Dicle University
Journal of Engineering
https://dergipark.org.tr/tr/pub/dumf
duje.dicle.edu.tr

Derleme Makalesi/Review Article

İşbirlikçi Yapay Zeka Konsepti: Federe Öğrenmeye Genel Bir Bakış

Collaborative Artifical Intelligence Concept: Federated Learning Review

Mehmet Nergiz[1*]

[1] Dicle Üniversitesi, Bilgisayar Mühendisliği Bölümü, mnergiz@dicle.edu.tr
ORCID: https://orcid.org/0000-0002-0867-5518

MAKALE BİLGİLERİ

Makale Geçmişi:

Geliş 14 Haziran 2022
Revizyon 17 Haziran 2022
Kabul 24 Haziran 2022
Online 28 Haziran 2022

Anahtar Kelimeler:

Federe Öğrenme, Merkezi Öğrenme, Dağıtık Öğrenme, Büyük Veri, Veri gizliliği, Makine Öğrenmesi

ÖZ

Yapay zeka (YZ) gücünü büyük veriden almaktadır. Ancak büyük veriye ulaşmak ve bu veriyi işlemek, gerek gizlilik, gerekse büyük verinin işlenmesi için gereken donanımsal ihtiyaçlardan ötürü her zaman mümkün olamayabilmektedir. Federe öğrenme (FÖ); bahsi geçen gizlilik & büyük veri ikilemini çözebilmek adına önerilen yeni bir konsepttir. FÖ, ortak bir YZ model parametrelerinin katılımcılar üzerinde güncellenmesi ve güncellenen parametrelerin koordinatör vasıtasıyla birleştirilmesini gerçekleştiren, bunu yaparken de veri gizliliğini koruyan bir çerçevedir. FÖ, mimarisi gereği veri gizliliği korunurken aynı zamanda iş yükü de paylaştırılmış olur. Ayrıca katılımcı sayısı açısından ölçeklenebilirlik ile beraber kimi problemlerde daha yüksek başarım oranı, daha düşük çalışma süreleri gibi avantajlar da sunar. İşbirliği yapan katılımcıların öznitelik ve örnek uzaylarının ne ölçüde ortak olduğuna bağlı olarak yatay, dikey ve transfer FÖ yaklaşımları mevcuttur. Makine öğenmesi yöntemlerinin kullanıldığı ve veri gizliliğinin önem arz ettiği her alanda FÖ kullanım alanı bulmaktadır. Sağlık hizmetleri, nakliye sektörü, finansal teknolojiler ve doğal dil işleme alanları yatay FÖ konseptinin kullanıldığı alanların başında gelmektedir. Öte yandan, dikey ve transfer FÖ konseptleriyle sektörler arasında YZ bazlı işbirlikleri geliştirilebilmektedir.

ARTICLE INFO

Article history:

Received 14 June 2022
Received in revised form 17 June 2022
Accepted 24 June 2022
Available online 28 June 2022

Keywords:

Federated Learning, Centralized Learning, Distributed Learning, Big Data, Data Privacy, Machine Learning

Doi: 10.24012/dumf.1130789

* Sorumlu Yazar

ABSTRACT

Artificial intelligence (AI) draws its power from big data. However, accessing and processing big data may not always be possible due to both confidentiality and hardware requirements for high computational performance. Federated learning (FL) is a new concept proposed to solve the aforementioned privacy & big data dilemma. FL is also a framework that performs updating of the parameters of a common AI model trained by the different participants and then combining the updated parameters through the coordinator while protecting data privacy. Due to the modular design of the FL concept, the workload is shared among the participants while protecting data privacy. It also provides advantages like scalability in terms of collaborator count and higher performance and lower execution time for some sort of problems. Depending on the similarity of the feature and sample spaces of the collaborators, there are some FL approaches such as horizontal, vertical and transfer. FL is applicable to any field in which machine learning methods are utilized and the data privacy is an important issue. Healthcare services, transportation sector, financial technologies and natural language processing are the prominent fields where horizontal FL concept is applied. On the other hand, AI-based collaborations between the sectors can be developed with vertical and transfer FL concepts.

Giriş

Teknolojik gelişimlere paralel olarak finans, sağlık, eğitim, alışveriş, iletişim gibi hayatın her alanında dijital ortamlarda devasa boyutlarda veri üretilmektedir. Üretilen bu veriler Yapay Zekâ teknolojilerinin hammaddesini oluşturmaktadır. Yapay Zekâ teknolojileri, siber güvenlik [1], otonom araçlar [2], hastalık teşhisi [3], uzaktan eğitim [4], çeşitli zaman serisi tahmin sistemleri gibi birçok stratejik alanda kullanılırken büyük verilere ihtiyaç duymaktadır. Geleneksel merkezileştirilmiş öğrenme, yerel cihazlardan toplanan tüm verilerin bir veri merkezinde veya bulut sunucusunda depolanmasını gerektirir. Bu gereklilik yalnızca gizlilik riskleri ve veri sızıntısı endişesini artırmakla kalmaz, aynı zamanda veri miktarı çok büyük olduğunda büyük depolama alanları ve yüksek kapasiteli işlemci gibi ihtiyaçları doğurur. Birden çok makinenin farklı veri gruplarıyla bir model replikasını paralel olarak eğitmesini sağlayan dağıtık öğrenme [5], depolama ve hesaplama kapasitesi sorununa potansiyel bir çözüm olarak hizmet etse de, veriyi önceden bölmek için tüm eğitim verilerine erişmesi gerekir.

