T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

MEDİKAL VERİLERİN SINIFLANDIRILMASINDA FEDERE ÖĞRENME

Hazırlayan
Beyza Nur AKŞİT

Danışmanlar
Prof. Dr. Bahriye AKAY
Assoc. Prof. Dr. Adam SLOWIK

Yüksek Lisans Tezi

Ağustos 2023
KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

MEDİKAL VERİLERİN SINIFLANDIRILMASINDA FEDERE ÖĞRENME

(Yüksek Lisans Tezi)

Hazırlayan
Beyza Nur AKŞİT

Danışmanlar
Prof. Dr. Bahriye AKAY
Assoc. Prof. Dr. Adam SLOWIK

Yüksek Lisans Tezi

Ağustos 2023
KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Beyza Nur AKŞİT

İmza

“Medikal Verilerin Sınıflandırılmasında Federe Öğrenme” adlı Yüksek Lisans Tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi’ ne uygun olarak hazırlanmıştır.

Hazırlayan
Beyza Nur AKŞİT
İmza

Danışman
Prof. Dr. Bahriye AKAY
İmza

Danışman
Assoc. Prof. Dr. Adam SLOWIK
İmza

Bilgisayar Mühendisliği ABD Başkanı

Prof. Dr. Veysel ASLANTAŞ
İmza

TEŞEKKÜR

Bana çalışmalarım süresince her türlü yardımı ve fedakârlığı sağlayan sevgili aileme, tez çalışmam sürecinde her türlü desteği veren Arş. Gör. Meryem ALTINGÖZ ve Arş. Gör. Demet KARACA hocalarıma, çalışmalarım sırasında bilgi ve deneyimleriyle yolumu aydınlatan, samimiyetle her türlü desteğini esirgemeyen kıymetli danışman hocam Prof. Dr. Bahriye AKAY'a, ve beni "Koszalin University of Technology " üniversitesine davet ederek çalışmalarımı inceleyip, çalışmalarıma yön veren ikinci danışmanım Assoc. Prof. Dr. Adam SLOWIK'e teşekkür ederim.

Beyza Nur AKŞİT

Ağustos 2023, KAYSERİ

MEDİKAL VERİLERİN SINIFLANDIRILMASINDA FEDERE ÖĞRENME

Beyza Nur AKŞİT

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Ağustos 2023
Danışmanlar: Prof. Dr. Bahriye AKAY, Assoc. Prof. Dr. Adam SLOWIK

ÖZET

Medikal alanda yapay zekâ ve derin öğrenme tekniklerinin kullanılması, hastalıkların daha hızlı ve doğru bir şekilde teşhis edilmesini ve tedavi süreçlerinin iyileştirilmesini sağlamaktadır. Medikal verilerin içerdikleri hassas bilgiler nedeniyle merkezi sunucuda toplanması ve depolanması, veri güvenliği risklerini beraberinde getirir. Bu nedenle, verilerin merkezi sunucuya gönderilmeden uç noktalarda kaldığı ve sadece güncellenmiş yerel model parametrelerinin merkezi sunucuya gönderildiği federe öğrenme yaklaşımları kullanılır. Bir federe öğrenme yaklaşımı olan FedAvg, federe öğrenme sürecine katılan tüm uç noktaların yerel model parametrelerinin ortalamasını alarak merkezi sunucudaki küresel modeli günceller. Ancak, tüm uç noktaların yerel model parametrelerini küresel model güncellemesinde kullanana bu yaklaşım küresel model performansında yavaş yakınsama ve düşük performans gibi durumları ortaya çıkarabilir. Bu tez çalışmasında, bu sınırlamaları ortadan kaldırmak için tüm uç noktalar yerine en yüksek yerel model test doğruluğuna sahip uç noktanın yerel model parametrelerini kullanarak küresel modeli güncelleyen FedBest yaklaşımı önerilmiştir. FedAvg ve FedBest yaklaşımları BloodMNIST, PathMNIST ve DermaMNIST veri setleri üzerinde yapılan deneylerle kıyaslanmıştır. Yapılan deneyler sonucunda, FedAvg'nin medikal sınıflandırmada başarılı olduğu, ancak FedBest yaklaşımının daha yüksek doğruluk oranları ve daha hızlı bir yakınsama sağladığı gözlemlenmiştir. Ayrıca iletişim topolojilerinin federe öğrenme yaklaşımlarının performansına olan etkileri incelenmiştir.

Anahtar Kelimeler: Federe Öğrenme, İşbirlikçi Öğrenme, Medikal Veri, Veri Gizliliği, Derin Öğrenme, İletişim Topolojileri, Star Topoloji, Ring Topoloji.

FEDERATED LEARNING FOR MEDICAL DATA CLASSIFICATION

Beyza Nur AKŞİT

Erciyes University, Graduate School of Natural and Applied Sciences
Master Thesis, August 2023
Supervisors: Prof. Dr. Bahriye AKAY, Assoc. Prof. Dr. Adam SLOWIK

ABSTRACT

The use of artificial intelligence and deep learning techniques in the medical field yields faster and more accurate diagnosis of diseases and improvement of treatment processes. The collection and storage of medical data on a central server brings security issues because it contains private information. Therefore, federated learning approaches are used, where data remains at clients without being sent to the central server, and only updated local model parameters are sent to the central server. FedAvg, one of federated learning approaches, updates the global model on the central server by averaging the local model parameters of all clients involved in the federated learning process. However, this approach that exploits the local model parameters of all clients in the global model update may suffer from slow convergence and poor performance. To overcome these limitations, in this thesis, a FedBest approach is proposed, which updates the global model using the local model parameters of the client with the highest local model testing accuracy, instead of all clients. In the experiments, the FedAvg and FedBest approaches were compared on the medical BloodMNIST, PathMNIST, and DermaMNIST datasets. From the results, it was observed that FedAvg was successful in medical classification, but the FedBest approach provided higher accuracy rates and a faster convergence. In addition, the effect of communication topologies on the performance of federated learning approaches were examined.

Keywords: Federated Learning, Collaborative Learning, Medical Data, Data Privacy, Deep Learning, Communication Topologies, Star Topology, Ring Topology.

İÇİNDEKİLER

MEDİKAL VERİLERİN SINIFLANDIRILMASINDA FEDERE ÖĞRENME

BİLİMSEL ETİĞE UYGUNLUK ii
YÖNERGEYE UYGUNLUK iii
KABUL VE ONAY iv
ÖNSÖZ v
ÖZET vi
ABSTRACT vii
İÇİNDEKİLER viii
TABLOLAR LİSTESİ x
ŞEKİLLER LİSTESİ xi
GİRİŞ 1

1. BÖLÜM

GENEL BİLGİLER ve LİTERATÜR ÇALIŞMASI

1.1. Problem Durumu 2
1.2. Araştırmanın Amacı 3
1.3. Araştırmanın Önemi ve Literatür Çalışması 4

2. BÖLÜM

YÖNTEM VE MATERYAL

2.1. Federe Öğrenme Mimarisi……...7
2.1.1. Federe Öğrenme Bileşenleri……9
2.1.2. Federe Öğrenme Türleri……10
2.1.2.1. Yatay Federe Öğrenme……..10
2.1.2.2. Dikey Federe Öğrenme……..11

2.1.2.3. Federe Transfer Öğrenme…….....11
2.1.3. Federe Öğrenme Kullanım Alanları……..……..12
2.1.4. Federated Averaging (FedaAvg)……..13
2.1.5. Önerilen Yöntem: FedBest...……....15
2.2. Derin Öğrenme……17
2.2.1. Evrişimli Sinir Ağı…….....17
2.3. İletişim Ağ Topolojisi……..19
2.3.1. Star Topolojisi…….…….20
2.3.2. Ring Topolojisi…….…21

3. BÖLÜM
DENEYSEL ÇALIŞMALAR VE BULGULAR

3.1. Çalışmada Kullanılan Medikal Veri Setleri…….....24
3.1.1. MedMNIST…….....24
3.1.1.1. BloodMNIST…….……..25
3.1.1.2. PathMNIST…….....26
3.1.1.3. DermaMNIST…….....27
3.2. MedMNIST Veri Setleri Deney Sonuçları……28
3.2.1. BloodMNIST Veri Seti Deney Sonuçları……..28
3.2.2.PathMNIST Veri Seti Deney Sonuçları……34
3.2.3. DermaMNIST Veri Seti Deney Sonuçları…….……...40
3.3. İletişim Topolojilerinin Performans Üzerindeki Etkileri……46

