanılmak istenmesi, FT öğrenme yönündeki çalışmaların hızlandırıldığını göstermektedir. Bu bağlamda Şekil 2, literatürün ihtiyaçlarla doğru orantılı olarak geliştiğini, aynı zamanda çalışmamızın güncelliğini ortaya koymaktadır.

3. LİTERATÜR TARAMASI

Bu bölümde, veri mahremiyeti gözden geçirilip, literatürden yararlanılarak veri gizliliğini koruyan teknolojik yaklaşımlar incelenecektir. Bunların genel özellikleri ve farklılıkları ortaya konarak FÖ ve FT öğrenme tekniğinin öne çıkan yönlerini irdelenip araştırma sorusuyla beraber konsept model önerisi oluşturulacaktır.

3.1. Veri Mahremiyeti ve Güvenliği

Gelişen donanımsal altyapılar, verilerin daha kolay depolanması ve hızlı işlenme olanağını arttırmıştır. Verilerin biriktirilmesi ile birlikte gelişen yapay zeka, nesnelerin interneti, mobil internet ve dijitalleşmede mobilitenin artması da veri mahremiyeti endişelerini arttırmaktadır (Acquisti ve ark., 2015). Bu endişeler sadece verinin kendisiyle alakalı değildir. Verilerin toplama yöntemi, bunları depolamak için oluşturulan alt yapının geliştirilmesi bütün bir yapı olarak ele alınmalıdır. (Solove, 2008). Özellikle sağlık ve genetik verilerinin kullanımı, kişisel haklarının zedelenmesine, yanıltıcı bilgiler üretilmesine ve ayrımcılık ya da ırkçılık gibi suçların işlenmesine yol açabilmektedir (Oktay, 2022).

Kişisel mahremiyet: kişilerin, grupların ya da organizasyonların kendileri hakkında başkalarıyla ne zaman, nasıl ve ne kadar bilgi paylaşacağı şeklinde anlaşılmaktadır (Fano, 1968; Nissim & Wood, 2018). Kişisel mahremiyet, insanın doğasından gelir; aynı zamanda sosyal insanın bilgi edinme merakı, bu olgunun çevresel ve kültürel bir yönü olduğunu da göstermektedir. Ayrıca insanın kişisel mahremiyeti dinamik kabiliyetler çerçevesi etrafında oluşan fırsat ve tehditleri algılamasına, ona göre kendisini dönüştürmesine sebep olmaktadır. Bu dinamik yapı, kişilerin veri mahremiyetini kendileri kontrol ettiğinde haklarının korunacağını gösterir. Bilginin bir güç olduğu aşikardır. Bu güçten faydalı bir sonuç çıkarmak için model oluşturularak, güvenirliği test edilip, sonuçları bağlamında gerekli hareket tarzının benimsenmesi gerekir. Bunun için bir dengenin oluşturulması, bu dengenin de gerektiğinde kişilerin kendi mahremiyeti hakkında karar vermesini sağlaması gerekmektedir (Barker ve ark., 2009; Fano, 1968). Literatürde kişisel bilginin uygunluğu ve dağıtımı tartışılmıştır. Modern toplumlarda ise bireylerin, kendi değerleri çerçevesinde yaptıkları iç tartışma sonucunda verilerinin uygunluğuna ve dağıtımı/dağılmasına karar verdikleri görüşü ağır basmıştır. Bilginin toplanması, işlenmesi, dağıtımı/dağılması, bilgi akışı ve istilasının veri mahremiyetinin değerlendirilmesi gereken ana temeller olduğu kanaati ortaya çıkmıştır (Mulligan ve ark., 2016). Ayrıca finansal, sağlık, kimliksel, ve davranışsal olarak da veri mahremiyetinin sınıflandırılması mümkün olmuştur (Dülger, 2021)

Tüm bu yaklaşımlar, veri mahremiyetinin kişisel olması, güvenliğin kişiselleştirilerek temin edilmesi gerekliliğini göstermektedir. Özellikle YZ teknolojilerinin ihtiyaç duyduğu hassas verilerin analizi, paylaşım ve saklama süreçlerindeki gizliliğin teminat altına alındığı koruma yöntemlerinin geliştirilmesi zorunlu hale gelmiştir (Al-Rubaie & Chang, 2019; T. Li ve ark., 2020; Ram Mohan Rao ve ark., 2018). Zorunluluk haline gelen verilerin güvenliği konusundaki bu beklentileri karşılamak için kişisel verileri güvenli hale getirecek teknolojik yöntemler aşağıdaki bölümde bahsedilmektedir.

3.2. Gizliliği Koruma Teknikleri

3.2.1. Kriptografik teknikler

Kriptografi bir iletişim metodu ya da stratejisi denilebilir. Alıcı ve gönderici arasındaki güvenli veri alışverişinin oluşmasını sağlar. Alıcı ve göndericinin arasındaki mesajın güvenli bir şekilde paylaşımını sağlarken içeriğin gizliliğini ve bütünlüğünü korumayı hedefleyen bir tekniktir (Khalid ve ark., 2023).

Kriptografi tekniğine bakıldığında homomorfik şifreleme, güvenli çok taraflı hesaplama, literatürde en sık kullanılan teknikler olarak karşımıza çıkmaktadır (Al-Rubaie & Chang, 2019; Khalid ve ark., 2023). Güvenli çok taraflı hesaplamalar da girdilerin gizli tutulmasını sağlayarak güvenilir merkezi bir otoriteye olan ihtiyacı ortadan kaldırmaktadır. Veri sayısı ve katılım arttıkça, iletişim karmaşıklığı ve hesaplama maliyetlerinin ortaya çıktığı görülmüştür (Al-Rubaie & Chang, 2019). Homomorfik şifrelemede, şifrelerin çözümlenmesine gerek kalmadan hesaplama yapılmasını sağlayan bir yöntem olsa da gecikme ve depolamanın artmasına sebep olması yöntemin eksikliklerindendir. Hassas sağlık verilerinde kullanılmakla beraber, sağlık verilerinin oluşturduğu büyüklük dolayısıyla verimi düşüktür (Acar ve ark., 2018).