Buna karşın veri gizliliği bakımından kişisel ve toplumsal hassasiyet artmaktadır. Dünya üzerinde birçok kurum verisini stratejik, hukuki ve ticari kaygılar sebebiyle paylaşmamaktadır. 2018 'de Facebook 'ta veri tabanlarından birçok kişisel verinin çalınması hadisesinin tetiklemesi ile Avrupa Birliği Genel Veri Koruma Tüzüğü'nde [6] yer almıştır. Böylece, kişisel veri gizliliği kanuni bir zemine oturtulmuştur. Tüzüğe göre herhangi bir kurum veya kuruluş, anlaşmaları olmadıkça, kullanıcının kendi verilerini kullanma yetkisine sahip değildir.

Yukarıda bahsi geçen, büyük veriye erişim & veri gizliliği ikileminden esinlenerek Google Yapay Zekâ ekibi 2016 'da, dağıtık ve gizliliği koruyan Federe Öğrenme (FÖ) [7] konseptini önermiştir. FÖ konsepti veri gizliliğini korurken aynı zamanda mimari yapısından ötürü iş yükünü de dağıtmış olur.

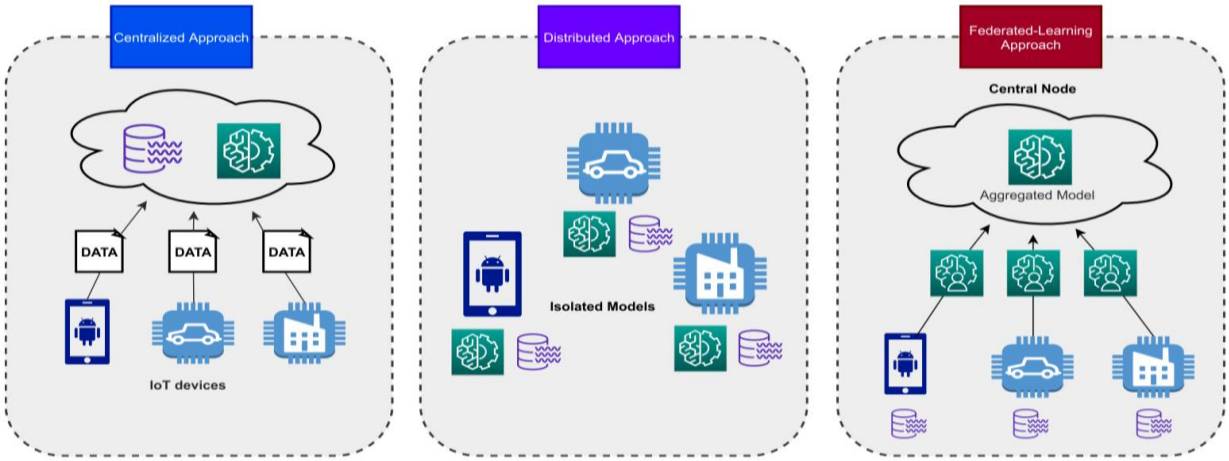
Literatüre kazandırıldığı günden beri FÖ konsepti gelişmekte ve araştırmacılar için oldukça geniş bir çalışma alanı sunmaktadır. Dünya çapında FÖ konsepti ile ilgili olarak araştırmacılar tarafından her yıl yüzlerce çalışma yapılmaktadır. Ancak gelişime son derece açık olan FÖ konseptine, ülkemizde yeterince ilgi gösterilmediği gözlemlenmektedir. Bu derleme Türkçe akademik yayın literatürüne öncü bir kaynak olması maksadıyla hazırlanmıştır.

Makalenin geri kalan kısmında ilk olarak Merkezi öğrenme, Dağıtık Öğrenme ve FÖ karşılaştırmalı şekilde sunulmuştur. Sonra FÖ'nün temel dinamikleri ve avantajlarından bahsedilmiş ve FÖ'nün temel bileşenleri ele alınmıştır. Sonrasında FÖ senaryoları tanıtılmış ve son olarak FÖ'nün kullanım alanları sunularak makale sonlandırılmıştır.