4. BÖLÜM
TARTIŞMA-SONUÇ ve ÖNERİLER

4.1.Tartışma……...50
4.2.Sonuç ve Öneriler ……..51

KAYNAKÇA……..53
ÖZGEÇMİŞ ……...58

TABLOLAR LİSTESİ

Tablo 2.1. FedBest algoritması……..…….15

Tablo 3.1. CNN modelinin yapısı ve parametre sayısı…….24

Tablo 3.2. BloodMNIST, PathMNIST ve DermaMNIST eğitim, doğrulama ve test veri sayıları…….29

Tablo 3.3. BloodMNIST eğitim, doğrulama ve test veri setleri miktarları…….…..30

Tablo 3.4. BloodMNIST veri seti deney sonuçları……...…29

Tablo 3.5. PathMNIST eğitim, doğrulama ve test veri setleri miktarları…….34

Tablo 3.6. PathMNIST veri seti deney sonuçları……....35

Tablo 3.7. DermaMNIST eğitim, doğrulama ve test veri setleri miktarları…….....….40

Tablo 3.8. DermaMNIST veri seti deney sonuçları…….…41

Tablo 3.9. BloodMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar.48

Tablo 3.10. PathMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar..49

Tablo 3.11. DermaMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar ……..…….……...50

ŞEKİLLER LİSTESİ

Şekil 2.1. Federe öğrenme süreç şeması…….8

Şekil 2.2. Yatay federe öğrenme şeması……..11

Şekil 2.3. Dikey federe öğrenme şeması……..11

Şekil 2.4. Federe transfer öğrenme……..12

Şekil 2.5. FedAvg algoritması…….13

Şekil 2.6. FedAvg süreç şeması……14

Şekil 2.7. FedBest süreç şeması……...……16

Şekil 2.8. Derin öğrenme ve makine öğrenimi özet süreci……..17

Şekil 2.9. CNN mimarisi…….19

Şekil 2.10. Federe öğrenmede kullanılan iletişim ağı topolojisi örnekleri …….19

Şekil 2.11. Star topolojisi…….20

Şekil 2.12. Ring topolojisi……22

Şekil 3.1. MedMNIST 'e genel bakış ……..25

Şekil 3.2. BloodMNIST veri seti çoklu sınıf örnekleri……26

Şekil 3.3. PathMNIST veri seti çoklu sınıf örnekleri……26

Şekil 3.4. DermaMNIST veri seti çoklu sınıf örnekleri……27

Şekil 3.5. Birinci eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri……....31

Şekil 3.6. İkinci eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri…….32

Şekil 3.7. Üçüncü eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri……..33

Şekil 3.8. Birinci eğitim sonu PathMNIST veri seti deney sonuçları grafikleri……..37

Şekil 3.9. İkinci eğitim sonu PathMNIST veri seti deney sonuçları grafikleri ……..…38

Şekil 3.10. Üçüncü eğitim sonu PathMNIST veri seti deney sonuçları grafikleri……...39

Şekil 3.11. Birinci eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri…….43

Şekil 3.12. İkinci eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri…….…44

Şekil 3.13. Üçüncü eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri…....45

GİRİŞ

Teknolojinin ilerlemesi ve veri boyutundaki artışla birlikte verilerin gizliliği ve güvenliği odak nokta haline gelmiştir. Ülkeler veri mahremiyetini sağlamak adına kanun seviyesinde çeşitli önlemler almıştır. GDPR- Genel Veri Koruma Yönetmeliği ve KVKK –Kişisel Verileri Koruma Kanunu bu mevzuatlardan bazılarıdır. Bu yasa ve yönetmeliklerin oluşturulması, yapay zekânın geleneksel veri işleme moduna değişen derecelerde yeni zorluklar getirmektedir. Veri mahremiyetini dikkate alacak şekilde yeni nesil bir yapay zekâ yaklaşımı olan federe öğrenme yaklaşımı geliştirilmiştir [1,2]. Federe öğrenme, uç noktalardaki verilerin uç noktalardan hiç çıkmadığı, eğitim sürecinin birçok uç nokta arasında dağıtıldığı, veri yerine model bilgilerinin paylaşıldığı işbirlikçi bir makine öğrenmesi yöntemidir. Bu şekilde verinin olduğu yerde işlenmesi ile veri mahremiyet ihlali riskleri giderilmiş olur.

Bir federe öğrenme yaklaşımı olan FedAvg, federe öğrenme sürecine katılan tüm uç noktaların yerel model parametrelerinin ortalamasını alarak merkezi sunucudaki küresel modeli günceller. Ancak, tüm uç noktaların yerel model parametrelerini küresel model güncellemesinde kullanana bu yaklaşım küresel model performansında yavaş yakınsama ve düşük performans gibi durumları ortaya çıkarabilir. Bu tez çalışmasında, bu sınırlamaları ortadan kaldırmak için tüm uç noktalar yerine en yüksek yerel model test doğruluğuna sahip uç noktanın yerel model parametrelerini kullanarak küresel modeli güncelleyen FedBest yaklaşımı önerilmiştir. FedAvg ve FedBest yaklaşımları medikal veri setleri üzerinde yapılan deneylerle kıyaslanmıştır.

Tezin organizasyonu şu şekildedir: Birinci bölümde konuyla ilgili literatüre sunulan çalışmalar verilmiştir. İkinci bölümde, federe öğrenme yöntemleri, derin öğrenme modeli ve çalışmada kullanılan iletişim topolojileri ile ilgili bilgiler verilerek federe öğrenme mimarisi için önerilen yöntem sunulmuştur. Üçüncü bölümde elde edilen sonuçlar verilmiştir. Dördüncü bölümde ise tartışma ve sonuca yer verilmiştir.

1. BÖLÜM

GENEL BİLGİLER ve LİTERATÜR ÇALIŞMASI

1.1. Problem Durumu

Sağlık sistemi ve süreçlerinin karmaşık yapısı nedeniyle veriler tek bir merkezde değil, farklı sağlık kurumları, hastaneler veya klinikler gibi çeşitli yerlerde tutularak yönetilirler. Medikal alanda hekimlerin karar destek sürecinde yapay zekâ modelleri başarıyla kullanılmaktadır. Bu modeller, hastalıkların tanısında, tedavi planlamasında ve hastaların sağlık durumlarını izlemede önemli bir rol oynamaktadır [3]. Geleneksel yapay zekâ modelleri, verilerin merkezi bir sunucuda birleştirilerek daha yüksek bir veri kütlesi ile daha yüksek başarı elde edebilirler. Ancak sağlık alanında bu verilerin merkezi bir sunucuya aktarılması, GDPR gibi Avrupa Birliği'nde uygulanan sıkı veri koruma kanunları ile çelişir. GDPR- Genel Veri Koruma Yönetmeliği ve KVKK – Kişisel Verileri Koruma Kanunu gibi yasa ve yönetmeliklerin oluşturulması, yapay zekânın geleneksel veri işleme moduna değişen derecelerde yeni zorluklar getirmektedir. Bu nedenle veri mahremiyetini dikkate alacak şekilde yeni nesil bir yapay zekâ yaklaşımı olan federe öğrenme yaklaşımı geliştirilmiştir [1,2].

Federe öğrenme, medikal alanında sağlık uygulamaları, doğal dil işleme, finans ve e-ticaret gibi birçok alanda uygulanmaktadır. Bu uygulama alanları, farklı veri kaynakları arasında veri paylaşımının önemli olduğu alanları kapsamaktadır. Örneğin, sağlık uygulamalarında farklı hastanelerde ve kliniklerde elde edilen medikal verilerin birleştirilerek daha kapsamlı sonuçlar elde edilmesi ve medikal verilerin hassas yapısı nedeniyle yapay zekâ sistemlerinin geliştirilmesi sırasında ortaya çıkan veri güvenliği ve gizlilik ihlallerini önlemek amacıyla geliştirilmiş bir öğrenme yöntemidir.

