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

Araştırma Makalesi / Research Article

Federe Öğrenmede Birleştirme Algoritmalarının Model Performansına Etkisi

The Impact of Aggregation Algorithms on Federated Learning Models

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 24 Ocak 2023
Revizyon 2 Şubat 2023
Kabul 4 Şubat 2023
Online 23 Mart 2023

Anahtar Kelimeler:

Federe Öğrenme, FedAVG, ResNet,MobileNet, Veri gizliliği, Derin Öğrenme

ÖZ

Hammaddesi büyük veri olan Yapay zeka (YZ) teknolojileri özellikle son yıllarda verinin gizliliği ve güvenliği gibi önemli gerekçelerle veriye ulaşmayı zorlaştıran sebeplerden ötürü bir takım zorluklarla karşılaşmaktadır. Öte yandan büyük verinin merkezi bir lokasyonda toplanmasının zorlukları ve yüksek kapasiteli depolama ve işlemci ihtiyaçları da YZ alanında karşılaşılan zorluklardır. Bu zorluklardan esinlenerek geliştirilen İşbirlikçi YZ konsepti olan Federe Öğrenme (FÖ), işbirliğine katılan katılımcıların, veri gizliliğini ihlal etmeden YZ model parametrelerinin kendi verileri ile işlenip model paremetrelerinin güncellenmesi ve güncellenen parametrelerin bir sunucuda belirli algoritmalar aracılığıyla birleştirilmesi ile iteratif olarak gerçekleştirilen bir konsepttir. FÖ konsepti, katılımcıların öznitelik ve örnek uzaylarının ortaklığına bağlı olarak Yatay FÖ, Dikey FÖ ve Federe Transfer Öğrenme şeklinde yaklaşımlar ile uygulanmaktadır. Bu çalışmada öznitelik uzaylarının ortak olduğu Yatay FÖ yaklaşımı için geliştirilen model parametrelerini birleştirme algoritmalarından FedAVG, FedAVGM ve FaultTolerantFedAVG'nin 5 katılımcı arasında özdeş olmayan bir şekilde dağıtılmış olan MNIST veri setinin ResNet-18 ve MobileNet V3 small sınıflandırıclarının performansına etkisi incelenmektedir.

ARTICLE INFO

Article history:

Received 24 January 2023
Received in revised form 2 February 2023
Accepted 4 February 2023
Available online 23 March 2023

Keywords:

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

ABSTRACT

Artificial intelligence (AI) technologies, whose raw material is big data, have been encountering some difficulties especially in recent years due to important reasons like data privacy and security concerns. On the other hand, the difficulties of collecting big data in a central location and the necessity of high-capacity storage and processors are also the challenges in the field of AI. Federated Learning (FL), which is a Collaborative AI concept inspired by these challenges, is an iterative concept that is carried out by the participants in the collaboration, by processing AI model parameters with their own local data, updating the model parameters, and then combining the updated parameters on a server through certain algorithms without violating data privacy. The FL concept is implemented with approaches such as Horizontal FL, Vertical FL and Federated Transfer Learning, depending on the feature and sample spaces of the partnership of the collaborator participants. In this study, the effect of the model parameter aggregation algorithms such as FedAVG, FedAVGM and FaultTolerantFedAVG which are developed for the Horizontal FL approach are analyzed using the ResNet-18 and MobileNet V3 small classifiers on the MNIST dataset which is distributed non-identically among 5 participants.

Doi: 10.24012/dumf.1241947

* Sorumlu Yazar

Giriş

Bilişim teknolojilerinin yaklaşık son 30 yıldaki hızlı gelişimi ile sağlık, eğitim, güvenlik, ticaret gibi neredeyse her alanda logaritmik şekilde artan devasa miktarlarda dijital veri birikmektedir. Gücünü büyük veriden alan Derin Öğrenme (DÖ) [1] algoritmaları için bu verilerin işlenmesi kritik derecede önemlidir. Ancak bu boyutlarda verinin depolanması ve işlenmesi gibi zorlukların yanında özellikle son yıllarda veri gizliliği ve güvenliği gibi endişelerle veriye erişimde de engeller ile karşılaşılmaktadır.

Klasik Merkezi Öğrenme konseptinde verilerin belirli bir lokasyonda toplanması gerekmektedir ve bu konseptte güçlü işlemci ve yüksek depolama kapasitesi gibi zorlukların yanında veri gizliliğinin ihlali söz konusudur. Verinin işlenmesi ve depolanmasına ilişkin Dağıtık Öğrenme gibi teknolojilerden faydalanarak çözümler üretilmiş olmasına karşın veri güvenliğinin sağlanması ve veri gizliliğinin korunması adına bu dağıtık teknolojiler de gerekli ve yeterli çözümü üretememiştir.

Bunlara ek olarak veri güvenliği ve gizliliği ile ilgili kişisel ve toplumsal hassasiyetin arttığı gözlemlenmektedir. 2018 yılında Facebook veri tabanından kişisel verilerin çalınması hadisesi ile beraber bu hassasiyet Uluslararası toplumu harekete geçirmiş veri güvenliği Avrupa Birliği Genel Veri Koruma Tüzüğü'nde [2] yer alarak güvence altına alınmıştır.