Merkezi Öğrenmeden Dağıtık Öğrenmeye, Dağıtık Öğrenmeden FÖ'ye

Yapay Zekâ, gelişim sürecinde zaman zaman popülaritesini yitirmiş olsa da son yıllarda yaşanan gelişmeler ile tekrardan ilgiyi üzerine çekmiştir. 2012 yılında yapılan 2012 ILSVRC ImageNet Büyük Ölçekli Görsel Tanıma yarışmasında AlexNet [8] derin öğrenme mimarisi birinci olmuştur. Örüntü tanımada hata oranını %26'lardan %15'lere indirgemiştir. Öte yandan yapay zekâ programı ile Derin Öğrenme 2016 yılında dünyadaki en profesyonel Alpha Go oyuncusunu yenmiştir. Bu sıra dışı deneyimin başarısının temelinde yapay zekanın 28,6 milyar adet örnek satranç hamlesi verisinin kullanılması vardır. Bu gelişmeler ile yapay zekanın büyük veri ile eğitilmesinin model başarımına doğrudan katkı sağladığı kanıtlanmıştır [9].

Ancak yapay zekânın başarısı için gerekli olan devasa verinin okunması, veri ön işlemlerinin yapılması ve model eğitimi süreçlerinin sürdürülmesi devasa veri depoları ve yüksek kapasiteli işlemciler gerektirir [9]. Verilerin merkezi bir lokasyonda toplanmasının zorlukları ve yüksek donanımsal maliyetlerden dolayı ilerleyen zamanlarda Derin Öğrenme modelleri, Dağıtık donanımsal kaynaklar aracılığıyla uygulanmıştır. Dağıtık Öğrenmenin avantajlarından faydalanılarak yapay zekâ modelleri daha hızlı gelişim imkânı bulmuştur.



Şekil 1. Merkezi, Dağıtık ve FÖ yaklaşımları [10]

Buna karşın, Dağıtık Öğrenme bu avantajları sağlarken veri gizliliğini ihlal etmektedir. Çünkü Dağıtık Öğrenmede, verilerin merkezi bir sunucu tarafından organize edilebilmesi için tüm verinin sunucunun erişimine sunulması gerekmektedir.

İlk olarak 2016 'da Google yapay zekâ ekibi tarafından literatüre kazandırılan FÖ'de ise Merkezi ve Dağıtık Öğrenmeden farklı olarak veri gizliliği ihlal edilmeden bir model eğitim süreci sürdürülmektedir. İşbirlikçi ' sürecine katılan bir katılımcı, verisini paylaşmazken koordinatör bir sunucu tarafından paylaşılan ortak bir modeli kendi gizli verisi ile kendi kaynaklarını kullanarak eğitir. FÖ konsepti ile eğitilen modeller daha yetkin ve hataya dayanıklıdır. Modeli eğitme süreci, iş birliğine katılan cihazlar veya kuruluşlar üzerinde yapıldığından ağdaki yükü azaltır. Ayrıca modeli eğitmek için gereken güç tüketimi de geleneksel yaklaşımlardan daha azdır.

FÖ

Şekil 2 'de görüleceği üzere temel FÖ konsepti [11] 4 adımdan oluşur:

1. İşbirlikçiler global modeli indirir.
2. Her işbirlikçi, indirilen global modeli kendi özel verileriyle eğitmesi sonucu model parametreleri güncellenir.
3. İşbirlikçiler, güncellenen model parametrelerini koordinatöre gönderir.
4. Koordinatör, güncellenen parametreleri belirli algoritmalar kullanarak birleştirir.

Bu döngü model yakınsayana kadar devam eder.

FÖ'nün geleneksel yöntemlere göre aşağıdaki gibi bazı avantajları vardır [12]:

Ölçeklenebilirlik: FÖ, model parametrelerinin güncellenmesi aracılığıyla farklı cihazların birbirinden öğrenmesini sağlayarak tüm ağı ölçeklenebilir hale getirir.

Düşük iş hacmi ve yüksek gecikme süresi zorluklarına çözüm: Yerel modeller oluşturmak, tek bir merkezi modeli eğitmeye kıyasla gecikmelerin ve güç tüketiminin azaltılmasına yardımcı olur.

Doğruluğu artırır: FÖ modelleri, birçok yerel modelin bir araya getirilmesi yoluyla eğitildiklerinden ve verilere aynı anda farklı perspektiflerden yaklaştığından, merkezi olarak eğitilen modellerden daha fazla tecrübe paylaşımını sağlar. Böylece model doğruluğuna çoğunlukla olumlu katkıda bulunurlar.

Eğitim süresinde ve eğitim maliyetinde azaltma: Bir modeli merkezi olarak eğitmek yerine, çeşitli yerel modelleri eğitmek ve ardından merkezi global bir model oluşturmak daha az zaman alan bir süreçtir. İş yükü iş birliğindeki katılımcılara dağıtıldığından eğitim maliyeti de daha düşüktür.

Gizliliği ve güvenlik: Eğitim verileri iş birliğine katılan katılımcıdan ayrılmadığından, tüm hassas bilgiler yerelde kalır, böylece kişisel verilerin gizliliği ve güvenliği sağlanır.