1.2. Araştırmanın Amacı

Bu çalışmada kullanılan Federe öğrenme, veri gizliliğini korurken birden fazla kaynaktan gelen verilerle yapay zekâ modellerini eğitmek için kullanılan ve böylece veri paylaşımının önündeki birçok engeli ortadan kaldıran bir yöntemdir. Sağlıktaki veriler için federe öğrenme mimarisinin kullanılmasıyla hem hassas olan medikal veriler gizliliği sağlanacak hem de farklı hastanelerde bulunan karmaşık verilerin paylaşılmasına gerek kalmadan model paylaşımı ile birçok kurumdaki verilerden faydalanılarak medikal verilerin sınıflandırılmasında daha global ve başarılı sonuçlar veren modeller eğitilebilecektir.

Federe öğrenme yaklaşımlarından biri olan FedAvg, uç noktalardan gelen yerel model parametrelerinin ortalamasının alınarak küresel modelin güncellenmesini sağlar. Ancak bu yöntemde, uç noktalar farklı model performanslarına sahip olduğunda yakınsama süresi ve performansı etkileyen sınırlamalar ortaya çıkar. Bu çalışmada bu sınırlamaları ortadan kaldırmak için en yüksek yerel model test doğruluğuna sahip uç noktanın yerel model parametrelerini kullanarak küresel modeli güncelleyen FedBest isimli bir yaklaşım önerilmiştir. FedBest, tüm uç noktaların yerine en yüksek test doğruluğuna sahip uç noktanın yerel model parametrelerini kullanır. Bu sayede, en iyi performansa sahip uç noktanın bilgisi daha fazla değerlendirilir.

Federe öğrenme mimarilerinde uç noktaların iletişiminde farklı topolojiler yakınsama hızını etkileyebilirler. Star ve Ring topolojileri, federe öğrenme iletişim yapısında kullanılan iki temel iletişim topolojisidir. Star topolojisinde, uç noktalar doğrudan merkezi sunucu ile iletişim kurar ve model güncellemeleri merkezi sunucu tarafından yönetilir. Ring topolojisinde ise uç noktalar birbirleriyle dairesel bir yapıda iletişim kurar, yani her uç nokta komşusu ile veri ve model güncellemelerini paylaşır.

Bu çalışmanın amacı, medikal verilerin sınıflandırılmasında farklı federe öğrenme yaklaşımlarının performansını değerlendirmektir. Aynı zamanda Star ve Ring topolojileri altında kullanılan FedAvg ve FedBest algoritmalarının medikal verilerin sınıflandırılması üzerindeki performans etkisini incelemek ve en uygun iletişim topolojisi ve algoritma seçimini belirlemektir.

1.3. Araştırmanın Önemi ve Literatür Çalışması

Veri gizliliğini korumak ve güvenlik risklerini azaltmak için kullanılan dağıtılmış bir öğrenme yöntemi olan federe öğrenme, sağlık hizmetlerinde büyük bir geleceğe sahiptir. Her tıp enstitüsünün çok sayıda hasta verisi olabilir, ancak bu kendi tahmin modellerini eğitmek için yeterli olmayabilir [4]. Medikal veri sınıflandırması bağlamında federe öğrenme, veri paylaşımına gerek kalmadan birden çok sağlık hizmeti sağlayıcısından alınan veriler üzerinde bir modelin eğitilmesine olanak sağlayabilir.

Lee ve ark. (2018), farklı hastanelere dağıtık hasta bilgilerini paylaşmadan bir federe hasta eşleştirme yöntemi önermişlerdir. Bu hasta eşleştirme yönteminin, doktorların genel durumu özetlemelerine ve hastaları daha fazla deneyimle tedavi etmeye yardımcı olabileceğini belirtmişlerdir [5]. Huang ve ark. (2019), yoğun bakım verilerinin önemli olduğu ancak farklı kaynaklarda ve cihazlarda saklandığı için veri paylaşımının zor olduğu bir ortamda, federe öğrenme yöntemini kullanarak verilerin paylaşılmasına gerek kalmadan hassas verilerin kullanılmasını sağlamayı amaçlamışlardır. Çalışmada, LoAdaBoost yöntemi kullanılarak yapılan deneylerde LoAdaBoost yönteminin temel yönteme göre daha yüksek tahmin doğruluğu ve daha düşük hesaplama karmaşıklığı elde ettiği gösterilmiştir [6]. Nazir ve Kaleem (2023), derin sinir ağları ile medikal görüntü analizinde federe öğrenme uygulamalarını incelemiş, federe öğrenme model performansını artırmak için yapılan bazı çalışmalara değinmiş ve federe öğrenmenin gelecekteki araştırma yönlerini vurgulamışlardır [7]. Kumar ve ark. (2021), Covid-19 teşhisi amacıyla veri mahremiyetini sağlayıp, doğruluğu ve iletişim verimliliğini artırmak için yeni bir yöntem önermişler ve kullandıkları yöntemin iyi bir performans gösterdiğini belirtmişlerdir [8].

Price ve Cohen (2019), hastaların mahremiyetinin yasal ve ahlaki zorluklarını analiz etmiş ve gelecekte veri mahremiyeti göz önünde bulundurarak hasta verilerinin nasıl kullanabileceklerini tartışmışlardır. Veri miktarının azlığının ve etiketlenmiş veri yetersizliğinin medikal veri işlemede karşılaşılan iki ana sorun olduğunu ve federe öğrenme yönteminin bu sorunları çözebileceğini ifade etmişlerdir [9]. Lee ve ark. (2019), doktorlara hastaların ileriye dönük hastalık teşhislerinde yardımcı olmak amacıyla gerçek hasta verilerini tıbbi teşhis kanıtlarına dönüştürebilmek için Apollo ağına dayalı bir federe öğrenme ağı tasarlamış ve uygulamışlardır [10]. Li ve ark. (2019), yaptıkları çalışmada

federe öğrenme yönteminde hasta verilerinin gizliliğini korumak için diferansiyel gizlilik tekniklerinin uygulanmasını araştırmışlardır. BraTS veri setinde beyin tümörü segmentasyonu için federe öğrenme yöntemlerini uygulayıp ve değerlendirmişlerdir. Deneysel sonuçlar, daha güçlü gizlilik koruma önlemleri alındığında, modelin performansının düşebileceğini veya daha zayıf gizlilik koruması sağlandığında modelin performansının artabileceğini bu nedenle model performansı ile veri gizliliği koruma maliyetleri arasında bir denge (ödünleşim) olduğunu göstermişlerdir [11]. Sheller ve ark. (2018), yaptıkları çalışmada hasta verilerini paylaşmadan derin öğrenme modeli eğitilmesini mümkün kılan çok kurumlu bir iş birliği için federe öğrenmenin kullanımını tanıtmışlardır. Nicel sonuçları, birleşik semantik segmentasyon modellerinin multimodal beyin taramalarındaki performansının, veri paylaşımıyla eğitilen modellerin performansına yakın değerde olduğunu göstermiştir [12].

Preuveneers ve ark. (2018), yaptıkları çalışmada federe öğrenme sistemi kurulumlarında kötü niyetli kullanıcıların yerel makine öğrenimi modellerini kötü niyetli eğitim örnekleriyle zehirlemesinin zorluğunu ele almışlardır. Çözüm olarak, blok zincir tabanlı federe öğrenme yöntemi önerilmiş ve bu yöntemle federe öğrenime katkıda bulunan tarafların sorumlu tutulabileceği ve model güncellemelerinin denetlenebileceği belirtilmiştir [13]. Roth ve ark. (2020), yaptıkları çalışmada gerçek dünya iş birliği ortamında medikal görüntüleme sınıflandırma modelleri oluşturmak için federe öğrenimi kullanımını araştırmışlardır. Yedi klinik kurum, Meme Görüntüleme, Raporlama ve Veri Sistemine (BI-RADS) dayalı meme yoğunluğu sınıflandırması amacıyla bir model eğitmek için federe öğrenme sistemine katılmışlardır. Sonuçlar, federe öğrenme kullanılarak eğitilen modellerin, yalnızca bir kurumun yerel verileriyle eğitilen modellerden ortalama %6,3 daha iyi performans elde ettiğini göstermiştir [14]. Ju ve ark. (2020), elektroensefalogram (EEG) sinyal sınıflandırması için federe öğrenmeye dayanan federe transfer öğrenimi (FTL) adlı veri gizliliğini koruyan yenir bir derin öğrenme mimarisi önermişlerdir. FTL, EEG verilerini yerel cihazlarda tutarsak kullanıcı gizliliğini korumuş ve bir girdi olarak uzamsal kovaryans matrisini kullanarak, EEG-MI görevinde diğer güncel derin öğrenme yöntemlerinden %6 daha iyi performans sağlamıştır [15]. BDair ve ark. (2021), Semi-supervised Federe öğrenmede (SSFL) model performansını koruyarak, gizlilik ihlalini önlemek ve iletişim maliyetini azaltmak için Peer Anonimleştirmesi (PA) yöntemini önermişlerdir. 38.000'den fazla cilt lezyonu

görüntüsünün kullanıldığı cilt lezyonu sınıflandırması için FedPerl'i değerlendirmişlerdir. PA, gizliliği korurken performansı etkilemeden iletişim maliyetini düşürmüş ve FedPerl, temel değerlere ve son teknoloji SSFL'ye göre sırasıyla %15,8 ve %1,8 oranında daha iyi performans elde etmiştir [16].