3.2.2. Veri pertürbasyon algoritması

Bu algoritmanın temel işlevi, gizlilik sızıntılarını veya saldırıları sınırlamak adına verilerin karşı tarafla paylaşılmadan önce değiştirmesidir. Değiştirilen veriler herhangi bir format değişimine maruz kalmazlar. Bu yüzden de kriptografik metotlara göre daha düşük zaman ve karmaşıklığa sahiptirler. Veri pertürbasyonunun kullanım tercihi bu yüzden daha fazladır (Chamikara ve ark., 2021a; Khalid ve ark., 2023). Bu yöntemin birçok farklı yaklaşımları mevcuttur. Bunlar; ek pertürbasyon, rastgele döndürme, geometrik pertürbasyon, rastgele yanıt, rastgele projeksiyon, mikro toplama, hibrit pertürbasyon, veri yoğunlaştırma, veri sarma, veri yuvarlama ve veri değiştirme olarak literatüre girmişlerdir (Chamikara ve ark., 2021a). Bunların her biri veri kümelerinde fark davranış sergilerler.

Veri pertürbasyon algoritmalarının en önemli dezavantajı belirli bir sorun için en uygun algoritmayı seçebilmektir. Bu karmaşıklık, gizlilik modellerinin farklı özellikleri, algoritmaların farklı özellikleri, giriş verilerinin farklı dinamikleri ve kullanılan farklı uygulama türlerinin olması veri gizliliğinin korunmasının etkinliğini ve sonuçlarını etkileyen niteliklere sahip olması dezavantaj olarak görülür. Açık bir uygulama seçim yöntemi olmadığından tercih edilebilirliği düşmektedir (Chamikara ve ark., 2021a; Keshk ve ark., 2020).

3.2.3. İstatistiksel gizlilik mekanizmaları

Bu teknik, verilere veya hesaplama sonuçlarına rastgelelik ekleyerek, veri üzerinde gizliliği ve korumayı sağlamaktadır. Diferansiyel gizlilik ise literatürde en sık kullanılan yöntem olarak karşımıza çıkmaktadır (Dwork & Roth, 2014). Bu yöntem gizliliğin korunması için matematiksel bir çerçeve sunmaktadır. Tek bir bireyin verilerinin bir veri kümesine dahil edilmesi ve bireysel kaydın etkisini maskelemek için

verilere yada sorgulara gürültü eklenerek diferansiyel gizlilik sağlanmış olur (Hassan ve ark., 2020). Kullanıcının kimliği paylaşılmadan veri üzerinden analiz yapma imkânı sağlamaktadır. Bu yöntemde çok fazla veriye gürültü eklenmesi ve gizliliğin kalibrasyonu, yöntemi dezavantajlı hale getirmektedir (Dwork & Roth, 2014; Hassan ve ark., 2020; Khalid ve ark., 2023).

3.2.4. Blokzinciri temelli gizlilik koruması

Blokzinciri, dağıtık yapısı ve şeffaflığı sayesinde farklı yöntem ve mimariler kullanarak gizliliği sağlamakta; değişmezliği ve doğrulanabilirliği güvence altına almaktadır. (Özcandan ve ark., 2020). Blokzinciri temelli gizlilikte, veri işlemlerinin gerçekleştiği ağ düğümleri arasındaki iletişim şifreleme yöntemleriyle korunur. Karma metodoloji şeklinde dijital imzalar, açık anahtar yapısı gibi kriptografik ilkelerle güvenlik sağlanır (Marijan & Lal, 2022). En yaygın kullanılan yöntemlerden biri sıfır-bilgi ispatlarıdır (Zero-Knowledge Proofs). Bu yapı sayesinde gönderen, alıcı ve miktarın gizlenmesi sağlanmaktadır (Ben-Sasson ve ark., 2014). Diğer bir yöntem de gizli işlem (Confidential Transaction) yöntemidir. Bu yöntemde Pedersen taahhütleri ve aralık ispatlarıyla işlem miktarını gizlerken, sistemin kalanları doğrulamasına imkan tanır (Bunz ve ark., 2018; Kardaş & Kiraz, 2018). Açık anahtar yapısı ise asimetrik kriptografi prensibine dayanır. Özel anahtar sadece sahibinde bulunur ve gizli tutulur. Bununla işlemler imzalanır. Herkesle paylaşılan açık anahtar, özel anahtarla matematiksel ilişkisi olan işlemlerin doğrulanmasında kullanılır. Alıcı yani diğer düğümler gönderenin verisini bu şekilde doğrular (Shin, 2019). Kriptografik çözümlerin dışında, zincir dışı yaklaşımlarla dağıtık dosya sistemleri üzerinden verilerin Blokzinciri dışında karma değerler (hash value) sayesinde zincire kaydedilmesi sağlanarak da güvenlik sağlanmaktadır (Kardaş & Kiraz, 2018).