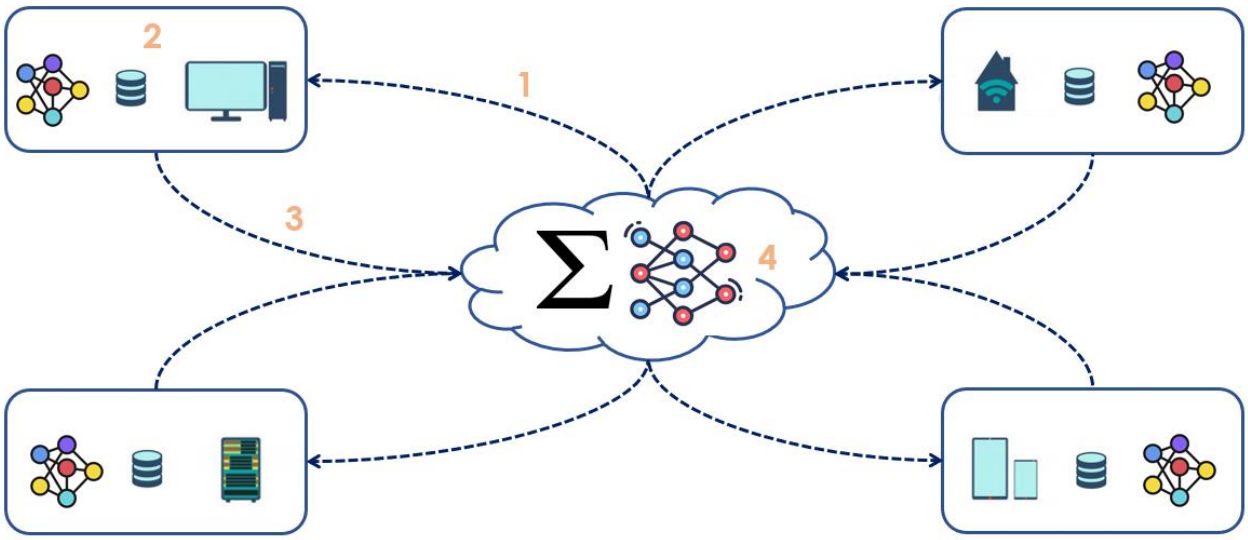
Veri minimizasyonu: FÖ, yalnızca öğrenilen modelin merkezi olarak işlenmesini ve ham verilerin gizli kalmasını sağlayarak veri minimizasyon ilkesini kullanır. Ayrıca gönderilen modeller geçicidir ve global modelle birleştikleri anda boşa çıkarlar.

FÖ'nün Bileşenleri

FÖ konseptinin 3 temel bileşeni vardır.

Katılımcılar

Bir FÖ konseptindeki veri sahipleri ve iş birliğinden faydalanan işbirlikçilerdir [13]. Kullanılacak olan yapay zekâ modeli katılımcılar üzerinde eğitilir. Katılımcıların donanımsal özellikleri [14], konsepte katılan katılımcı sayıları ve iş birliğine katılma kararlılığı [15], katılımcılar üzerindeki verinin dağılımı [11] konseptin başarısına direk olarak etki eden faktörlerdir ve FÖ'nün zorlukları olarak araştırmaya açıktır.



Şekil 2. FÖ'nün Temel Adımları

Koordinatör

Genellikle güçlü donanımsal özelliklere sahip bir merkezi sunucudur. Sunucunun güvenilirliği konseptin en önemli zorluklarındandır. Öte yandan Merkeziyetsiz FÖ konseptinde koordinatöre ihtiyaç duyulmaz. Ancak bu konseptte de yüksek iletişim maliyetleri söz konusudur [16].

İşlem ve İletişim Çerçevesi

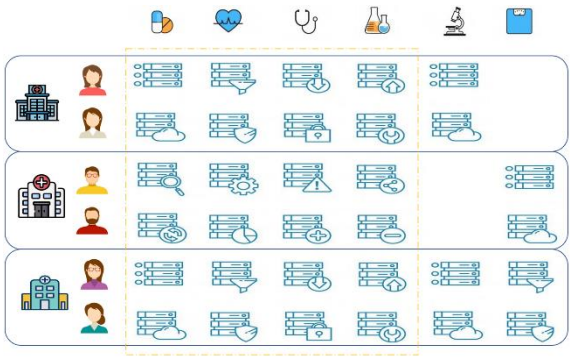
FÖ konseptinde, işlemler katılımcılar ve koordinatör üzerinde gerçekleşirken, iletişim katılımcılar ile koordinatör arasında gerçekleşir. İşlemlerin amacı model eğitimi için, iletişimin amacı katılımcılardan gelen model parametrelerinin birleştirilerek ortak yeni bir model elde edilmesi içindir. En temel ve kullanımı en yaygın olan FedAVG 'dir [7]. Ayrıca FedAVG dışında kullanılan başka model birleştirme stratejileri vardır [17]. FedAVGM, FaultTolerantFedAvg, FedOpt, FedAdagrad, FedAdam ve FedYogi bunlardan bazılarıdır. FedAVGM stratejisi, klasik FedAvg yöntemine sunucu momentumunun eklenmesi ile geliştirilmiştir. FaultTolerantFedAvg ise normal FedAVG'ye ek olarak model birleştirme aşamasına eksik katılım gösteren katılımcıların olması durumunda bu eksikliği tolere ederek o an hazırda var olan katılımcılarla model birleşimini gerçekleştirir. FedOpt, FedAdagrad, FedAdam ve FedYogi stratejileri de model birleşimi aşamasında server tarafındaki adaptif optimizasyon algoritmaları uygulamaktadırlar. Bu alan yeni ve güncel bir araştırma alanıdır [18].