Literatüre sunulmuş bu çalışmalardan görüldüğü üzere federe öğrenme yaklaşımı sağlık alanında yaygın olarak kullanılmaya başlanmıştır. İncelenen çalışmalar federe öğrenme yöntemi kullanılarak eğitilen modellerin, yalnızca bir kurumun yerel verileriyle eğitilen modellerden ortalama olarak daha iyi performans gösterdiğini göstermiştir.

Bu çalışmanın federe öğrenme yöntemi araştırmalarına katkıları aşağıdaki gibidir:

1. Uç nokta seçimi ile en iyi test doğruluğuna sahip uç nokta yerel model parametrelerinin küresel model güncellemesinde kullanılmasına izin veren yeni bir yaklaşım önermek ve daha yüksek küresel model doğruluğu ile hızlı yakınsama sağlamak.

2. Doğrulama amacıyla yaygın olarak kullanılan FedAvg yaklaşımı ile kıyaslamak.

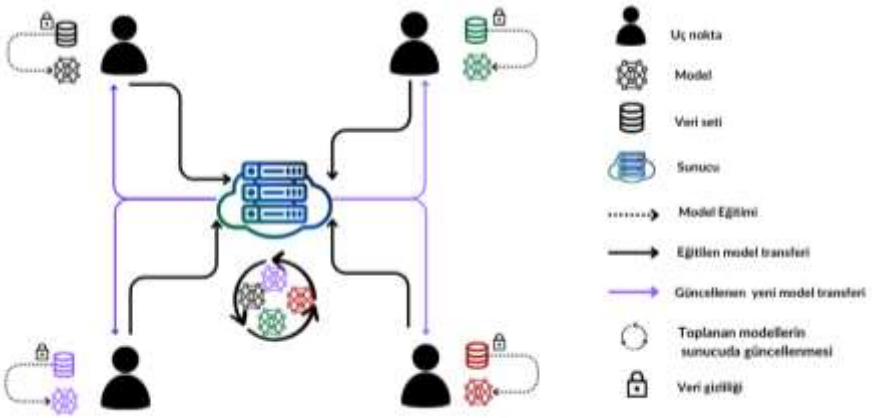
3. Uç noktaların iletişiminde farklı topolojilerin etkisini incelemek ve Federe öğrenme yaklaşımlarının iletişim verimliliğini artırmak.

2. BÖLÜM

YÖNTEM VE MATERYAL

2.1. Federe Öğrenme Mimarisi

Klasik makine öğrenme modelleri, eğitim verilerinin bir makinede veya bir veri merkezinde toplanmasını gerektirir. Bu durumda veri ihlalleri ile karşılaşılabilir. Federe öğrenme, birden çok uç noktanın kendi özel verilerini paylaşmadan, merkezi bir sunucuda birleştirmeden küresel bir modelin iş birliği içinde eğitilmesine olanak tanıyan bir makine öğrenimi yöntemidir. Veri sahibi olan uç noktalar, kendi yerel verilerini kullanarak merkezi sunucudan gelen modeli eğitir ve eğitilen model parametrelerini merkezi sunucuya geri gönderirler. Merkezi sunucu, uç noktalardan gelen model parametrelerini bir arada değerlendirerek küresel modeli günceller. Bu süreç, model eğitiminde belirlenen durma kriteri elde edilene kadar yinelenir. Federe öğrenme, verileri uç noktalarda tutarak merkezi makine öğrenimi sistemleriyle ilişkili gizlilik ve güvenlik risklerini giderir. Ayrıca, farklı veri dağılımları veya farklı veri türleri gibi heterojen verilere sahip uç noktalar arasında iş birliğine de olanak tanır [17]. Federe öğrenmenin temel süreci Şekil 2.1'de sunulmuştur.



Şekil 2.1. Federe öğrenme süreç şeması.

Şekil 2.1'de görüldüğü gibi federe öğrenme süreci 4 temel adımdan oluşur:

1. Uç noktalara merkezi sunucudan küresel model gönderilir.
2. Her uç nokta, merkezi sunucudan gelen modeli kendi yerel verileriyle eğitmesi sonucu yerel model parametreleri güncellenir.
3. Uç noktalar, güncellenen yerel model parametrelerini merkezi sunucuya geri gönderir.
4. Merkezi sunucu, güncellenen parametreleri belirli federe öğrenme algoritmalarını kullanarak birleştirir. Bu döngü model yakınsayana kadar devam eder.

Federe öğrenme, geleneksel makine öğrenimi yöntemlerine yöntemlere kıyasla bazı avantajlar sunmaktadır [18]:

- **Ölçeklenebilirlik:** Federe öğrenme, model parametrelerinin güncellenmesi yoluyla çeşitli cihazların iş birliği içinde öğrenmesini kolaylaştırarak, ağın genişlemesini mümkün kılar.
- **Düşük iş hacmi ve yüksek gecikme süresi zorluklarına çözüm:** Yerel modeller eğitmek, tek bir merkezi modeli eğitmeye kıyasla gecikmelerin ve güç tüketiminin azaltılmasına yardımcı olur.
- **Doğruluğu artırır:** Federe öğrenme sürecinde küresel model, birçok uç noktadaki yerel model parametrelerinin bir araya getirilmesi ile güncellendiğinden, model doğruluğuna çoğunlukla olumlu katkıda bulunur.
- **Eğitim süresinde ve eğitim maliyetinde azaltma:** Bir modeli sunucuda merkezi olarak eğitmek yerine, çeşitli yerel modelleri eğitmek ve ardından merkezi küresel bir model oluşturmak daha az zaman alan bir süreçtir. İş yükü iş birliğindeki uç noktalara dağıtıldığından eğitim maliyeti de daha düşüktür.
- **Gizliliği ve güvenlik:** Eğitim verileri iş birliğine katılan uç noktalardan ayrılmadığından, tüm hassas bilgiler yerelde kalır, böylece kişisel verilerin gizliliği ve güvenliği sağlanır.

- **Veri minimizasyonu:** Federe öğrenme, yalnızca öğrenilen modelin merkezi olarak işlenmesini ve ham verilerin gizli kalmasını sağlayarak, ilgili ve sadece gerek duyulan verilerle işlem yapar.

2.1.1. Federe Öğrenme Bileşenleri

Federe öğrenmenin bileşenleri, bu öğrenme yönteminin temel yapı taşlarını oluşturan unsurlardır. Bu bileşenler, federe öğrenmenin işleyişini ve başarısını etkileyen önemli unsurlardır. Federe öğrenmenin bileşenleri şunlardır [19]:

- **Katılımcılar (Uç noktalar):** Katılımcılar**,** federe öğrenme sürecinde veri sahipleri ve iş birliğinden faydalanan işbirlikçilerdir [20]. Katılımcıların donanımsal özellikleri, federe öğrenme sürecine katılan katılımcı sayıları ve iş birliğine katılma kararlılığı, katılımcılar üzerindeki verinin dağılımı federe öğrenme süreci başarısına direk olarak etki eder.

- **Merkezi Sunucu (Server):** Merkezi sunucu, tüm uç noktaların öğrenme modellerini güncellemek ve birleştirmek için kullanılan merkezi noktadır. Uç noktalar, eğittikleri yerel modellerin parametrelerini merkezi sunucuya gönderir ve merkezi sunucu bu parametreleri kullanarak küresel modeli günceller.

- **Küresel Model:** Öğrenme modeli (küresel model), federe öğrenme sürecinde kullanılan yapay zekâ modelidir. Uç noktalarda yerel olarak eğitilen bu model, veri setlerini analiz ederek öğrenme sürecini gerçekleştirir.