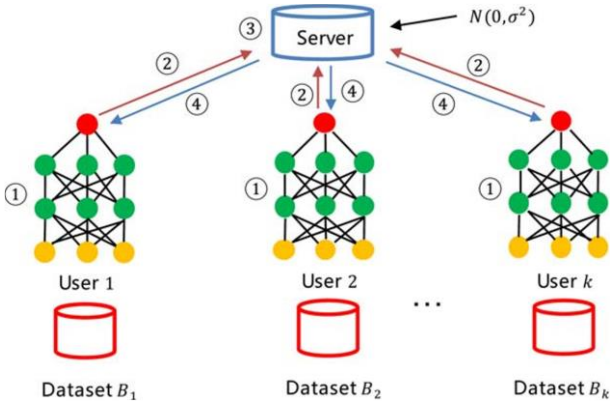
Veriye erişim & veri gizliliği ikilemini çözmek adına Google Yapay Zekâ ekibi tarafından ilk olarak 2016 yılında Federe Öğrenme (FÖ) [3] konsepti önerilmiştir. FÖ veri gizliliğini sağlamasının yanında modelin kullanıcının kendi yerel kaynakları üzerinde kendi verisi ile eğitilmesini gerçekleştirerek işlemci ve veri depolama yükünün de katılımcılara dağıtılmasını sağlamaktadır. FÖ sürecinde katılımcılar verilerini paylaşmazken merkezi koordinatör sunucusundan aldıkları ortak bir modeli kendi verisi ile öz kaynaklarını kullanarak model eğitimini gerçekleştirir. FÖ konseptinde modellerin hata toleransı daha yüksektir. Model eğitimi katılımcılar üzerinden gerçekleştiğinden dolayı FÖ, DÖ'ye nispeten ağdaki yükü azaltır. Ek olarak model eğitimi için tüketilen güç de geleneksel yaklaşımlardan daha azdır. Yapılan çalışmalar incelenince FÖ konseptinin henüz emekleme aşamasında olduğu ve gelişime açık bir alan olduğu anlaşılmaktadır.

Federe Öğrenme

Şekil 1 'de görüleceği üzere temel FÖ konsepti [4] 4 adımdan oluşur:

1. Katılımcılar koordinatör sunucudan global modeli alır.
2. Her katılımcı, aldığı modeli kendi özel verisiyle eğitir. Bu işlem neticesinde model parametreleri güncellenmiş olur.
3. Güncellenen model parametreleri koordinatöre gönderilir.
4. Koordinatör, güncellenen parametreleri belirli algoritmalar kullanarak birleştirir. Ve yeni parametreler katılımcılara gönderilir.

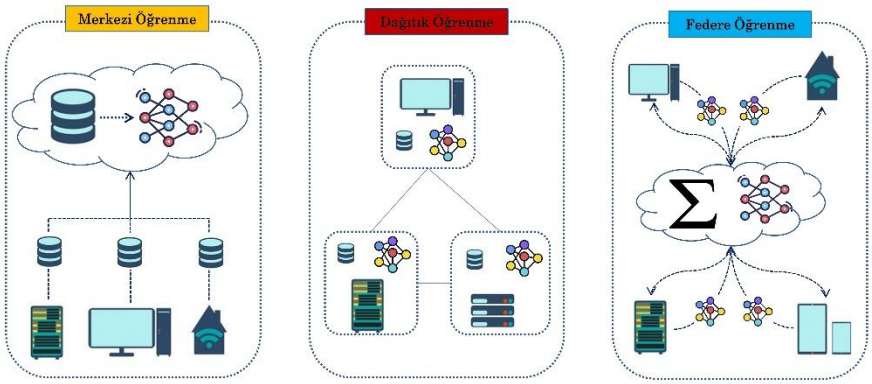
Bu döngü model yakınsayana kadar devam eder.



Şekil 1. FÖ temel konsepti [5]

İncelenen problemin niteliğine göre 3 farklı FÖ türünden bahsedilebilir [6]. Öznitelik uzayının katılımcılar arasında ortak olduğu problemlerde Yatay FÖ, örnek uzayının katılımcılar arasında ortak olduğu problemlerde ise Dikey FÖ kullanılmalıdır. Öte yandan hem öznitelik, hem de örnek uzayının cüzi miktarlarda ortak olduğu modeller için ise Federe Transfer Öğrenme tercih edilmektedir.

Bu çalışmada Yatay FÖ birleştirme algoritmalarının sınıflandırıcıların performansına etkisi araştırılmıştır. Çalışmada literatürde sıkça görüntü sınıflandırma araştırmalarında benchmark testleri amacıyla kullanılan MNIST veri seti kullanılmıştır. FÖ birleştirme algoritmalarından FedAVG, FedAVGM ve FaultTolerantFedAVG algoritmalarının sonuca etkisi incelenmiştir.



Şekil 2. Merkezi, Dağıtık ve FÖ yaklaşımları

Makalenin geri kalan kısmında ilk olarak literatürde FÖ birleştirme algoritmaları ile ilgili çalışmalar özetlenmiştir. Materyal bölümünde çalışmada kullanılan veri seti tanıtılmıştır. Metod bölümünde katılımcılarda kullanılan DÖ modelleri ve FÖ sırasında kullanılan birleştirme algoritmaları detaylandırılmıştır. Uygulama bölümünde deneyler için dizayn edilen senaryolar tanıtılmıştır. Son olarak sonuçlar karşılaştırmalı olarak değerlendirilmiştir.

Literatür

Literatürde Federe Öğrenme Birleştirme algoritmaları ile yapılan çalışmalardan bir kısmı:

Nilsson ve ark . [7] 3 FÖ algoritmasını kıyaslamış ve performanslarını verilerin merkezi bir sunucuda toplandığı yaklaşımla kıyaslamışlardır. Çalışmada Federated Averaging (FedAvg), Federated StochasticVariance Reduced Gradient ve CO-OP algoritmaları, verilerin hem IID hem de non-IID durumlarında kıyaslanmıştır. Veri seti olarak MNIST kullanılmıştır. Sonuçlar, hem IID hem non-IID veri durumunda FedAvg' nin birleştirme algoritmaları arasında en yüksek doğruluğu elde ettiğini göstermiştir. FedAvg ile merkezi öğrenme arasındaki karşılaştırmada, IID verileri kullanılması durumunda sonuçların çok yakın olduğu, ancak merkezileştirilmiş yaklaşımın non-IID verilerde FedAvg'den daha iyi performans gösterdiği tespit edilmiştir.