FÖ'nün Sınıflandırılması

FÖ Konseptinde kullanılacak olan yönteme karar verebilmek için işbirlikçilerin öznitelik veya örnek uzayının hangisinde ortak noktalarının olduğunun tespit edilmesi gerekir. Bu açıdan bakınca FÖ'yü veri dağılımı bakımından; Yatay FÖ, Dikey FÖ ve Federe Transfer Öğrenme olmak üzere 3 sınıfa ayırabiliriz [19].

Yatay FÖ

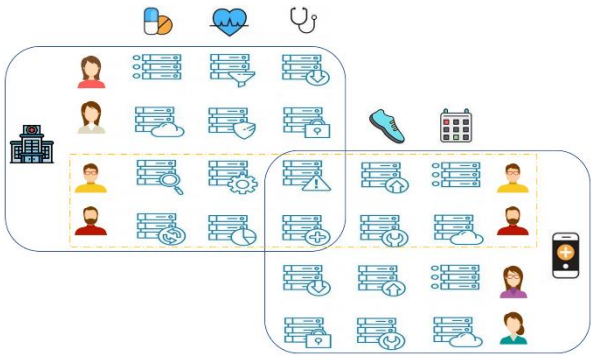
Yatay FÖ, verilerin aynı öznitelik uzayına ancak ayrı örnek uzayına sahip olduğu senaryoda kullanılır. Buna örnek olarak: Farklı şehirlerde konumlanan N adet farklı hastanenin, bireylerin sağlık durumlarını takip etmek için ortak bir model oluşturma niyetinde olduklarını düşünelim. Şekil 3 'te de görüleceği üzere bu durumda hastanelerin hastaları tamamen farklı iken, yapılan tahliller, kullanılan ilaçlar, muayene raporları, kronik rahatsızlıkları gibi bilgiler ortak öznitelikler olacaktır. Böyle bir senaryoda ortak bir model oluşturmak için birinci bölümde bahsedilen merkezi veya dağıtık öğrenme modelleri uygulanabilir. Ancak hasta mahremiyetinin korunması gerekliliği nedeniyle taraflar veri paylaşımından kaçınmaktadır. Böyle bir senaryoda öznitelik uzayının aynı, örnek uzayının farklı olduğu yatay FÖ konsepti kullanılarak hasta mahremiyeti ihlal edilmeden ortak model oluşturulabilir.



Şekil 3. Yatay FÖ'de örnek uzayı ile öznitelik uzayı çakışması

Dikey FÖ

Dikey FÖ, aynı örnek uzayına ancak ayrı öznitelik uzayına sahip olma senaryosunda kullanılır. Buna örnek olarak: Şekil 4 'teki gibi, bir ülkedeki yaygın kurumsal bir hastane ve bu hastaneden bağımsız bir mobil sağlık uygulaması olduğunu varsayalım. Ve aynı anda bu hastanelerden ve mobil sağlık uygulamasından hizmet alan ortak bireyler olduğunu varsayalım. Böyle bir senaryoda dikey FÖ konseptinden faydalanılarak bireylere beslenme programı öneren bir uygulama üretilebilir.



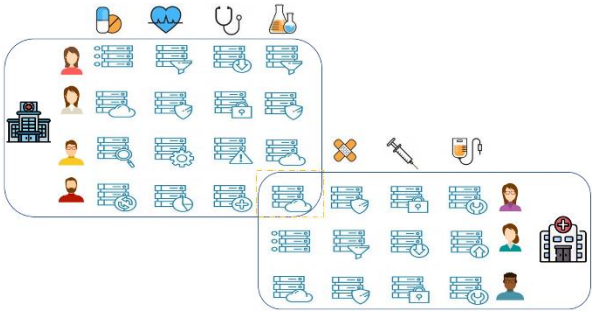
Şekil 4. Dikey FÖ'de örnek uzayı ile öznitelik uzayı çakışması

Federe Transfer Öğrenme

Yatay ve Dikey FÖ'deki senaryoların aksine, çoğu durumda, veriler ne örnek uzayını ne de öznitelik uzayını paylaşır. Transfer öğrenme, bu duruma uygun daha iyi öğrenme sonuçları elde etmek için bir alandaki bilgi birikimini başka bir alana taşımayı sağlar.