- **Veri Minimizasyonu:** Ham veriler yerel cihazlarda kalır ve sadece güncellenmiş öğrenme parametreleri merkezi sunucuya gönderilir, bu da veri güvenliğini artırır.

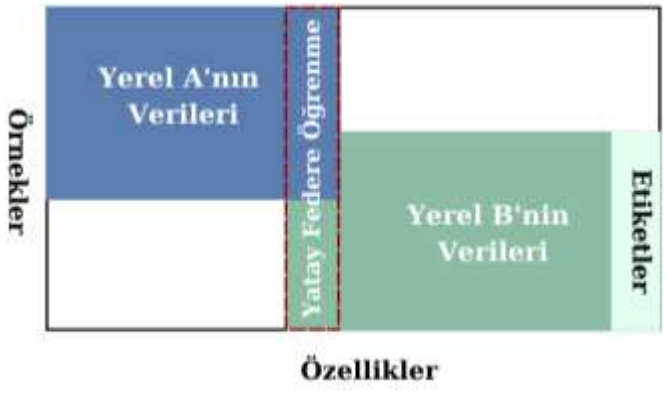
- **Model Güncelleme Stratejileri:** Federe öğrenme, merkezi sunucu ve uç noktalar arasındaki küresel model güncellemelerini yönetmek için çeşitli yaklaşımlar kullanır. En temel ve kullanımı en yaygın olan FedAvg ‘dir [21]. Ayrıca FedAvg dışında kullanılan başka model birleştirme stratejileri vardır [22]. FedAvgM [23], FedProx [24], FedOpt [25], FedAdagrad [26], FedAdam [26] ve FedYogi [26] bunlardan bazılarıdır.

2.1.2. Federe Öğrenme Türleri

Federe öğrenme mimarisinde kullanılacak yöntemi belirlemek için katılımcıların öznitelik veya örnek uzayında paylaştığı ortak yönlerin belirlenmesi gerekmektedir. Bu bağlamda, veri dağılımına dayalı olarak üç farklı kategoriye ayrılır: Yatay Federe Öğrenme, Dikey Federe Öğrenme ve Federe Transfer Öğrenme [27].

2.1.2.1. Yatay Federe Öğrenme

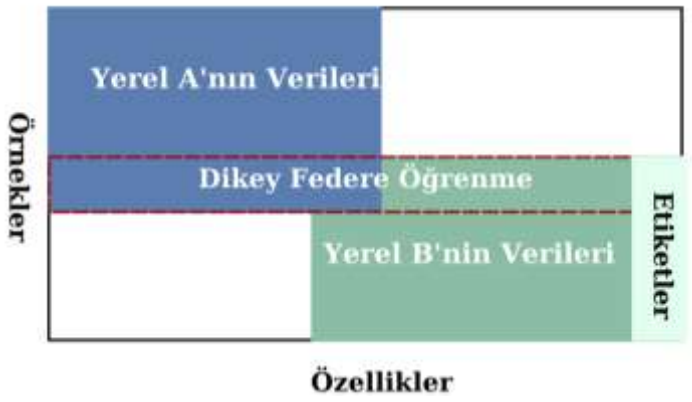
Yatay Federe Öğrenme, federe öğrenme türlerinden biridir ve genellikle homojen veri dağılımına sahip işbirlikçi uç noktalar arasında kullanılır. Bu yaklaşımda, işbirlikçi uç noktalar benzer özelliklere sahip verilere sahiptir ve eğitim verileri hemen hemen aynı özniteliklere sahip olan verilerden oluşur. Yatay Federe Öğrenme, bu homojen veri dağılımı sayesinde işbirlikçi uç noktaların eğitim verilerini doğrudan birleştirmek ve küresel bir model oluşturmak için kullanılır. Yatay Federe Öğrenme yöntemi, özellikle medikal alanda kullanılan bir senaryoda gerçek hayatta uygulanabilir. Örneğin, farklı hastaneler, farklı bölgelerde bulunuyor ve kendi hastalarından elde ettikleri medikal verilere sahiplerdir. Bu hastaneler, gizlilik nedeniyle verilerini merkezi bir sunucuda paylaşmak istemeyebilirler. Böyle bir senaryoda yatay federe öğrenme yöntemi devreye girecektir. Her bir hastane, kendi yerel verilerini kullanarak hasta mahremiyeti ihlal edilmeden ortak model oluşturulabilir. Bu sayede, tüm hastaneler birbirlerinin verilerinden yararlanabilir ve daha iyi bir medikal sınıflandırma modeli geliştirmek için iş birliği yapabilirler. Yatay federe öğrenme şeması Şekil 2.2'de sunulmuştur.



Şekil 2.2. Yatay federe öğrenme şeması.

2.1.2.2. Dikey Federe Öğrenme

Dikey Federe Öğrenme, aynı örnek uzayına ancak ayrı öznitelik uzayına sahip olma senaryosunda kullanılır. Örneğin, gerçek hayatta bir bankanın müşteri verilerini ele alalım. Banka, müşterilerin finansal bilgilerini ve demografik bilgilerini toplamaktadır. Ancak, finansal bilgiler (örneğin gelir, harcama alışkanlıkları) banka tarafından toplanırken, demografik bilgiler (örneğin yaş, cinsiyet) farklı bir kurum veya veri sahibi tarafından elde edilebilir. Bu durumda, banka ve diğer veri sahibi (örneğin bir kamu kurumu) arasında Dikey Federe Öğrenme kullanılabilir. Her iki veri sahibi, kendi verilerini yerel olarak tutar ve sadece belirli sütunları (örneğin demografik bilgiler) paylaşır. Bu paylaşılan sütunlar üzerinden ortak bir model oluşturulur ve güncellenir. Dikey federe öğrenme şeması Şekil 2.3'te sunulmuştur.

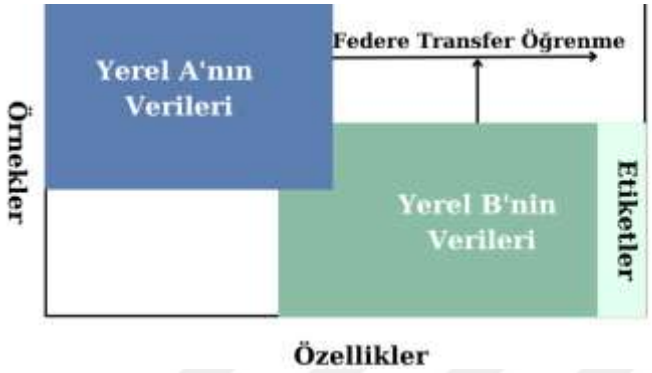


Şekil 2.3. Dikey federe öğrenme şeması.

2.1.2.3. Federe Transfer Öğrenme

Yatay ve Dikey Federe öğrenmedeki 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. Bir hastane, kendi bünyesindeki verileri kullanarak bir hastalık tespit modeli geliştirmiş olabilir. Bu model, hastalık teşhisinde oldukça başarılı olmuş olabilir. Ancak, başka bir hastanenin elinde farklı tipte veriler ve farklı bir hastalık tespit görevi için yeterli veri bulunmayabilir. Bu durumda, Federe Transfer Öğrenme kullanılabilir. Birincil hastane, kendi modelini ikincil hastaneye gönderir. İkincil hastane, kendi verilerini kullanarak bu modeli eğitebilir ve öğrenilen bilgiyi kendi hastalık tespit görevine

uyarlayabilir. Bu sayede, ikincil hastane daha az miktarda veriyle bile kendi hastalık tespit modelini geliştirebilir ve başarı oranını artırabilir. Federe Transfer öğrenme şeması Şekil 2.4'te sunulmuştur.



Şekil 2.4. Federe transfer öğrenme.

2.1.3. Federe Öğrenme Kullanım Alanları

- **Sağlık Uygulamaları:** Sağlık alanında, özel ve hassas hasta verilerini merkezi bir sunucuda toplamak yerine, federe öğrenme kullanılarak verileri yerel uç noktalarda tutarak model eğitilebilir. Bu, hastane veya sağlık kuruluşları arasında iş birliği yaparak daha güçlü ve genelleştirilebilir medikal teşhis veya tedavi modelleri oluşturmada faydalı olabilir. Literatürde sağlık alanında federe öğrenme tabanlı Çok Katmanlı Algılayıcılar [28], Evrişimsel Sinir Ağları [29], Oto Kodlayıcı [30] modelleri ile araştırmalar yapılmıştır.