Sannara ve ark. [8] katılımcıların belirli nöronları arasındaki farklılıkları belirleyerek model mimarisini değiştirebilen FedDist adlı yeni bir birleştirme algoritması önermişlerdir. Veri seti olarak HAR (Human Activity Recognition-Akıllı Telefonlarla İnsan Etkinliğini Tanıma) veri seti kullanılmıştır. Çalışmada önerdikleri FedDist algoritması klasik FedAVG, FedMA (Federated Matched Averaging), FedPER (Federated Learning with Personalization Layers) olmak üzere 3 adet FÖ birleştirme algoritmasıyla karşılaştırılmıştır. 200 FÖ turu neticesinde elde ettikleri sonuçlara göre önerdikleri FedDist birleştirme algoritmasının diğerlerinden daha başarılı olduğunu belirtmişlerdir.

Campos ve ark. [9] bir IoT senaryosundaki farklı saldırıların tespiti için farklı veri dağılımlarını dikkate alan çok sınıflı bir sınıflandırıcıya dayalı FÖ özellikli bir IDS (Intrusion Detection System-Saldırı Tespit Sistemi) yaklaşımını değerlendirmişlerdir. Çalışmada en güncel IDS veri setlerinden biri olan ToN-IoT veri setini IoT cihazlarının IP adreslerine ve saldırı türlerine göre bölümleyerek elde ettikleri üç farklı senaryoda değerlendirmişlerdir. FÖ uygulaması olarak en son IBMFL çerçevesini kullanarak FedAVG ile FED+ birleştirme algoritmalarının da kıyaslamalarını yapmışlardır.

Materyal

Veri Seti

Bu çalışmada literatürdeki görüntü sınıflandırma ile ilgili yapılan birçok bilimsel araştırmada benchmark veri seti olarak kabul gören MNIST (Modified National Institue of Standarts) veri seti kullanılmıştır.

Şekil 3. MNIST veri setinden bir kesit

Tablo 1. MNIST verisinin 5 katılımcı üzerindeki dağılımı

	K1	K2	K3	K4	K 5
0	5923	100	100	100	100
1	6742	100	100	100	100
2	100	5958	100	100	100
3	100	6131	100	100	100
4	100	100	5842	100	100
5	100	100	5421	100	100
6	100	100	100	5918	100
7	100	100	100	6265	100
8	100	100	100	100	5851
9	100	100	100	100	5949

MNIST veri seti el yazması 0’ dan 9’a kadar olan rakamların 28x28 piksel boyutlarında dijital ortama aktarıldığı bir veri kümesidir. Şekil 3 de veri setinden bir kesit görülmektedir. MNIST veri seti eğitim ve test amaçlı sırasıyla toplamda 60000 ve 10000 adet görüntü içermektedir [10]. Bu çalışmada MNIST veri setine ait görüntüler 5 katılımcıya özdeş olmayan bir şekilde dağıtılmıştır. Bu şekilde non-IID veri durumunda değişik derin öğrenme algoritmalarının değişik birleştirme algoritmaları bağlamında performans değişiklikleri incelenmiştir. Bu çalışmada katılımcılar arasındaki özdeş olmayan veri dağılımı Tablo 4’te gösterilmiştir.

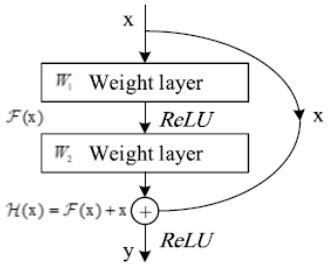
Metod

Bu bölümde FÖ sürecinde katılımcılarda kullanılan derin ağ modelleri ve FÖ birleştirme algoritmaları tanıtılmaktadır.

ResNet-18

Resnet (Residual Networks) ağları 2015 yılında Kaiming He ve ark. [11] tarafından sunulan ve çoğunlukla görüntü işleme alanında kullanılan bir derin ağ modelidir. Şekil 4

'te 1 artık blok şeması gösterilmiştir. Eğik ok kısayol bağlantısını temsil etmektedir.



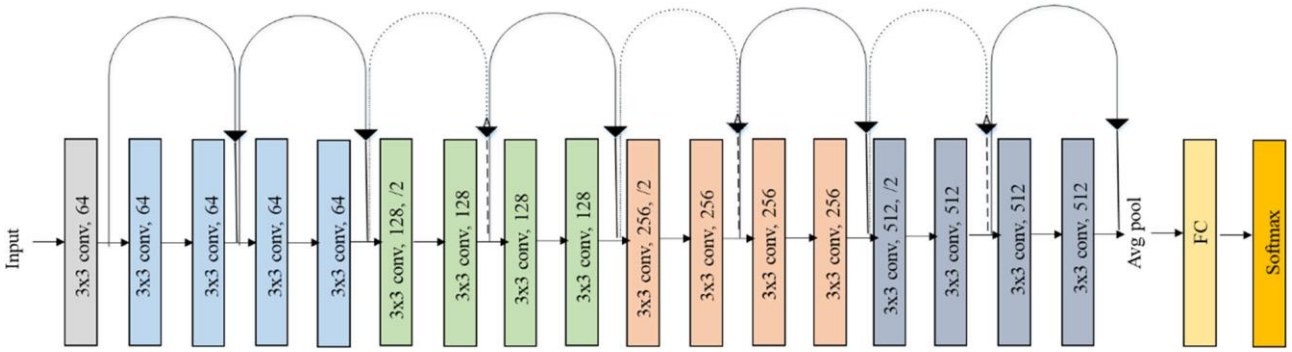
Şekil 4. ResNet Artık Blok Yapısı

Giriş ile çıkış arasındaki bağıntı deklem 1'de gösterilmiştir.

$$y = \mathcal{F}(x, \{W_i\}) + x \quad (1)$$

$\mathcal{F}(x, \{W_i\})$, x girdi değerinin W_i katmanlarındaki konvolüsyon işlemleri ve ReLU fonksiyonundan geçirilmesini ifade eden genel bir fonksiyondur. Başka bir ifadeyle $\mathcal{F}$ önceki katmanın ek bilgilerini korumaya yarar. Artık blok Şekil 4 'te görüldüğü üzere W_1 ve W_2 olmak üzere 2 adet ağırlık katmanı ve arada ReLU aktivasyon fonksiyonunu ve kısa yol bağlantısını içerir.