Şekil 5'te gösterildiği üzere, bir hastanedeki bazı hastalık tanı ve tedavi bilgileri, Federe Transfer Öğrenme ile diğer hastalıkların teşhisine yardımcı olmak için başka bir hastaneye aktarılabilir. Federe Transfer Öğrenme modeli henüz tam olarak olgunlaşmamıştır, bu nedenle farklı veri yapılarıyla daha esnek hale getirmek için hala bolca araştırma alanı vardır. Veri adaları ve gizlilik koruma sorunları, makine öğreniminin endüstriyel alandaki kullanımında karşılaşılan, önde gelen sorunlardandır. Bununla birlikte, Federe Transfer Öğrenme, veri

adalarının engellerini aşarken hem veri güvenliğini hem de kullanıcı gizliliğini korumanın etkili bir yoludur.



Şekil 5. Federe Transfer Öğrenmede örnek uzayı ile öznitelik uzayı çakışması

FÖ'nün Kullanım Alanları

Sağlık Hizmetleri

Tahlil sonuçları, biyomedikal görüntüler, aşı durumu gibi elektronik sağlık kayıtları, makine öğrenimi uygulamaları için sağlık verilerinin ana kaynağı olarak kabul edilir [20]. Makine öğrenimi modelleri yalnızca tek bir hastanede bulunan sınırlı veriler kullanılarak eğitilirse, tahminlerde bir miktar yanlılık ortaya çıkabilir. Bu nedenle, modelleri daha genellenebilir bir seviyeye getirebilmek için, kuruluşlar arasında veri paylaşımı aracılığıyla veriyi arttırarak yapay zekâ modelinin eğitimini gerçekleştirmek gerekmektedir. Ancak sağlık verilerinin hassas yapısı nedeniyle, hastaların elektronik sağlık kayıtlarının hastaneler arasında paylaşılması mümkün olmayabilir. Bu gibi durumlarda, FÖ, sağlık hizmetleri verileri için işbirlikçi bir öğrenme modeli oluşturmak adına iyi bir seçenek olarak hizmet edebilir. Literatürde sağlık alanında FÖ tabanlı Çok Katmanlı Algılayıcılar [21], Evrişimsel Sinir Ağları [22], Oto Kodlayıcı [23] modelleri ile araştırmalar yapılmıştır.

Nakliye

Araç ağlarında sensörlerin artmasıyla, özellikle de otonom araçların yaygınlaşması ile bu alanda daha fazla veri kullanabilmek ve Makine Öğrenimi modellerini eğitmek mümkün hale gelmiştir. Makine Öğrenimi tabanlı modeller genellikle hem araç yönetimine hem de trafik yönetimine uygulanır [24]. Mevcut otonom sürüş modelleri eğitimin yapıldığı konumun dinamik doğası ile sınırlıdır. FÖ ile farklı coğrafi konumlardan çevrimiçi eğitim araçlarıyla daha doğru modeller dizayn edilebilir. Benzer şekilde trafik akışı tahmin teknikleri için de büyük miktarda veri gereklidir, ancak verilerin çoğu çeşitli kuruluşlar arasında bölünmüştür ve gizliliği korumak için değiş tokuş edilemez [25]. Bu tür durumları da ele almak için FÖ yöntemlerini uygulayabiliriz. Literatürde FÖ tabanlı otonom sürüş [26], akıllı ulaşım sistemleri [27] üzerine yapılmış araştırmalar mevcuttur.

Finans

Finansta FÖ'nün en iyi kullanımı, kredi riski değerlendirmesi için bankacılık sektöründedir [28]. Normalde bankalar, merkez bankalarından gelen kredi kartı raporlarını kullanan müşterileri dışlamak için beyaz liste tekniklerini kullanır. Vergilendirme, itibar vb. unsurlar da diğer finans kuruluşları ve e-ticaret şirketleri ile iş birliği yapılarak risk yönetimi için kullanılabilir. Müşterilerin özel bilgilerini kuruluşlar arasında paylaşmak riskli olduğundan, bir risk değerlendirme modeli oluşturmak için FÖ'den yararlanılabilir. Nitekim, müşteri mali durum takibi [29] ve açık bankacılık [30] gibi finansal alanlarda FÖ tabanlı araştırmalar literatürde yer bulmuştur.