Blokzincirinde paydaşlar, her bir ağın düğüm noktası olarak faaliyet gösterir. İşlemlerin bütünlüğünü doğrulayan, bir problemin çözümüyle oluşturulan bu ağ noktaları dağıtık vaziyettedir. Ağ noktalarından biri işlemleri oluştururken, diğeri bunları doğrulayarak defterde depolar (Marijan & Lal, 2022). Her işlem kaydı blok zincirine defter bloğu olarak sıkıştırılmıştır. Kaydedilen bu blok içerikleri birer muhasebe defteri olarak kabul edilirler. Ağ içerisinde bulunan her bir blok eş zamanlı güncellenir, böylece her bir defterin kopyası her bir ağ noktasında tutulmuş olur. Yeni blok eklemek için kullanılan uzlaşı algoritmaları vardır. En popülerleri proof of work (PoW) ve proof of stake (PoS) algoritmalarıdır. Ancak en büyük riski kötü niyetli bir blok oluşturucusunun (madenci) %51' den daha yüksek bir bilgisayar gücüne sahip olması durumunda, algoritmaların kullanım prensipleri ihlal edilebilir (Keshk ve ark., 2020). Blokzincinin gizlilik koruma uygulamalarının daha çok fiziksel siber sistemlerde, belirli noktasal alanlarda kullandığı görülmektedir. Özellikle akıllı şehirlerde, fiziksel ağların oluşumunda, veri sağlayıcıların doğrulanması, güç ve enerji noktalarının saldırılara karşı korunması uygulamalarında blokzinciri tabanlı uygulamaların denendiği literatürde görülmüştür (Keshk ve ark., 2020). Aynı zamanda blokzinciri teknolojisinde yeterli protokollerin oluşmaması kullanıcılarda işlemlerin gizliliği konusunda endişeler oluşturmaktadır. Bu yüzden blokzinciri teknolojisi uygulandığında, gizliliğin korunması yöntemlerinin hibrit olarak kullanılmasıyla işlemlerin daha güvenli hale geleceği ön görülmektedir (Hassan ve ark., 2020).

Blokzincirinde diğer güvenli depolama yöntemi akıllı kontratlardır. Bu yöntemde güvenli depolamayış sağlamak için çok katmanlı teknikler kullanılır. Kriptografi, diferansiyel gizlilik, homomorfik şifreleme ve sıfır bilgi ispatları gibi yöntemlerin kullanılmasıyla akıllı kontratlar işlemlerin otomatik ve güvenilir bir şekilde yürütümünü sağlar (Giancaspro, 2017). Kontratta yazılı olan sözleşmenin koşullarının sağlanması, şartların doğrulanmasıyla merkezi olmayan otomasyon işleme başlar. Sözleşmenin kuralları, işlemlerin güvenliğini sağlamada önemli rol oyamaktadır. Kontrat sayesinde blokzincirinde güvenilir üçüncü bir tarafın olmasına gerek duyulmamaktadır (Hassan ve ark., 2020). Blokzincirinin işlem gizliliği ve güvenliğinde akıllı kontratların önemli bir işlevinin olduğu gözlemlenir. Akıllı kontralar veri birleştirmede, onay yöntemlerinde, hassas sistemlerin erişim kontrolünde ve işlem masraflarının azaltılmasında fayda sağladıkları düşünülmektedir. İlaveten, saldırılara karşı direnç, merkeziyetsizlik ve şeffaflık gibi özellikleriyle güven duyulan platformlar haline gelmişlerdir. Ancak, her yazılımda olduğu gibi güvenlik açıklarına yol açabilen yazılım hataları çıkabilir. Bunlarda güvenli yazılım geliştirme prensipleri kullanılarak bertaraf edilebilir. En büyük zorluğu, kontrat işleme konulduktan sonra değiştirilmesi çok zordur. En fazla kullanım alanını hassas veriye dayalı ve duyarlı uygulamalarda kullanım alanı bulmaktadır (Marijan & Lal, 2022).