Bu çalışmada kullanılan ResNet-18 modelinin orijinal blok şeması Şekil 5'te gösterilmektedir.



Şekil 5. Orijinal ResNet-18 Modeli [12]

MobileNet V3 small

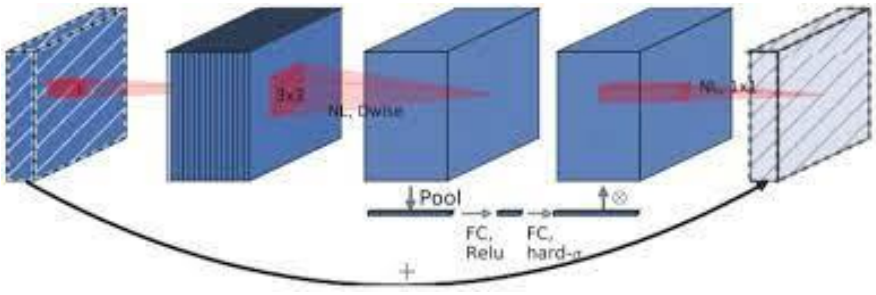
MobileNet ağları adından da anlaşılacağı üzere mobil uygulamalarda kullanılmak üzere tasarlanan Tensorflow 'un ilk mobil bilgisayar görüntü işleme modelidir. Özellikle güç ve işlemci kaynağı kısıtlı olduğu durumlarda minimum parametre ile doğruluğu maximize etmeyi amaçlar.

MobileNET V3 modeli; MobileNET V1, MobileNET V2 ve MnasNet (Mobile Neural Architecture Search Network) ağlarında sırasıyla bulunan derinlemesine ayrılabilir konvolüsyon, ters artık ve doğrusal darboğaz ile sıkma ve uyarma bloklarını içermektedir. Ayrıca doğrusal olmayan fonksiyon olarak ReLU yerine h-swish fonksiyonu kullanılmıştır. h-swish (hard-swish) fonksiyonu x input olmak üzere denklem 2'de gösterilmiştir [13]:

$$h - swish[x] = x\frac{ReLU6(x+3)}{6} \quad (2)$$

Klasik Swish fonksiyonu x*sigmoid(x) ifadesi hesaplanıyor iken, hard-swish'te onun yerine normalize edilmiş, parçalı doğrusal Relu6() fonksiyonu kullanılarak performans arttırılmıştır [13]. MobileNet V3 orijinal blok şeması Şekil 6 da gösterilmiştir.

Ağlarda aynı derinliğe sahip düzenli konvolüsyonlara sahip ağa kıyasla parametre sayısını önemli ölçüde azaltır [13].



Şekil 6. MobileNet V3 blok yapısı [13]

Federe Öğrenme Birleştirme Algoritmaları

Yatay FÖ 'de koordinatör sunucular konseptin en kritik bileşenlerinden biridir. Koordinatör sunuculuk görevini katılımcılardan biri yapabileceği gibi konseptin kullanım amacına bağlı olarak bağımsız bir sunucu da yapabilir. Koordinatör sunucu katılımcıların kendi kişisel verileri ile eğitmiş oldukları model parametrelerini belirli algoritmalar ile birleştirir. Bu çalışmada Flower-Federated çerçevesinin sunmuş olduğu FedAVG [3], FedAVGM [14] ve FedAVG Fault Tolerant algoritmaları kullanılmıştır.

FedAVG

Federated Averaging algoritması ilk olarak Mc Mahan ve ark. tarafından FÖ 'nün ilk birleştirme algoritması olarak ortaya çıkmıştır. FederatedAveraging (FedAVG) her bir istemcideki yerel stokastik gradyan iniş (SGD) değerlerinin ortalamasını alarak yeni bir model oluşturur. K katılımcı sayısı, n bütün katılımcılarda bulunan toplam örnek sayısı, n_k k'ıncı katılımcının örnek sayısını temsil etmek üzere FedAVG algoritmasının ağırlıklı ortalama alma formülü denklem 3 ve 4'teki gibidir:

$$w_t^k \leftarrow \sum_{k=1}^{K} \left(\frac{n_k}{n} w_t^k\right) \tag{3}$$

şeklinde ifade edilir. Güncelleme işlemi de matematiksel olarak:

$$w_{t+1}^k \leftarrow w_t^k - \nabla w_t^k \tag{4}$$

şeklinde ifade edilir.

FedAVGM

FedAVGM, standart FedAVG yöntemine sunucu momentumunun eklenmesi ile geliştirilmiştir. Temel olarak non-IID [15] terimi ile ifade edilen verinin katılımcılardaki dengesiz dağılması durumunun klasik FedAVG nin performansını ciddi anlamda düşürmesine bir çözüm olarak önerilmiştir [14]. FedAVG'yi tanımlayan denklem 3 ve 4'teki formüllerden farklı olarak gradyan değişimleri için sunucudaki momentum (β) kavramı bir yenilik olarak denklem 5 ve 6'daki gibi dâhil edilmiştir.

$$w_{t+1}^k \leftarrow w_t^k - v_t^k \tag{5}$$

$$v_t^k \leftarrow \beta v_t^k + \nabla w_t^k \tag{6}$$

FaultTolerantFedAVG

Herhangi bir katılımcı bağlantısının kesilmesi veya gecikmesi durumunda hatalı katılımcı koşullarıyla başa çıkabilen, FLOWER kitaplığında kullanılan bir FedAvg çeşididir.