Doğal Dil İşleme

Doğal Dil İşleme, makine öğrenimi modelleri üzerine kurulu en yaygın uygulamalardan biri olup, insan dili semantiğini daha iyi anlamamıza yardımcı olur. Ancak, son derece doğru dil modellerini eğitmek için büyük miktarda veri gerekir. Bu veriler cep telefonlarından, tabletlerden ve benzeri ağ erişimi olan elektronik cihazlardan kolaylıkla toplanabilir. Yine, her uç cihazdan gelen metinsel bilgiler kullanıcı bilgilerini içerdiğinden, merkezi dil öğrenme modelleri için gizlilik burada bir darboğaz olarak karşımıza çıkar. Bu kapsamda [31] 'de yazarlar, bir FÖ çerçevesi kullanarak Doğal Dil İşleme modelleri oluşturmanın mümkün olduğunu göstermişlerdir.

Network Saldırı Tespiti

Siber güvenlik konusu dünyada önemi her geçen gün artan alanlardan biridir. Bu alana kurumlar, şirketler ve devletler tarafından yapılan yatırımların miktarı ve her geçen gün daha da artmaktadır. Network saldırı tespiti ismi ile de anılan otomatik siber güvenlik sistemleri çoğunlukla makine öğrenmesi yöntemlerinden faydalanmaktadırlar [1]. Dünyada her an farklı merkezler hedef alınarak farklı saldırganlar tarafından çok çeşitli saldırı tipleri düzenlenmektedir. Bu durum da her bir merkezin kendi saldırı veri tabanıyla kısıtlı bir makine öğrenmesine dayalı network saldırı tespiti yapabildiği ve en etkili yöntemin ancak bu veri tabanlarının birleştirilerek tek bir merkezi network saldırı tespiti veri tabanı üzerinden eğitilecek olan bir model ile korunmaya çalışmasıdır. Oysaki ticari ve stratejik sebeplerle bu tür bir işbirliği mümkün olmamaktadır. FÖ sayesinde çeşitli merkezler verilerini paylaşmadan her bir tekil sistemden daha güçlü bir bağışıklık sistemine sahip ortak bir network saldırı tespiti modeli geliştirebilmektedirler.

Sonuç

Yapay zekanın gelişimi için ihtiyaç duyduğu büyük veri gereksinimi ilerleyen dönemlerde, veri gizliliği ve pahalı donanımsal gereklilikler nedeniyle bir darboğaza girmiştir. FÖ konsepti bu darboğazın aşılması için son

derece etkili çözümler sunmaktadır. 2016 'da Google yapay zekâ takımının literatüre kazandırmasıyla ilk temelleri atılan FÖ, dünyadaki araştırmacılar tarafından büyük ilgi görmüştür. FÖ ile ilgili olarak Sağlık, Nakliye, Finans, Doğal dil işleme gibi birçok alanda araştırmalar yapılmaktadır. Öte yandan, ülkemizde FÖ hak ettiği ilgiyi henüz görmemektedir. Bu bağlamda öncü bir Türkçe kaynak olması amacıyla bu derleme hazırlanmıştır.

Gelecek Çalışmalar

Bu makalede FÖ konseptinin temel çalışma mantığı, hangi problemlere çözümler getirdiği, FÖ konseptinin bileşenleri, FÖ'nün sınıflandırılması ve kullanım alanları ile ilgili genel bilgiler verilmiştir. FÖ yapay zekânın önünü açmak için son derece etkili bir çözüm olmakla beraber pahalı iletişim, sistem heterojenliği, istatistiksel zorluklar, gizlilik endişeleri ve algoritmik zorluklar gibi birçok geliştirilmeye açık konuları da beraberinde getirmiştir. Önümüzdeki çalışmalarda FÖ'nün gelişime açık alanlarının ve karşılaştığı zorlukların araştırılması planlanmaktadır.

Kaynaklar

[1] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey," pp. 1–43, 2017, [Online]. Available: http://arxiv.org/abs/1701.02145.

[2] Y. Ma, Z. Wang, H. Yang, and L. Yang, "Artificial intelligence applications in the development of autonomous vehicles: A survey," *IEEE/CAA J. Autom. Sin.*, vol. 7, no. 2, pp. 315–329, 2020, doi: 10.1109/JAS.2020.1003021.

[3] J. Bullock, A. Luccioni, K. H. Pham, C. S. N. Lam, and M. Luengo-Oroz, "Mapping the landscape of artificial intelligence applications against COVID-19," *J. Artif. Intell. Res.*, vol. 69, pp. 807–845, 2020, doi: 10.1613/JAIR.1.12162.

[4] O. Zawacki-Richter, V. I. Marín, M. Bond, and F. Gouverneur, "Systematic review of research on artificial intelligence applications in higher education-where are the educators?," doi: 10.1186/s41239-019-0171-0.

[5] J. Park *et al.*, "Communication-Efficient and Distributed Learning over Wireless Networks: Principles and Applications," *Proc. IEEE*, vol. 109, no. 5, pp. 796–819, 2021, doi: 10.1109/JPROC.2021.3055679.

[6] "I (Legislative acts) REGULATIONS REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)."

[7] H. Brendan McMahan, E. Moore, D. Ramage, S. Hampson, and B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," *Proc. 20th Int. Conf. Artif. Intell. Stat. AISTATS 2017*, vol. 54, 2017.