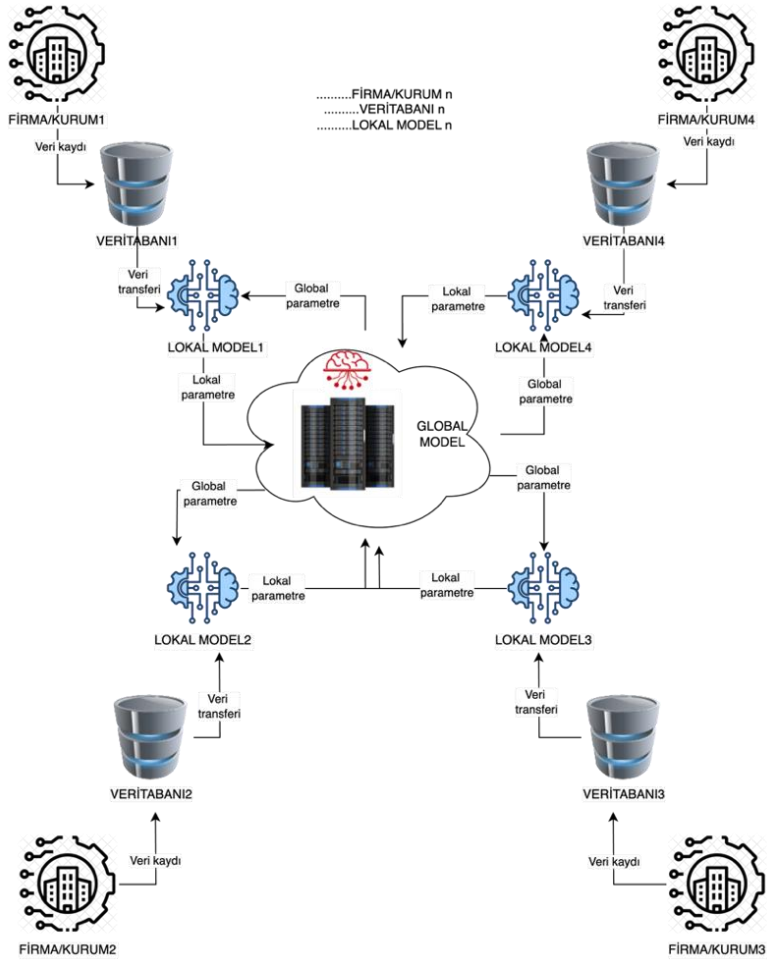
3.2.5. Federe öğrenme

Federe öğrenme, bir makine öğrenmesi (MÖ) yöntemidir. Modeller dağıtık mekanlardaki cihazlarda yerel olarak eğitilir; güncellemeler merkezi sunucuya gönderilir ve ana model bununla güncellenir (Khalid ve ark., 2023; McMahan ve ark., 2017; Oktay, 2022). Aslında temel olarak MÖ modellerinin geliştirilmesi için algoritmik bir çerçeve oluşturmaktadır (Khalid ve ark., 2023). Model eğitim sürecinde veri paylaşılmaz ve federe öğrenme yapılan her lokasyonda verinin korunması gereken kısmı açık edilmez. FÖ aynı zamanda ortak çalışma kültürüyle model eğitmede kolektif bakış açısını desteklemektedir. İki ya da daha fazla taraf, ellerinde bulundurdukları veriyle model eğitme sürecine katkı sağlar. Model, paylaşılan tarafın verileri yeniden tasarlayıp değiştirmesini önleyen bir şifreleme yöntemiyle iletilmektedir. Eğitilen yeni model ise birden fazla katkı sayesinde ideal modele yakın yaklaşımı içerecektir (Khalid ve ark., 2023). Federe öğrenmenin özelliği ham verilerin cihazda saklı tutularak, sunuculara iletilen güncellemelerin belli bir amaca odaklanan geçici, mümkün olan en az veriyle, en kısa sürede modelin eğitiminin gerçekleşmesini sağlar (Khalid ve ark., 2023; McMahan ve ark., 2017)

Mobil cihazların günümüzde yaygın olması, aynı zamanda kendi verilerini cihazda tutabilen özellikte alt yapıların geliştirilmesi, lokasyon verileriyle beraber birçok kişisel verilerin kaydedilmesine olanak sağlamaktadır. Kişisel cihazlarda veya kurumsal sunucularda tutulan verilerin değişik nedenlerden dolayı işlenerek bunlardan belirli anlamları çıkarmak mümkündür. Özellikle iş hayatında müşteri davranışlarını takip ederek rekabet avantajı elde etmek isteyen kurumlar hem mobil uygulamalarla hem de kurumsal sunucularında tuttukları bu verileri kullanma eğilimindedir. Ancak hassas verilerin merkezi cihazlara çekilerek buralarda işleme tabi tutulması kişisel verilerin kullanımını riske atacaktır. Bu riski ortadan kaldırmak için geliştirilen FÖ modelleri, merkezi sistemin kabiliyetiyle uzakta bulunan başka sistemlere dağıtılır. Uzaktaki bu sistemler, kendi işlemci kaynaklarını kullanarak modeli yerel verilerle eğitir. Eğitilen modeldeki parametreler merkezi sisteme geri gönderilerek çeşitli algoritmalarla model

genelleştirilir (Briggs ve ark., 2020). Mesela, TensorFlow, PySyft gibi model araçları yöntemin geliştirilmesinde kullanılan yazılım kütüphaneleridir. Bu yöntemle uzaktan öğrenme sürecinin gerçekleştirilmesi mümkün olacaktır (McMahan ve ark., 2017; Oktay, 2022)

FÖ'nün genel çalışma prensibi Şekil 3' de gösterilmektedir. Aynı yapıyı içeren verilerin kendi içlerindeki MÖ modelinde eğitilmesi sonrasında gerekli parametrelerin FÖ algoritmasıyla çalışan ana makineye gönderilmesi prensibine dayanır. Bu süreci tüm sistem içerisindeki katılımcılar işleterek ellerindeki modelleri merkezi sisteme yüklerler. Ana makinedeki FÖ kabiliyeti sayesinde paylaşılan parametrelerle ana model eğitim süreci oluşturularak ana model güncellenir. Güncellenmiş bu model ise tekrardan tüm paydaşlara indirilerek olgunlaşmış model tüm katılımcıların hizmetine sunulmuş olur. Böylelikle veri gizliliği sağlanarak ortak paylaşımla daha iyiye yakın bir model tüm katılımcıların istifadesine sunulmuş olur. Bu genel FÖ modelinde katılımcıların verilerinin aynı yapıda olması gerekmektedir (Zhou ve ark., 2023). Bu yöntem ancak aynı veri yapısını kullanan katılımcıların, işletmelerin, kurumların ve araştırma merkezlerinin ortak çalışmasına imkân verir. Ancak işletmelerin günümüzde yaygın olarak yapay zekayı (YZ) kullanmak istemelerinden kaynaklanan farklı veri setlerinin güvenli eğitilmesi için gerekli olanakları sağlamadığı aşikardır. Dolayısıyla araştırma sorumuzdaki problemi FÖ yönteminin tam olarak karşılamadığı görülmüştür.



Şekil 3. Federe Öğrenme Temel Çalışma Prensibi (Zheng ve ark., 2023)

3.3. Heterojen Yapı ve Verilere Model Önerisi

Farklı yapıların ve olguların olduğu senaryolarda tek bir yöntem üzerinden gidilerek sonuç üretmek mümkün değildir. Verilerin farklı yapılarda bulunması ve farklı parametreler içermesi, karşılaşılan en büyük engellerden biridir. İşletmeler veri çeşitliliği bakımından heterojen yapıya sahiptirler. FÖ yöntemi, homojen yapıdaki cihazlarda oluşturulan modellerin lokal olarak işlenip, merkezi bir sunucuda genel modelle eğitilerek lokal modellere güncellenme göndermesiyle çalışmaktadır. Bu yöntem, farklı örnekler olsa da aynı özellikteki verileri eğitmeye dayanmaktadır (Chamikara ve ark., 2021b; Liu ve ark., 2020; Putra ve ark., 2023). Ancak en büyük problem, finans, muhasebe, pazarlama ve bilişim gibi farklı özelliklere sahip veriler içeren işletmelerin oluşturduğu heterojen yapılardan kaynaklanmaktadır. Bu tür ortamlarda veri güvenliği sağlandıktan sonra, söz konusu eğitimlerin güvenli bir şekilde gerçekleştirilebilmesi mümkün olmaktadır. Ayrıca farklı işletme tiplerinin aynı