- **Doğal Dil İşleme:** Dil modellerinin eğitiminde federe öğrenme, kullanıcıların metin verilerini yerel cihazlarında koruyarak ve merkezi bir sunucuda toplamadan daha fazla gizlilik sağlayabilir. Böylece, metin tabanlı uygulamalarda daha güvenli ve özelleştirilmiş çözümler elde etmek mümkün olabilir. Bu kapsamda [31] 'de yazarlar, bir federe öğrenme mimarisi kullanarak Doğal Dil İşleme modelleri oluşturmanın mümkün olduğunu göstermişlerdir.

- **Finans:** Finansal kurumlar, müşteri verilerini gizli tutarak ve verileri merkezi bir sunucuda bir araya getirmeden müşteri profilleri veya kredi riski değerlendirmesi için öğrenme modelleri oluşturabilir. Bu, veri güvenliği açısından önemli bir avantaj sağlayabilir. Nitekim, müşteri mali durum takibi [32] ve açık bankacılık

[33] gibi finansal alanlarda federe öğrenme tabanlı araştırmalar literatürde yer bulmuştur.

- **E-Ticaret:** E-ticaret platformları, kullanıcıların satın alma alışkanlıkları hakkında öğrenme modelleri oluşturmak için federe öğrenme mimarisi kullanabilir. Böylece, kullanıcı verilerinin mahremiyetini koruyarak ve merkezi bir sunucuya ihtiyaç duymadan kişiselleştirilmiş öneriler sunabilirler. E-Ticaret işletmeleri, yatay federe öğrenme tabanlı araştırmalarla literatürde yer bulmuştur [34].

2.1.4. Federated Averaging (FedAvg)

Birleşik ortalama algoritması (FedAvg), federe öğrenme için yaygın olarak kullanılan bir algoritmadır [21]. FedAvg, iş birliği sürecinde veri gizliliğini koruyarak uç noktalardan gelen model parametrelerinin ortalamasını alarak merkezi sunucudaki küresel modeli günceller. Şekil 2.5'te FedAvg algoritması sunulmuştur.

FedAvg Algoritması

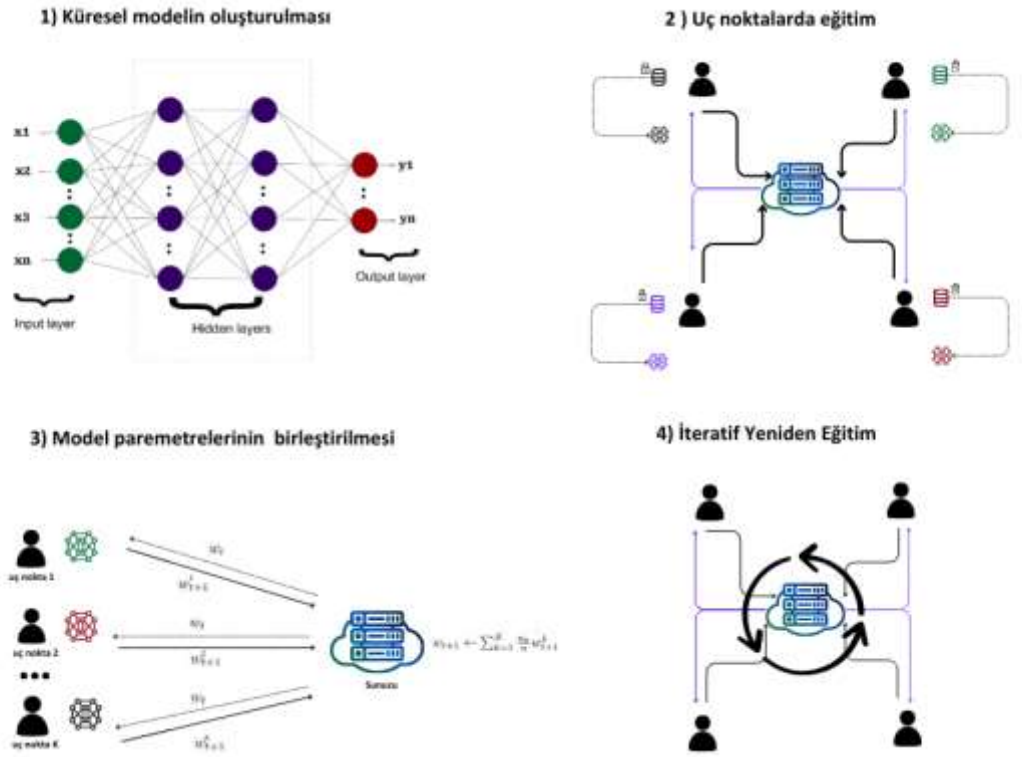
Server executes:
initialize w_0
for each round $t = 1, 2, \dots$ **do**
$S_t = (\text{random set of } \max(C \cdot K, 1) \text{ clients})$
for each client $k \in S_t$ **in parallel do**
$w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$
$w_{t+1} \leftarrow \sum_{t=1}^{K} \frac{n_k}{n} w_{t+1}^k$

ClientUpdate(k, w): *// Executed on client k*
for each local epoch i from 1 to E **do**
batches $\leftarrow$ (data $\mathcal{P}_k$ split into batches of size B)
for batch b in batches **do**
$w \leftarrow w - \eta \nabla \ell(w; b)$
return w to server

Şekil 2.5. FedAvg algoritması [35]: K, k değişkeni tarafından endeksli uç nokta sayısı; n bütün katılımcılarda bulunan toplam örnek sayısı; nk k'ıncı katılımcının örnek sayısı, B, yerel minibatch boyutu; E, yerel epoch sayısı ve η, öğrenme oranıdır.

Merkezi sunucuda, *k* değişkeni tarafından endekslenen *K* sayıda uç nokta seçilir. Seçilen uç noktalarda eğitilen yerel modellerin parametreleri merkezi sunucuya *ClientUpdate* () işlevi ile gönderilir. Son olarak, sunucu, *K* sayıda uç noktadan alınan tüm yerel model

parametrelerinin (w_{t+1}^{K}) ortalamasını alarak küresel modeli günceller. Şekil 2.6'da FedAvg yaklaşımı sürecinin şeması sunulmuştur.



Şekil 2.6. FedAvg süreç şeması.

1. **Başlangıç Modelinin Oluşturulması:** Merkezi sunucu tarafından başlangıç küresel modeli oluşturulur. Bu model, sistemdeki tüm uç noktaların ortak olarak kullanacağı ilk modeldir.

2. **Uç Noktalarda Eğitim:** Başlangıç modeli uç noktalara gönderilir ve her uç nokta, kendi yerel verileriyle başlangıç modeli üzerinde eğitime başlar.

3. **Model Parametrelerinin Birleştirilmesi:** Uç noktaların eğitimini tamamlamasının ardından, merkezi sunucu, uç noktalardan gelen yerel model parametrelerinin ortalamasını alarak küresel modeli günceller.

4. **İteratif Yeniden Eğitim:** Adımlar 2-3, belirli bir sayıda iterasyon (döngü) gerçekleştirilene veya belirlenmiş bir durma kriteri elde edilene kadar tekrarlanır. Her iterasyonda, uç noktalar yerel verileriyle modeli tekrar eğitir ve güncel model parametreleri merkezi sunucuya iletilir.

2.1.5. Önerilen Yöntem: FedBest

Bu tez kapsamında FedAvg yönteminin yakınsama hızını artırmak ve daha yüksek doğruluk değerleri elde etmek amacıyla en iyi test doğruluğu performansını gösteren uç nokta yerel model parametresiyle küresel model güncellemesini gerçekleştiren bir yaklaşım önerilmiştir ve FedBest olarak isimlendirilmiştir. Bu yaklaşımda, her uç nokta kendi verileri üzerinde bir öğrenme modeli eğitir ve kendi verisiyle eğitilen yerel model parametreleri, bir merkezi sunucuya gönderilir ve sunucu, en yüksek model test doğruluğuna sahip uç noktayı seçer ve küresel modeli güncellemek için kullanır. FedBest algoritmasının temel adımları Tablo 2.1'de verilmiştir.

Tablo 2.1. FedBest algoritması.