Uygulama

Bu çalışmada kullanılan tüm derin öğrenme yöntemleri, Lokal Öğrenme (LÖ), Merkezi Öğrenme (MÖ) ve FÖ olmak üzere üç farklı mimari üzerinde yürütülmektedir. LÖ mimarisi, işbirliği yapan tüm katılımcıların kendi yerel verilerini kullanarak her birinin kendi farklı modellerini eğittiği ve ortak test verilerinin global olarak kullanıldığı durumu ifade eder. MÖ mimarisi, iş birliği yapan tüm katılımcıların verilerini tek bir sunucuda birleştirdiği ve mümkün olan en yüksek doğruluğun elde edilmesinin beklendiği durumu sunar. FÖ mimarisi ise iş birliği yapan tüm katılımcıların kendi yerel verilerini tuttukları ve nihai genel modelin yalnızca model parametresi güncellemelerinin yinelemeli olarak merkezi bir sunucu ile paylaşılarak elde edildiği bir durumdur.

Sonuçlar ve Tartışma

ResNet-18 ve MobileNet V3 small ağlarının her biri özdeş olmayan bir şekilde 5 katılımcı üzerinde dağıtılmış olan MNIST veri seti üzerinde LÖ, MÖ ve FÖ konseptlerine göre eğitilip test edilmiştir. LÖ ve MÖ için epok sayısı 50 olarak ayarlanmış ve iki epokta bir defa test veri seti ile test edilmiştir. FÖ konspetinde ise her bir katılımcının lokal kaynaklarındaki eğitimi sırasındaki epoch sayısı 1 olarak, katılımcılar ve sunucu arasındaki döngü sayısını ifade eden global epoch sayısı 50 olarak belirlenmiştir. ResNet-18 ve MobileNet V3 small modelleri IMAGENET1K_V2 veri seti üzerinde ön eğitimden geçirilmiş olan pytorch torchvision kütüphanesindeki ağırlık değerleri ile eğitime başlatılmışlardır [16]. ResNet-18 ve MobileNet V3 small modelleri için LÖ,MÖ ve FÖ konseptlerine göre yapılan eğitimler sonucunda elde edilen performans sonuçları sırasıyla Tablo 2 ve 3'te verilmiştir. Performans farkları Doğruluk, Kesinlik, Duyarlılık, F1 skor ve AUC açısından ele alınmıştır. Bu çalışmada, AUC, Kesinlik, Duyarlılık ve F1 skor verileri 10 adet sınıf için ayrı ayrı elde edildikten sonra ortalamaları alınarak aşağıdaki tablolarda performans karşılaştırma amaçlı kullanılmıştır. AUC değeri OVR(one versus rest) mantığı ile yani her bir sınıfın AUC başarısı geriye kalan tüm sınıflara karşı hesaplanmıştır.

Tablo 2 verileri incelendiğinde, ResNet-18 modelinin LÖ konseptine göre 0.8127 ile 0.8840 arasında AUC başarımları gösteriyorken, MÖ konseptine göre 0.9873 AUC başarım gösterdiği görülmektedir. FÖ konseptine göre ise en yüksek başarımın 0.9803 AUC değeri ile FedAVGM birleştirme algoritması ile elde edildiği gözlenmektedir. FÖ konseptine sahip diğer birleştirme algoritmaları olan FedAVG ve FaultTolerantFedAVG algoritmalarının da sırasıyla 0.9774 ve 0.9764 değerlerini elde ettiklerini görülmektedir. Dolayısıyla, FÖ konseptinin LÖ konseptine göre en az %9.24 AUC artışı avantajı sağladığı, MÖ konseptine göre ise en fazla %1.04 kadar AUC değerinden feragat ettiği Tablo 2'de gözlenebilmektedir.

Tablo 2 diğer metriklere göre incelendiğinde FÖ'nün avantajı çok daha bariz bir şekilde görülmektedir. FÖ konseptinin LÖ konseptine göre, Doğruluk, Kesinlik, Duyarlılık ve F1 Skor metriklerine göre sağladığı avantaj sırasıyla en az %37.28 , %14.40 , %37.96 , %42.18 kadardır. Öte yandan, FÖ konseptinin MÖ konseptine göre, Doğruluk, Kesinlik, Duyarlılık ve F1 Skor metriklerine göre dezavantajı da sırasıyla en fazla %12.12 , %10.34 , %12.03 , %12.19 kadardır.

Tablo 3 verileri incelendiğinde, MobileNet V3 small modelinin LÖ konseptine göre 0.8112 ile 0.8803 arasında AUC başarımları gösteriyorken, MÖ konseptine göre 0.9868 AUC başarım gösterdiği görülmektedir. FÖ konseptine göre ise en yüksek başarımın 0.9745 AUC değeri ile FedAVG birleştirme algoritması ile elde edildiği gözlenmektedir. FÖ konseptine sahip diğer birleştirme algoritmaları olan FedAVGM ve FaultTolerantFedAVG algoritmalarının da sırasıyla 0.9728 ve 0.9721 değerlerini elde ettiklerini görülmektedir. Dolayısıyla, FÖ konseptinin LÖ konseptine göre en az %9.18 AUC artışı avantajı sağladığı, MÖ konseptine göre ise en fazla %1.47 kadar AUC değerinden feragat ettiği Tablo 2'de gözlenebilmektedir.

Tablo 3 diğer metriklere göre incelendiğinde FÖ'nün avantajı net bir şekilde görülmektedir. FÖ konseptinin LÖ konseptine göre, Doğruluk, Kesinlik, Duyarlılık ve F1

Skor metriklerine göre sağladığı avantaj sırasıyla en az %34.43 , %9.94 , %34.94 , %40.57 kadardır. Öte yandan, FÖ konseptinin MÖ konseptine göre, Doğruluk, Kesinlik, Duyarlılık ve F1 Skor metriklerine göre dezavantajı da sırasıyla en fazla %11.37 , %11.79 , %11.33 , %12.12 kadardır.