problemlerde YZ ile çözüm üretmesini sağlayabilmek en önemli zorluklardandır. Heterojen yapıdaki işletmelerin verilerinin yapay zeka (YZ) modellerinde eğitilmesi tek bir yöntemle değil ancak birkaç yöntemin ortak özelliklerinin birleştirilmesi sonucunda çözüme kavuşturulabilir (Liu ve ark., 2020; Putra ve ark., 2023). İşletmelerde oluşan karmaşık özellikler, veri güvenliğinin sağlanmasındaki zorluklar, firmaların YZ ve MÖ becerilerine mesafeli yaklaşmalarına sebep olmaktadır. Literatürde incelenen yöntemler heterojen yapılara çoğunlukla cevap vermemektedir. Veriyi olduğu gibi kullanmaları, performans kaybına sebebiyet vermeleri, model eğitimini sağlamamaları, saylayanları da sadece aynı ortamı eğitmeleri işletmelerin heterojen yapısına alternatif yöntem ihtiyacını doğurmuştur. FÖ' nin oluşturduğu güvenli ve verilerin paylaşılmadan model halinde eğitildiği bir ortam, farklı özellikteki veri barından işletmelerin gündemine girecek yaklaşımlar sağlamaktadır. Ancak bu yöntemlerin bilgisayar, iletişim bilimleri açısından modellerin test edilmesiyle araştırmaları yapılsa da gerçek düzeyde işletmelerin kullanımına yönelik yaklaşımların gündeme alınmadığı görülmüştür. Örneğin, sağlık sektöründe en fazla örneklerin görüldüğü FÖ modelleri sadece aynı özellikteki verileri öncelemiş, sağlık sektörünün diğer unsurlarını oluşturan işletme parametrelerini farklı özellikte olmalarından dolayı göz ardı etmiştir. Yapılan çalışmaların çoğu bilgisayar mühendisliği çerçevesinde kalmıştır. Bu çalışmanın en büyük katkısı önerdiğimiz yaklaşımın bilgisayar mimarisi seviyesinden bir iş modeli seviyesine indirgeyebilmesidir.

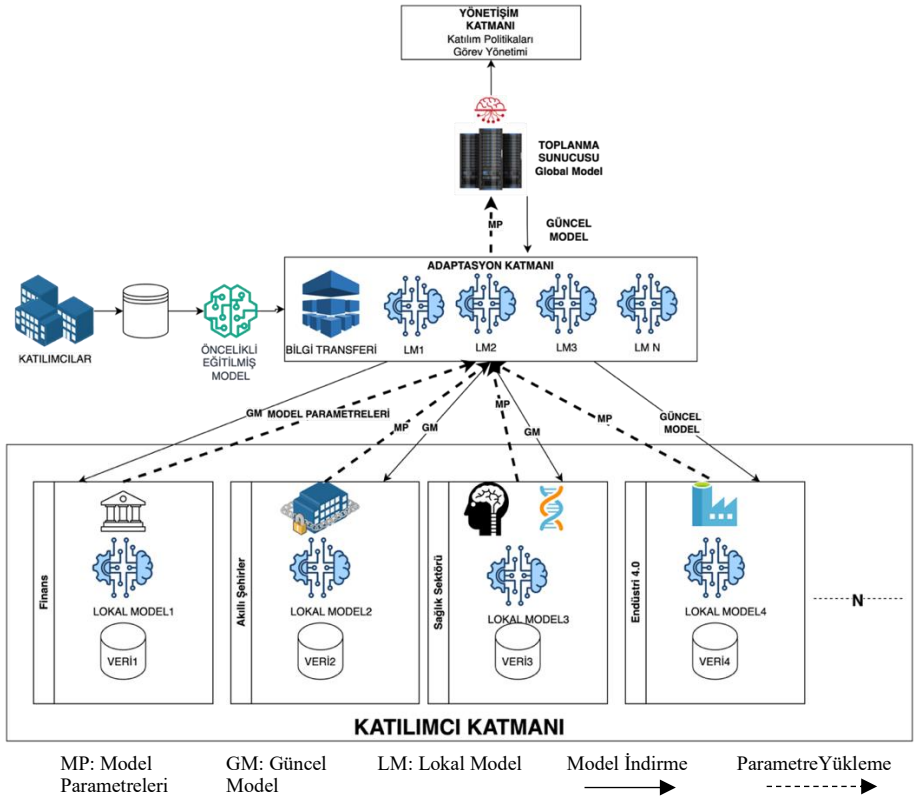
Çalışmanın araştırma sorusu çerçevesinde, işletmelerde farklı özellikteki verilerin YZ modellerinde kullanılabilmesi için önerilen çözüm Federe Transfer Öğrenimi (FT) yöntemidir. Bu yöntemde, önceden eğitilmiş bir kaynak model her katılımcıya dağıtılır, katılımcılar kendi yerel verileriyle bu modeli uyarlayarak hassas ayarlama yapar ve elde ettikleri güncellenmiş modelleri merkezi sunucuya gönderir. Merkezi sunucuda oluşturulan global model tekrar katılımcılara gönderilerek sürekli bir öğrenme döngüsü sağlanır. Böylelikle FT öğrenme yöntemi yalnızca heterojen veri problemini aşmakla kalmayıp, veri güvenliği ve gizliliğini koruyacaktır. Bu yöntemle önceden eğitilmiş modeller sayesinde maliyetlerin düşürülmesi, sektörler arası iş birliğinin teşvik edilmesi ve sürekli öğrenen dinamik kapasitenin yakalanması beklenmektedir.