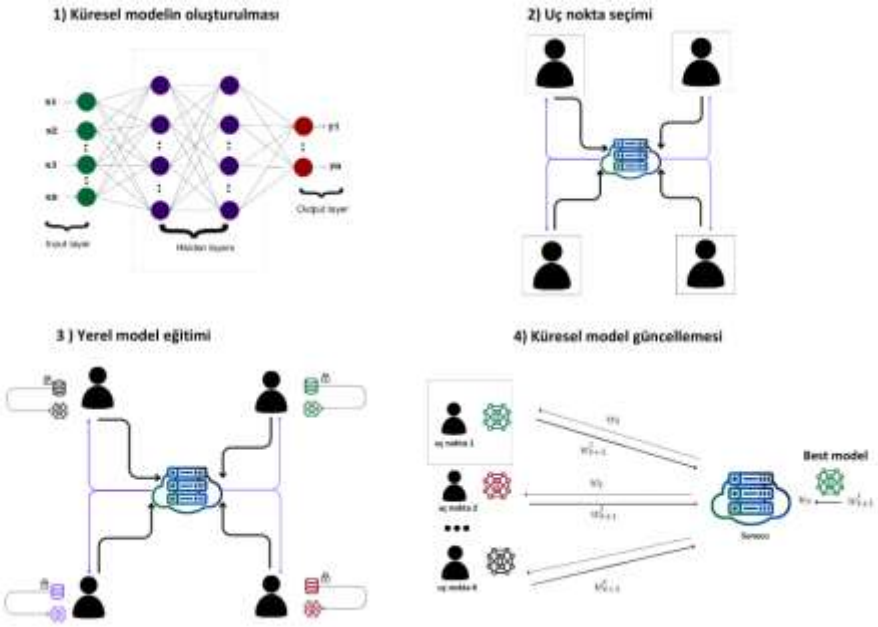
FedBest Algoritması
1. Başlangıç küresel modelin oluşturulması. 2. Rasgele uç noktaların seçilmesi. ***repeat*** 3. Seçilen uç noktanın yerel model güncellemesi yapması: a. Seçilen uç nokta, yerel verilerini kullanarak yerel modeli eğitir. b. Güncellenen yerel model, merkezi sunucuya iletilir. 4. Küresel model güncelleme işlemi: a. Merkezi sunucu, tüm uç noktalardan gelen yerel modelleri alır. b. Küresel model,en iyi performans gösteren yerel modelin parametreleri ile güncellenir. ***until*** Belirli bir durum sağlanana kadar (örneğin, maksimum iterasyon sayısına ulaşılana kadar veya belirli bir durma kriterine kadar).

Başlangıç küresel modelin oluşturulması: Oluşturulan başlangıç küresel model, verilerin özelliklerini yakalamak ve sınıflar arasında ayrım yapmak için etkili bir yapıda olmalıdır. Bu çalışmada CNN (Convolutional Neural Network) tabanlı bir başlangıç modeli oluşturulmuştur.

1. **Rastgele uç noktaların seçilmesi:** Rastgele uç nokta seçimi, federe öğrenme sürecinin dağıtılmış ve işbirlikçi yapısını sağlar. Farklı uç noktaların katılımı, daha

çeşitli ve kapsayıcı bir veri seti temsili anlamına gelir. Bu da küresel modelin daha genel ve güncel bir şekilde güncellenmesini sağlar.

2. **Seçilen uç noktaların yerel model güncellemesi yapması:**
    a. **Seçilen uç nokta, yerel verilerini kullanarak yerel modeli eğitir**: Her seçilen uç nokta, kendi yerel verilerini kullanarak eğitim işlemini gerçekleştirir. Yerel model, uç noktanın sahip olduğu veriye özgü bilgileri içerir ve yerel eğitim süreci boyunca güncellenir.
    b. **Güncellenen yerel model, merkezi sunucuya iletilir:** Uç noktalardaki yerel eğitim tamamlandıktan sonra güncellenen yerel model, merkezi sunucuya iletilir.
3. **Küresel model güncelleme işlemi:**
    a. **Merkezi sunucu, tüm uç noktalardan gelen yerel modelleri alır.**
    b. **Küresel model en iyi performans gösteren yerel modelin parametreleri ile güncellenir**: Merkezi sunucu, alınan yerel modeller arasından en iyi performans gösteren modeli seçer. Bu yaklaşım, küresel modelin daha iyi performans gösteren yerel modelin bilgisini küresel modele entegre etmesini sağlar. En iyi performans gösteren yerel model parametreleri, küresel modelin performansını artırmak için kullanılır. Şekil 2.7'de FedBest yaklaşımı süreç şeması sunulmuştur.



Şekil 2.7. FedBest süreç şeması.

2.2. Derin Öğrenme

Derin öğrenme disiplininde, sinir ağları, insan beyninin bir taklidini oluşturmak için kullanılır. Temel olarak, insan beyninin en temel birimi olan nörona dayanır. Derin öğrenme, nöronların nasıl bir araya gelerek bir sinir ağı modeli oluşturduğunu incelemek için kullanılan bir terimdir. Bir derin öğrenme modeli, bir sinir ağının sonucunda elde edilen karmaşık ve hiyerarşik yapıya sahip bir yapay zekâ modelidir. Genellikle, derin öğrenmede, model, özellikleri otomatik olarak öğrenmek için yapılandırılmamış verileri kullanır ve bu verilerle tekrar tekrar eğitilerek gelişir. Şekil 2.8'de Derin öğrenme ve Makine öğrenimi özet süreci sunulmuştur.

Şekil 2.8. Derin öğrenme ve makine öğrenimi özet süreci.

2.2.1 Evrişimli Sinir Ağı (CNN)

Evrişimli Sinir Ağı (CNN), derin öğrenme alanında yaygın olarak kullanılan ve özellikle görüntü işleme görevlerinde büyük başarı elde etmiş bir yapay sinir ağı türüdür. Yüksek doğruluk oranına sahip görüntü işleme uygulamalarından biri olarak Cireşan ve arkadaşlarının evrişimli sinir ağı (CNN) yaklaşımıyla yaptığı GPU uygulaması gösterilebilir. Olasılıksal gradyan iniş metodu ile eğitilen bu sinir ağı sonucunda elde edilen sonuçlara göre el yazısı tanıma için %0,35, nesne tanıma için %2,53 ve çözünürlüğü düşük doğal resimler için %19,51'lik bir doğruluk oranı yakalanmıştır. 2012'de yapılan bu çalışma için bu sonuçlar literatürdeki en iyi sonuçlar olarak belirtilmiştir [36].

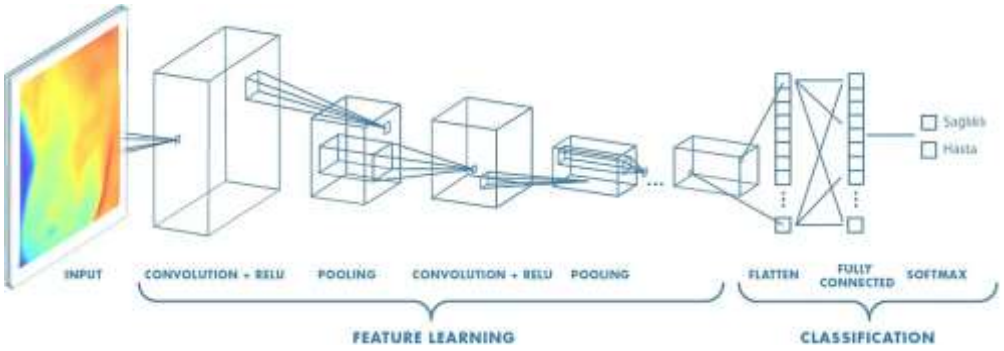
CNN, özellikle resimlerdeki özellikleri çıkarabilmek ve nesneleri tanımak için tasarlanmıştır. Şekil 2.9'da sunulan, görüntü işleme problemlerinde etkili olan, bu mimari görüntüyü çeşitli katmanlarla işler:

- **Evrişim Katmanı (Convolutional Layer):** Bu katmanlar, görüntü üzerinde farklı özellikleri tanımak için birbirinden bağımsız filtreler kullanır. Filtreler, görüntü üzerinde özel bir matematiksel operasyon olan "evrişim" işlemini uygular ve özellik haritalarını üretir. Bu özellik haritaları, daha basit formların (kenarlar, çizgiler vb.) veya daha yüksek düzeyde soyut özelliklerin (gözler, yüzler, araçlar gibi) algılanmasına yardımcı olur.