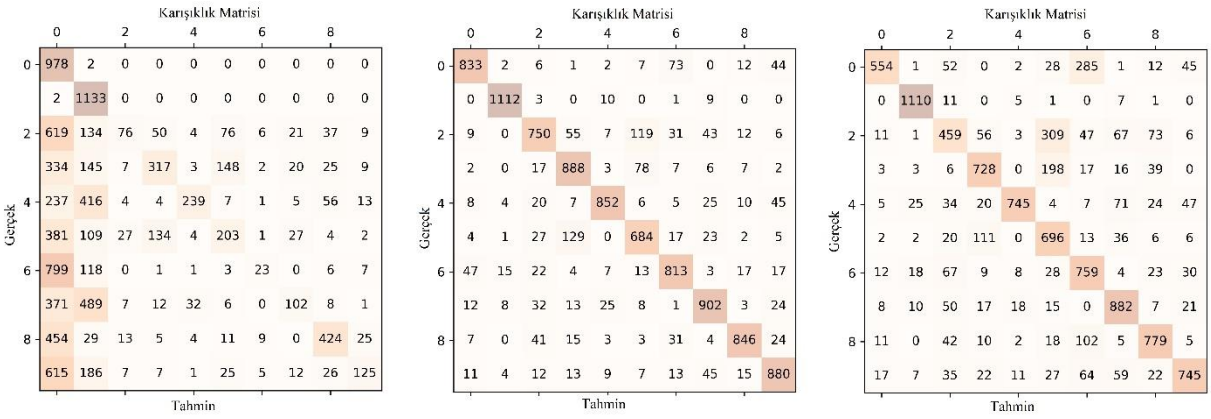
ResNet-18 ve MobileNet V3 small modelerinin LÖ, MÖ ve FÖ konseptlerine göre karışıklık matrisleri Şekil 7 ve 8'de gösterilmiştir. MobileNet V3 small ve ResNEt-18 modelleri üzerinde FÖ konseptinde her bir katılımcının Eğitim Kaybı (training loss) ve Test Kaybı (validation loss) sırasıyla Şekil 10 ve 11'de gösterilmiştir. Hem Eğitim Kaybı hem de Test Kaybındaki azalma tüm epoklarda devam ettiği için, her üç birleştirme algoritmasının da hiçbir modelde veya katılımcıda aşırı öğrenme (overfitting) göstermediği anlaşılmaktadır. Şekil 9'da ise ResNet-18 ve MobileNet V3 small modellerinin LÖ, MÖ ve FÖ konseptlerine göre tüm katılımcıların AUC değerlerinin artış eğrileri gösterilmiştir. Görüldüğü gibi ResNet-18 modeli üzerinde öncelik sırasıyla FedAVGM, FaultTolerantFedAVG ve FedAVG, MobileNet V3 small modeli üzerinde ise sırasıyla FedAVG, FedAVGM ve FaultTolerantFedAVG birleştirme algoritmaları yakınsamaktadır. FÖ konseptinin, bu çalışmadaki gibi özdeş olmadan dağıtılmış 5 katılımcılı bir veri setinin 30 epok gibi bir sürede MÖ sınırına yakınsayabildiği gözlenmektedir. LÖ konseptinde ise her bir katılımcının kendi veri setindeki veri dağılımının temsil kapasitesine göre farklı AUC değerlerinden başlayarak MÖ ve FÖ'ye uzak bir noktaya yakınsadıkları görülmektedir.

Tablo 2. ResNet-18 modelinin 5 katılımcı üzerinde LÖ, MÖ ve FÖ konseptlerine göre eğitilerek elde edilen test sonuçları

							FedAVG	**FedAVGM**	**FaultTolerant FedAVG**
METRİK	**LÖ 1**	**LÖ 2**	**LÖ 3**	**LÖ 4**	**LÖ 5**	**MÖ**	**FÖ**	**FÖ**	**FÖ**
Doğruluk	0.3620	0.2275	0.2194	0.2094	0.2458	0.856	0.7457	0.7384	0.7348
F1 Skor	0.31	0.1220	0.1241	0.0924	0.1354	0.8537	0.7418	0.7318	0.7327
Kesinlik	0.5418	0.4053	0.4717	0.6079	0.5169	0.8553	0.7604	0.7519	0.7556
Duyarlılık	0.3537	0.2198	0.2328	0.2110	0.2412	0.8536	0.7436	0.7368	0.7333
AUC	0.8840	0.8127	0.8337	0.8681	0.8461	0.9873	0.9774	0.9803	0.9764

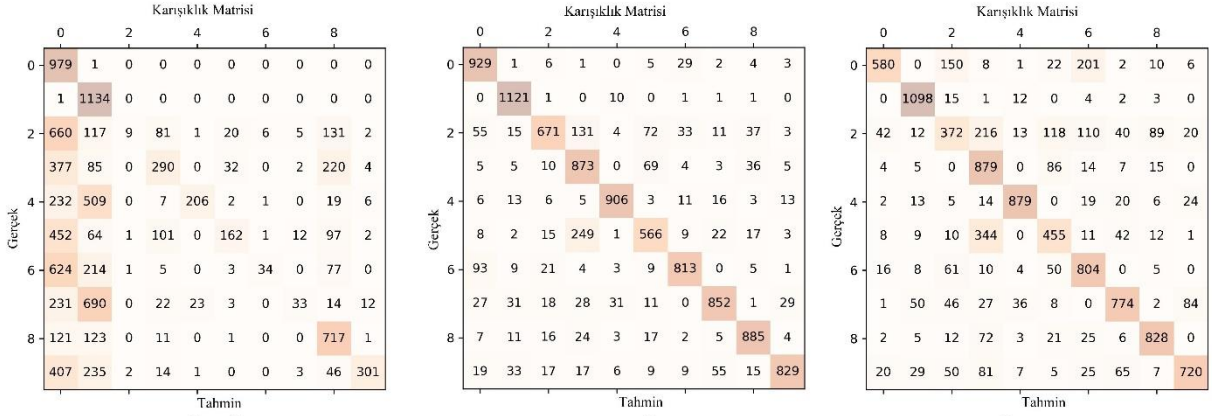
Tablo 3. MobileNet V3 small modelinin 5 katılımcı üzerinde LÖ, MÖ ve FÖ konseptlerine göre eğitilerek elde edilen test sonuçları