Transfer öğreniminin temel amacı, farklı ortamlarda bulunan bilgiyi yeni bir alana aktarmak ve böylece alanlar arasındaki farklılıkları azaltmaktır. Özellikle örneklerin ve özelliklerin yeterince ortak olamadığı senaryolarda Federe Transfer Öğrenimi (FT) gündeme gelmektedir (Chen ve ark., 2020; Pouriyeh ve ark., 2022). Federe öğrenme, her katılımcıyı hem kaynak hem de hedef olarak gören; model parametrelerini merkezi sunucuda toplayarak bilgi alışverişini mümkün kılan bir yapıya sahiptir. Bu süreçte, yerel bir modelin transfer öğrenme aracılığıyla diğer katılımcılar tarafından da kullanılabilmesi sağlanır ve böylece veri heterojenliği, sistem farklılıkları, artırımlı veri ve etiket eksikliği gibi sınırlamalar önemli ölçüde azaltılır (Guo, Zhuang, ve ark., 2024).

Çalışma prensibinde, önceden eğitilmiş kaynak model tüm katılımcılara dağıtılır. Her katılımcı, yerel verilerini kullanarak bu modeli ilgili hedef doğrultusunda uyarlamakta, ardından güncellenmiş modeli merkezi sunucuya göndermektedir. Sunucuda iyileştirilmiş global model oluşturulduktan sonra, tekrar katılımcılara dağıtılarak sürekli öğrenen bir döngü sağlanmaktadır (Guo, Zhuang, ve ark., 2024; Putra ve ark., 2023; Zhang ve ark., 2024).

Bu yaklaşım, işletmelerin farklı özellikteki verilerini güvenli bir şekilde kullanarak YZ ve MÖ modellerinden faydalanmalarına imkân tanımaktadır. Şekil 4'te sunulan öneri modelimiz, sektör içi veya sektörel ilişkileri olan işletmelerin veri gizliliğini koruyarak ortak modeller geliştirmesini ve iş birliği kültürü oluşturmasını desteklemektedir. Böylelikle farklı sektörlerden gelen heterojen veriler, ortak konular çerçevesinde modellerde eğitilerek karar mekanizmalarına katkı sağlayabilmekte ve işletmelerin daha doğru sonuçlara ulaşmasına olanak tanımaktadır. Adaptasyon katmanında, önceden eğitilmiş modellerin minimum ortak gösterimler aracılığıyla paylaşılmış modellere uyumlaştırılması, global modelin yeniden eğitilmeye hazır hale gelmesini sağlamaktadır.

Sonuç olarak Şekil 4'de modelini sunduğumuz FT öğrenme yöntemi işletmelere; veri güvenliği, GDPR ve KVKK gibi kanunlara uyumluluk, kurumsal iş birliğinin gelişerek değişik sektörlerde benzer özellikteki sorunlara çözüm bulma, önceden eğitilmiş model sayesinde maliyeti azaltma, sürekli öğrenen modellerle dinamik kapasite kazanma avantajlarını sağlayacaktır.



Şekil 4. Önerilen Federe Transfer Öğrenme Çerçeve Modeli

4. SONUÇ VE ÖNERİLER

Günümüz iş modelleri statik bir yapıdan dinamik ve heterojen bir yapıya dönüşmüştür. Dijitalleşme ve dijital dönüşüm, işletmelerin yalnızca kendi konularıyla alakalı bilgileri edinmeleri, toplamaları, saklamaları ve işlemelerinin yeterli olmadığını göstermektedir. Dijital dönüşümü sağlamış ya da en azından işletmesini takip için kurumsal kaynak planlama (KKP) sistemlerini entegre etmiş firmalarda kullanılan ilişkisel veriler tek başına yeterli olmamaktadır. İlişkisel verilerle birlikte yapısal olmayan verilerin karar mekanizmalarına dahil edilmesi, sistemleri heterojen hale getirmektedir. Sadece verinin yapısı değil, miktarı da üstel hızla artmaktadır. Bu artış işletmelerin birçok veriyi kendi sunucularında ya da hizmet aldıkları sunucularda tutması, ilaveten bulut sistemlerinin devreye girmesiyle verilerin farklı ülkelerde tutulmasına olanak sağlamaktadır. Bu durumda veri güvenliği ile kişisel ve kurumsal gizliliğin korunması kritik bir ihtiyaç haline gelmiştir. Özellikle de sağlık ve finans sektörlerinde veri güvenliği ülke bazında korunması gereken milli bir varlık olarak görüldüğünden ülke dışında tutulması yasaklanmıştır. Son yıllarda YZ kullanımının artması, halka açık geniş dil modellerinin entegre edilmesi, kişisel ve kurumsal olarak biriktirilen tüm verileri hedef haline getirmiştir. YZ'nin sağladığı katkılar hem kişisel hayat için hem de iş hayatı için yadsınamaz haldedir. Ancak biriktirilen her verinin YZ'nin kullanım alanına girmesi tüm kurumları ve ülkeleri tedbir almaya itmiştir. Kanunlarla gizliliğin korunması bir tedbir oluşturduğu gibi birçok kısıtı da beraberinde getirmektedir. Ortak çalışan, belli konularda iş birliği yapması gereken ve fakat farklı verilere sahip olan işletmelerin ortak karar alma ve strateji geliştirme olanakları kanunlarla düzenlenmiştir. Rekabetin teknolojiyle kızıştığı bir ortamda hem kişisel hem de işletmelerin ortak problemlerine YZ ve benzeri teknolojilerle çözüm bulunması gerekmektedir. Örneğin, tekstil ve imalat sektöründe çalışanların karşılaştıkları kanser hastalıklarının değerlendirilmesi, finansal yapıların analiz edilerek gelecek tahminlerinin yapılması veya ortak yatırımlar için öngörü geliştirilmesi gibi vakalarda, klasik veri güvenliği yöntemleri bu karmaşık yapılarda YZ modeli kurmayı zorlaşmaktadır. İş performansının ölçüldüğü, sistemlerin gözlemlendiği ve çalışanların yüz ifadelerinden yorgunluklarının tahmin edildiği karmaşık sistemlerde çözümler oluşturulmaya çalışılmaktadır (X. Li ve ark., 2021). İşte bu noktada çalışmadaki FT öğrenme yöntemi önerisi, farklı yapıların beraber çalışmasıyla ortak problemlerini veri paylaşımı yapmadan model halinde eğiterek, farklılıklarını önceden eğitilmiş bir modelle uyumlaştırarak spesifik ihtiyaca dönük bir model halinde çözümlenebileceği görülmüştür (Chen ve ark., 2020; Guo, Wang, ve ark., 2024; X. Li ve ark., 2021). Farklı üretim ortamlarında yapılan performans değerlendirmeleri, sonrasında katılımcıya özgü bilginin transferiyle model üretimi ve FT öğrenmenin katılımcıların kendi üretim performanslarını iyileştirmedeki etkisi (Guo ve ark., 2024), çalışmamızın gerekliliğini literatür desteğiyle göstermektedir. Ancak Türkiye'de özellikle işletme performanslarının daha iyi hale getirilmesinde böyle bir çalışmanın olmaması, önerdiğimiz çerçeve modelinin Türkiye şartlarında test edilmesini gerekli kılmaktadır. Yaptığımız çalışma, %95 seviyesinde KOBİ özelliği gösteren ülkemizde FT öğrenmenin sağladığı veri güvenliğiyle ülkemiz içerisindeki tecrübe birikimini ortak payda da buluşturabileceği gösterir. Her bir KOBİ, ortak sorunlarından türetilerek eğitilmiş modeli alıp kendi ihtiyaçlarına göre bilgi transferiyle lokal modellerini güncellediğinde; bu durum modellerini olgunlaştırmanın yanı sıra karar verme, analiz ve performans ölçümünde daha doğru sonuçlara ulaşmalarını sağlayacaktır. İşletmelerin kollektif birçok verinin eğittiği modellerle kendi modellerini