[8] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, Jun. 2017, doi: 10.1145/3065386.

[9] Z. Tang, S. Shi, X. Chu, W. Wang, and B. Li, "Communication-Efficient Distributed Deep Learning: A Comprehensive Survey," no. 1, pp. 1–23, 2020, [Online]. Available: http://arxiv.org/abs/2003.06307.

[10] E. M. Campos *et al.*, "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges," *Comput. Networks*, vol. 203, p. 108661, Feb. 2022, doi: 10.1016/J.COMNET.2021.108661.

[11] P. Kairouz *et al.*, "Advances and open problems in federated learning," *arXiv*, pp. 1–105, 2019.

[12] D. Jatain, V. Singh, and N. Dahiya, "A contemplative perspective on federated machine learning: Taxonomy, threats & vulnerability assessment and challenges," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.05.016.

[13] Q. Li *et al.*, "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," *IEEE Trans. Knowl. Data Eng.*, pp. 1–44, 2021, doi: 10.1109/TKDE.2021.3124599.

[14] S. Wang *et al.*, "Adaptive Federated Learning in Resource Constrained Edge Computing Systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1205–1221, 2019, doi: 10.1109/JSAC.2019.2904348.

[15] V. Smith, C. Chiang, M. Sanjabi, and A. Talwalkar, "Federated Multi-Task Learning," no. Nips, 2017.

[16] Q. Li, Z. Wen, and B. He, "Practical federated gradient boosting decision trees," *AAAI 2020 - 34th AAAI Conf. Artif. Intell.*, pp. 4642–4649, 2020, doi: 10.1609/aaai.v34i04.5895.

[17] "Flower aggregation algorithms." https://flower.dev/docs/.

[18] S. Reddi *et al.*, "Adaptive Federated Optimization," no. 2, pp. 1–38, 2020, [Online]. Available: http://arxiv.org/abs/2003.00295.

[19] L. Li, Y. Fan, M. Tse, and K. Y. Lin, "A review

of applications in federated learning," *Comput. Ind. Eng.*, vol. 149, no. September, 2020, doi: 10.1016/j.cie.2020.106854.

[20] M. Ghassemi, T. Naumann, P. Schulam, A. L. Beam, I. Y. Chen, and R. Ranganath, "A Review of Challenges and Opportunities in Machine Learning for Health.," *AMIA Jt. Summits Transl. Sci. proceedings. AMIA Jt. Summits Transl. Sci.*, vol. 2020, pp. 191–200, 2020, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/32477638%0Ahttp://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC7233077.

[21] Q. Dou *et al.*, "ARTICLE Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study," doi: 10.1038/s41746-021-00431-6.

[22] X. Li, Y. Gu, N. Dvornek, L. H. Staib, P. Ventola, and J. S. Duncan, "Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results," *Med. Image Anal.*, vol. 65, 2020, doi: 10.1016/j.media.2020.101765.

[23] L. Huang, A. L. Shea, H. Qian, A. Masurkar, H. Deng, and D. Liu, "Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records," *J. Biomed. Inform.*, vol. 99, no. September, p. 103291, 2019, doi: 10.1016/j.jbi.2019.103291.

[24] K. Tan, D. Bremner, J. Le Kernec, and M. Imran, "Federated Machine Learning in Vehicular Networks: A summary of Recent Applications," *2020 Int. Conf. UK-China Emerg. Technol. UCET 2020*, no. August, 2020, doi: 10.1109/UCET51115.2020.9205482.

[25] Y. Liu, J. J. Q. Yu, J. Kang, D. Niyato, and S. Zhang, "Privacy-Preserving Traffic Flow Prediction: A Federated Learning Approach," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7751–7763, 2020, doi: 10.1109/JIOT.2020.2991401.

[26] A. Nguyen *et al.*, "Deep Federated Learning for Autonomous Driving." [Online]. Available: https://github.com/aioz-ai/FADNet.

[27] A. M. Elbir, B. Soner, and S. Coleri, "Federated Learning in Vehicular Networks," pp. 1–6, 2020, [Online]. Available: http://arxiv.org/abs/2006.01412.

[28] G. Long, T. Shen, Y. Tan, L. Gerrard, A. Clarke, and J. Jiang, "Federated Learning for Privacy-Preserving Open Innovation Future on Digital Health," *Humanit. Driven AI*, pp. 113–133, 2022, doi: 10.1007/978-3-030-72188-6_6.

[29] A. Imteaj and M. H. Amini, "Leveraging asynchronous federated learning to predict customers financial distress," *Intell. Syst. with Appl.*, vol. 14, 2022, doi: 10.1016/j.iswa.2022.200064.

[30] G. Long, "Federated Learning for Open Banking."

[31] D. G. Bernal, "Decentralizing Large-Scale Natural Language Processing with Federated Learning," *Degree Proj. Comput. Sci. Eng.*, 2020, [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1455825.