							FedAVG	**FedAVGM**	**FaultTolerant FedAVG**
METRİK	**LÖ 1**	**LÖ 2**	**LÖ 3**	**LÖ 4**	**LÖ 5**	**MÖ**	**FÖ**	**FÖ**	**FÖ**
Doğruluk	0.3865	0.2050	0.2309	0.2183	0.2101	0.8445	0.7389	0.7333	0.7308
F1 Skor	0.3141	0.0886	0.1484	0.1069	0.0940	0.8410	0.7312	0.7237	0.7198
Kesinlik	0.6323	0.2076	0.4197	0.5301	0.2388	0.8496	0.7476	0.7425	0.7317
Duyarlılık	0.3787	0.1895	0.2436	0.2199	0.2101	0.8414	0.7351	0.7293	0.7281
AUC	0.8803	0.8112	0.8122	0.8590	0.8299	0.9868	0.9745	0.9728	0.9721



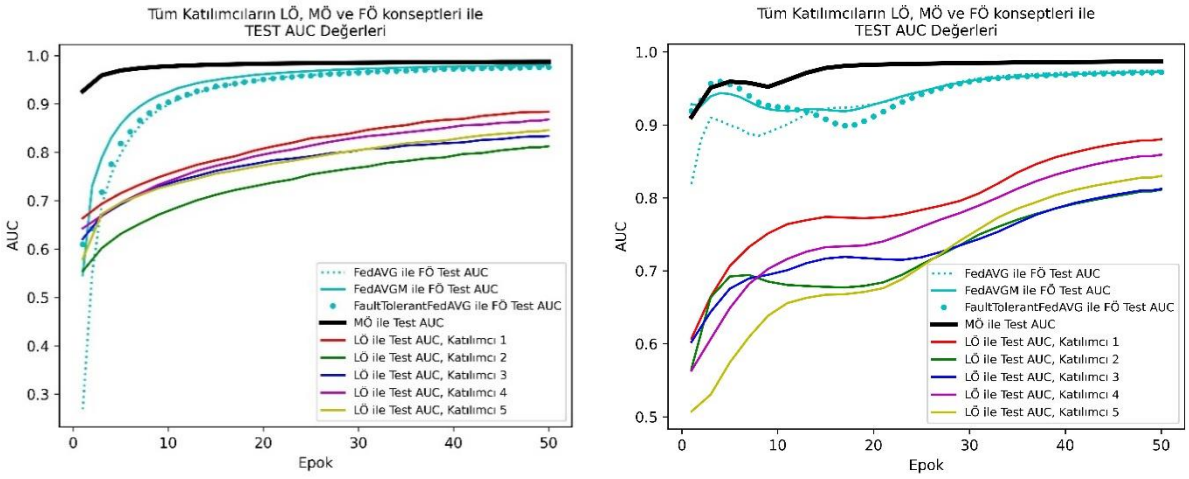
a) LÖ (LÖ 1) b) MÖ c) FÖ (FedAVG)

Şekil 7. ResNet-18 modelinin LÖ, MÖ ve FÖ konseptlerine göre karışıklık matrisleri



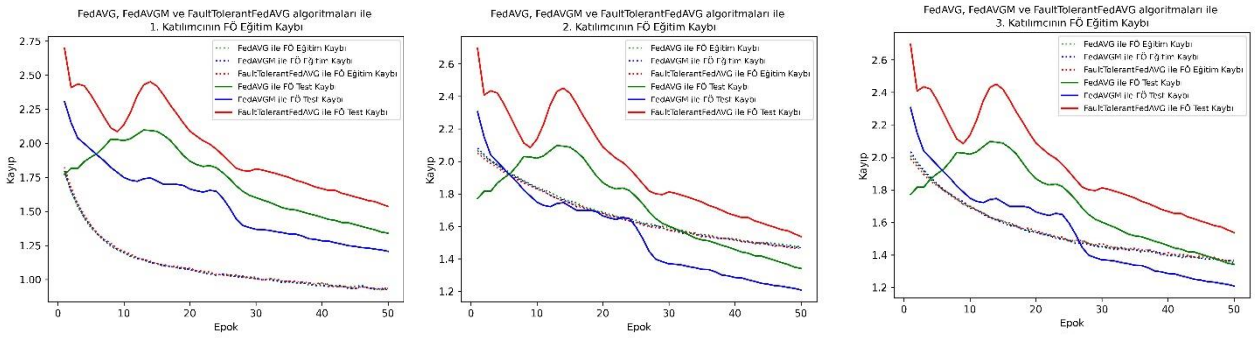
a) LÖ (LÖ 1) b) MÖ c) FÖ (FedAVG)

Şekil 8. MobileNet V3 small modelinin LÖ, MÖ ve FÖ konseptlerine göre karışıklık matrisleri

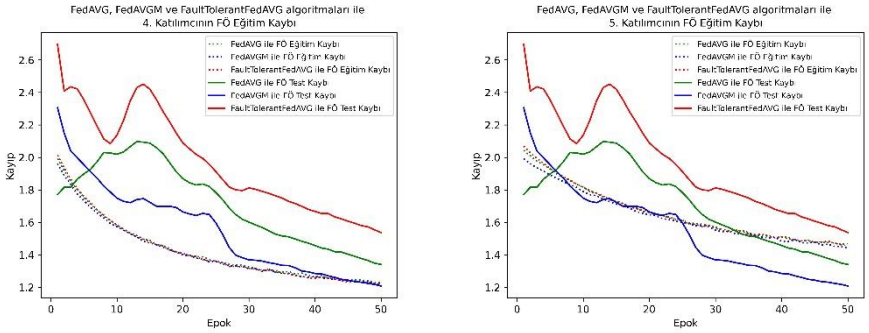


a) ResNet-18 b)MobileNet V3 small

Şekil 9. ResNet-18 ve MobileNet V3 small modellerinin LÖ, MÖ ve FÖ konseptlerine tüm katılımcıların AUC değerleri