olgunlaştırmaları, veri güvenliğini standartlar dahilinde korumaları uluslararası bağlamda işletmelere stratejik üstünlük elde etmesini sağlayacaktır. Ayrıca GDPR ve KVKK gibi kurallara FT öğrenmeyle teknik çözüm önermenin yanında, mahremiyet etki değerlendirmesinin FT öğrenmeye entegre edilmesiyle veri toplama, işleme ve model güncelleme aşamalarında ortaya çıkabilecek gizlilik risklerinin sistematik bir biçimde yönetilmesi sağlanabilir (Metin ve ark., 2019). Buda veri için bütüncül bir koruma sağlayacaktır. İleri teknoloji ve YZ'nin birleşmesiyle, FT öğrenmenin KOBİ'ler için kullanılması, Sanayi ve Teknoloji Bakanlığının koordinasyonunda ulusal ölçekte bir proje çıktısına dönüşebilir. Tüm ülke genelinde böylelikle kaynakların verimli kullanımı sağlanmış olur. Uluslararası bağlamda bakıldığında, yapılan akademik makale analizlerinden de görüldüğü üzere konunun yeni olması, Türkiye dışındaki örneklerin de az olduğunun göstergesidir. Elbette bu yöntemlerin sınırlıkları mevcuttur. Bunların aşılması için işletmelerin ve FT öğrenme konusundaki bilimsel çalışmaların ortak olarak yürütülerek gerçek veri setleriyle pratik hale getirilmesi başarının temel şartıdır.

Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

KAYNAKÇA

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys*, *51*(4). https://doi.org/10.1145/3214303

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1017/9781108943321

Al-Rubaie, M., & Chang, J. M. (2019). Privacy-Preserving Machine Learning: Threats and Solutions. *IEEE Security and Privacy*, *17*(2), 49–58. https://doi.org/10.1109/MSEC.2018.2888775

Barker, K., Askari, M., Banerjee, M., Ghazinour, K., MacKas, B., Majedi, M., Pun, S., & Williams, A. (2009). A data privacy taxonomy. *Lecture Notes in Computer Science (subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5588 LNCS*, 42–54. https://doi.org/10.1007/978-3-642-02843-4_7

Baumeister, R. F., & Leary, M. R. (1997). Writing narrative literature reviews. *Review of General Psychology*, *1*(3), 311–320. https://doi.org/10.1037/1089-2680.1.3.311

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *Proceedings - IEEE Symposium on Security and Privacy*, 459–474. https://doi.org/10.1109/SP.2014.36

Briggs, C., Fan, Z., & Andras, P. (2020). Federated learning with hierarchical clustering of local updates to improve training on non-IID data. *Proceedings of the International Joint Conference on Neural Networks*. https://doi.org/10.1109/IJCNN48605.2020.9207469

Bunz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short Proofs for Confidential Transactions and More. *Proceedings - IEEE Symposium on Security and Privacy*, *2018-May*, 315–334. https://doi.org/10.1109/SP.2018.00020

Chamikara, M. A. P., Bertok, P., Khalil, I., Liu, D., & Camtepe, S. (2021a). PPaaS: Privacy Preservation as a Service. *Computer Communications*, *173*(December 2020), 192–205. https://doi.org/10.1016/j.comcom.2021.04.006

Chamikara, M. A. P., Bertok, P., Khalil, I., Liu, D., & Camtepe, S. (2021b). Privacy preserving distributed machine learning with federated learning. *Computer Communications*, *171*(April 2020), 112–125. https://doi.org/10.1016/j.comcom.2021.02.014

Chen, Y., Qin, X., Wang, J., Yu, C., & Gao, W. (2020). FedHealth: A Federated Transfer Learning Framework for Wearable Healthcare. *IEEE Intelligent Systems*, *35*(4), 83–93. https://doi.org/10.1109/MIS.2020.2988604

Dülger, M. V. (2021). Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti (Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti. *Ssrn*, *1*(2), 43–80. https://ssrn.com/abstract=3792208%0Ahttp://dx.doi.org/10.2139/ssrn.3792208

Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, *9*(3–4), 211–487. https://doi.org/10.1561/0400000042

European Parliament & Council of the European Union. (2016). General Data Protection Regulation. *Official Journal of the European Union*, *2014*(March 2014).

Fano, R. M. (1968). The balance of knowledge and the balance of power. *Scientific American*, *218*(5), 149–152.

Giancaspro, M. (2017). Is a 'smart contract' really a smart idea? Insights from a legal perspective. *Computer Law and Security Review*, *33*(6), 825–835. https://doi.org/10.1016/j.clsr.2017.05.007

Guo, W., Wang, Y., Chen, X., & Jiang, P. (2024). Federated transfer learning for auxiliary classifier generative adversarial networks: framework and industrial application. *Journal of Intelligent Manufacturing*, *35*(4), 1439–1454. https://doi.org/10.1007/s10845-023-02126-z

Guo, W., Zhuang, F., Zhang, X., Tong, Y., & Dong, J. (2024). A comprehensive survey of federated transfer learning: challenges, methods and applications. *Frontiers of Computer Science*, *18*(6). https://doi.org/10.1007/s11704-024-40065-x

Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential Privacy Techniques for Cyber Physical Systems: A Survey. *IEEE Communications Surveys and Tutorials*, *22*(1), 746–789. https://doi.org/10.1109/COMST.2019.2944748

Kardaş, S., & Kiraz, M. (2018). Bitcoin'DMahremiyeti SağlamaYöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(1), 1–9. https://doi.org/10.18640/ubgmd.429461

Keshk, M., Turnbull, B., Moustafa, N., Vatsalan, D., & Choo, K. K. R. (2020). A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks. *IEEE Transactions on Industrial Informatics*, *16*(8), 5110–5118. https://doi.org/10.1109/TII.2019.2957140

Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine*, *158*(April), 106848. https://doi.org/10.1016/j.compbiomed.2023.106848

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, *37*(3), 50–60. https://doi.org/10.1109/MSP.2020.2975749

Li, X., Chi, H. lin, Lu, W., Xue, F., Zeng, J., & Li, C. Z. (2021). Federated transfer learning enabled smart work packaging for preserving personal image information of construction worker. *Automation in Construction*, *128*(January), 103738. https://doi.org/10.1016/j.autcon.2021.103738

Liu, L., Zhang, J., Song, S. H., & Letaief, K. B. (2020). Client-Edge-Cloud Hierarchical Federated Learning. *IEEE International Conference on Communications*, *2020-June*. https://doi.org/10.1109/ICC40277.2020.9148862

Marijan, D., & Lal, C. (2022). Blockchain verification and validation: Techniques, challenges, and research directions. *Computer Science Review*, *45*, 100492. https://doi.org/10.1016/j.cosrev.2022.100492

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, *54*, 10.

Metin, B., Erkan, S., Atasu, İ., & Yılmaz, E. (2019). Privacy Impact Assessment as a Tool for GDPR Compliance Preparation. *Kişisel Verileri Koruma Dergisi*, *1*(2), 75–86.

Mulligan, D. K., Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083). https://doi.org/10.1098/rsta.2016.0118

Nissim, K., & Wood, A. (2018). Is privacy privacy? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128).

Oktay, E. (2022). *Genomik Çalişmalarda Kullanilan Makine Öğrenmesi Modellerinin Blokzincir Temelli Bir Eko Sistemde Federe Öğrenme Yöntemiyle Geliştirilmesi İçin Kavramsal Bir Çalişma*. Istanbul Medeniyet Üniversitesi.

Özcandan, N., Kalkar, Ö., Bingöl, M. A., Sertaya, İ., Dursun, T., Yıldız, O., & Türk, E. (2020). *Blokzincirlerde Güvenlik ve Mahremiyet*.

Pouriyeh, S., Shahid, O., Parizi, R. M., Sheng, Q. Z., Srivastava, G., Zhao, L., & Nasajpour, M. (2022). Secure Smart Communication Efficiency in Federated Learning: Achievements and Challenges. *Applied Sciences (Switzerland)*, *12*(18). https://doi.org/10.3390/app12188980

Putra, M. A. P., Rachmawati, S. M., Abisado, M., & Sampedro, G. A. (2023). HFTL: Hierarchical Federated Transfer Learning for Secure and Efficient Fault Classification in Additive Manufacturing. *IEEE Access*, *11*, 54795–54807. https://doi.org/10.1109/ACCESS.2023.3280471

Ram Mohan Rao, P., Murali Krishna, S., & Siva Kumar, A. P. (2018). Privacy preservation techniques in big data analytics: a survey. *Journal of Big Data*, *5*(1). https://doi.org/10.1186/s40537-018-0141-8

Shin, D. D. H. (2019). Blockchain: The emerging technology of digital trust. *Telematics and Informatics*, *45*(August). https://doi.org/10.1016/j.tele.2019.101278

Solove, D. J. (2008). Understanding Privacy. Massachusetts: Harvard University Press.

Türkiye Büyük Millet Meclisi (T.B.M.M). (2016). Kişisel verilerin korunmasi kanunu. *Resmi Gazete*, 12301–12317.

Zhang, Z., Ming, Y., & Wang, Y. (2024). A federated transfer learning approach for surface electromyographic hand gesture recognition with emphasis on privacy preservation. *Engineering Applications of Artificial Intelligence*, *136*(PA), 108952. https://doi.org/10.1016/j.engappai.2024.108952

Zheng, G., Kong, L., & Brintrup, A. (2023). Federated machine learning for privacy preserving, collective supply chain risk prediction. *International Journal of Production Research*, *61*(23), 8115–8132. https://doi.org/10.1080/00207543.2022.2164628

Zhou, X., Ye, X., Wang, K. I. K., Liang, W., Nair, N. K. C., Shimizu, S., Yan, Z., & Jin, Q. (2023). Hierarchical Federated Learning With Social Context Clustering-Based Participant Selection for Internet of Medical Things Applications. *IEEE Transactions on Computational Social Systems*, *10*(4), 1742–1751. https://doi.org/10.1109/TCSS.2023.3259431