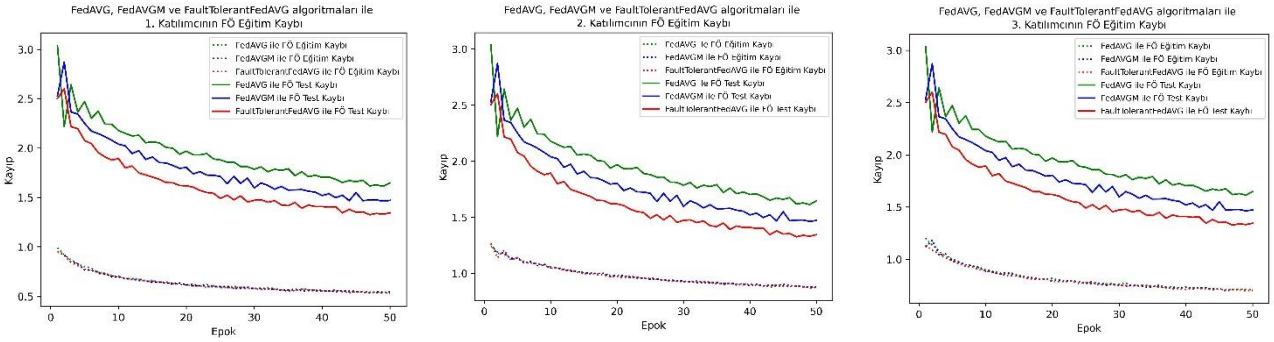


a) Katılımcı 1 b) Katılımcı 2 c) Katılımcı 3

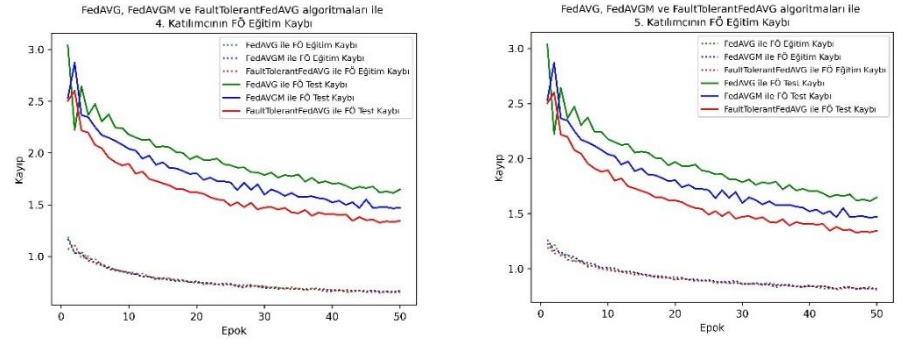


d) Katılımcı 4 e) Katılımcı 5

Şekil 10. MobileNet V3 small modelinin LÖ, MÖ ve FÖ konseptlerine göre FÖ Eğitim ve Test Kayıpları



a) Katılımcı 1 b) Katılımcı 2 c) Katılımcı 3



b) Katılımcı 4 e) Katılımcı 5

Şekil 11. ResNet-18 modelinin LÖ, MÖ ve FÖ konseptlerine göre FÖ Eğitim ve Test Kayıpları

Gelecek Çalışmalar

Mevcut çalışmanın ileride farklı birleştirme algoritmaları üzerinde test edilmesi, veri setinin farklı medikal görüntüler üzerinde uygulanması ve özgün birleştirme algoritmalarının tasarlanması planlanmaktadır.

Kaynaklar

[1] 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.

[2] "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)."

[3] 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.

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

[5] X. Huang, Y. Ding, Z. L. Jiang, S. Qi, X. Wang, and Q. Liao, "DP-FL: a novel differentially private federated learning framework for the unbalanced data," *World Wide Web*, vol. 23, no. 4, pp. 2529–2545, Jul. 2020, doi: 10.1007/s11280-020-00780-4.

[6] M. NERGİZ, "Collaborative Artifical Intelligence Concept: Federated Learning Review," *DÜMF Mühendislik Derg.*, Jun. 2022, doi: 10.24012/dumf.1130789.

[7] A. Nilsson, S. Smith, G. Ulm, E. Gustavsson, and M. Jirstrand, "A performance evaluation of federated learning algorithms," in *DIDL 2018 - Proceedings of the 2nd Workshop on Distributed Infrastructures for Deep Learning, Part of Middleware 2018*, Dec. 2018, pp. 1–8, doi: 10.1145/3286490.3286559.

[8] S. Ek, F. Portet, P. Lalanda, and G. Vega, "A Federated Learning Aggregation Algorithm for Pervasive Computing: Evaluation and Comparison," Oct. 2021, doi: 10.1109/PERCOM50583.2021.9439129.

[9] 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.

[10] "MNIST dataset," [Online]. Available: https://github.com/myleott/mnist_png.

[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," Dec. 2015, [Online]. Available: http://arxiv.org/abs/1512.03385.

[12] F. Ramzan *et al.*, "A Deep Learning Approach for Automated Diagnosis and Multi-Class Classification of Alzheimer's Disease Stages Using Resting-State fMRI and Residual Neural Networks," *J. Med. Syst.*, vol. 44, no. 2, Feb. 2020, doi: 10.1007/s10916-019-1475-2.

[13] A. Howard *et al.*, "Searching for MobileNetV3."

[14] T.-M. H. Hsu, H. Qi, and M. Brown, "Measuring the Effects of Non-Identical Data Distribution for Federated Visual Classification," Sep. 2019, [Online]. Available: http://arxiv.org/abs/1909.06335.

[15] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated Learning with Non-IID Data," 2018, [Online]. Available: http://arxiv.org/abs/1806.00582.

[16] "PYTORCH," [Online]. Available: https://pytorch.org/vision/stable/models.html.