- **Doğrusal Olmayan (Non-Linearity) katman:** Doğrusal olmayan aktivasyon fonksiyonlarından birini kullandığı için bu katman aktivasyon katmanı (Activation Layer) olarak adlandırılır. Bu fonksiyonlar, çıktıları sıfırdan küçük değerleri olan bir lineer fonksiyona dönüştürerek ağın öğrenme kapasitesini artırır. Aktivasyon fonksiyonları, yapay sinir ağı modelinin her bir katmanında kullanılabilir. Çoğu durumda, ReLU, genellikle eğitim sürecini hızlandıran ve aşırı uydurma (overfitting) riskini azaltan tercih edilen bir seçenektir. Ancak, hangi aktivasyon fonksiyonunun kullanılacağı, modelin yapısına, veri setine ve çözülmek istenen probleme bağlı olarak değişebilir.

- **Havuzlama (Pooling) Katmanı:** Bu katmanın görevi, gösterimin kayma boyutunu (stride), filtrenin ne kadar adım atacağını, ağ içindeki parametreleri ve hesaplama sayısını azaltmak içindir. Bu sayede ağdaki uyumsuzluk kontrol edilmiş olur. Birçok Pooling işlemleri vardır, fakat en popüleri max pooling'dir. Yine aynı prensipte çalışan average pooling, ve L2-norm pooling algoritmaları da vardır.

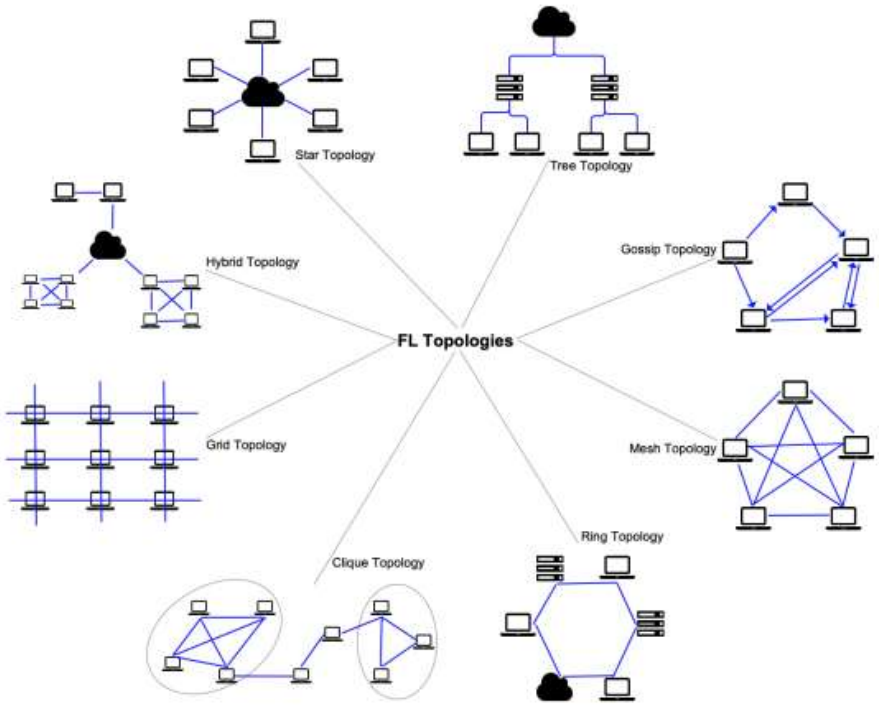
- **Tamamen Bağlı Katman (Fully-Connected Layer):** Bu katmanlar, ağın çıktısını elde etmek için havuzlama ve evrişim katmanlarının çıktılarını düzleştirerek veya vektörleştirerek kullanır. Bu katmanlar, tüm özellikleri bir araya getirerek ve sınıflandırma, tespit veya başka bir görev için sonuçları üretmek için kullanılır.



Şekil 2.9. CNN mimarisi.

2.3. İletişim Ağı Topolojisi

Ağ topolojisi, bir ağdaki cihazlar arasındaki bağlantıların ve veri iletişiminin nasıl düzenlendiğini belirleyen yapısal bir düzeni ifade eder. Bu yapı, ağdaki düğümlerin fiziksel bağlantıları ve veri akış yollarını içerir. Farklı ağ topolojileri, farklı bağlantı ve veri iletim düzenlemelerine sahip olabilir ve bu da ağın performansı, güvenilirliği ve ölçeklenebilirliği üzerinde etkili olabilir [37]. Şekil 2.10'da federe öğrenmede kullanılan iletişim ağı topoloji örnekleri sunulmuştur.



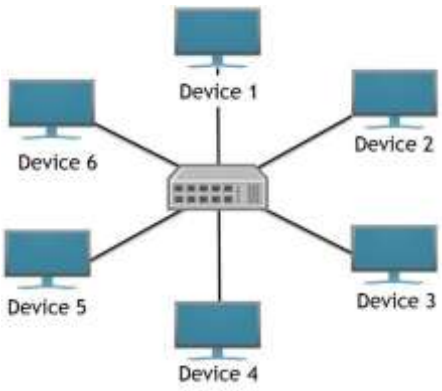
Şekil 2.10. Federe öğrenmede kullanılan iletişim ağı topolojisi örnekleri [37].

2.3.1. Star Topolojisi

Alternatif olarak yıldız ağı olarak adlandırılan yıldız topolojisi, en yaygın ağ kurulumlarından biridir. Bu yapılandırmadaki her düğüm, hub, anahtar veya bilgisayar gibi merkezi bir ağ cihazına bağlanır. Merkezi ağ aygıtı bir sunucu görevi görür ve çevresel uç noktalar istemci görevi görür. Bir star topolojisinde kaç bilgisayarın bağlanabileceği konusunda teknik olarak bir sınır yoktur. Ancak, daha fazla bilgisayar bağlandıkça ağ performansı düşebilir ve bu da ağ hızlarının düşmesine neden olabilir [38].

Federe öğrenmede en yaygın kullanılan ağ topolojisi, orijinal federe öğrenme araştırmalarında olduğu gibi merkezi toplama ve dağıtım mimarisi olarak bilinen star topolojisidir. Sonuç olarak, merkezi sunucu-istemci (uç nokta) mimarisinin grafiği bir yıldızı andırır. Bu yaklaşım, merkezi sunucunun tüm iletişimi koordine etmesini ve verilerin güvenli bir şekilde toplandığından emin olmasını sağlamasına rağmen, star ağ topolojisi yüksek iletişim maliyetleri, merkezi sunucuya gizlilik sızıntısı ve güvenlik sorunları ile karşı karşıya kalır. Bazı çalışmalar bu sorunları çözmek için çözümler sunmuştur [39]. Şekil 2.11'de star topolojisi şeması sunulmuştur.

Star topolojisinin avantajları şunlardır: Merkezi bilgisayar, hub veya anahtarın kullanımı yoluyla ağın merkezi yönetimi sağlanabilir. Ağa başka bir bilgisayar eklemek kolaydır ve ağdaki bir bilgisayar arızalandığında ağın geri kalanı normal şekilde çalışmaya devam eder. Star topolojisinin dezavantajları ise şunlardır: Özellikle merkezi ağ cihazı olarak bir anahtar veya yönlendirici kullanıldığında, uygulama maliyeti daha yüksek olabilir ve bu cihaz ağın işleyebileceği uç noktaların performansını ve sayısını belirler. Ayrıca, merkezi bilgisayar, hub veya anahtar arızalanırsa, tüm ağ çöker ve tüm bilgisayarların ağla bağlantısı kesilir.



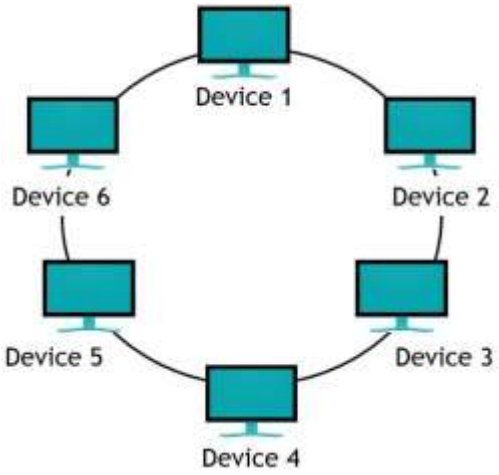
Şekil 2.11. Star topolojisi.

2.2.2. Ring Topolojisi

Ring topolojisi cihaz bağlantılarının dairesel bir veri yolu oluşturduğu bir ağ yapılandırmasıdır. Ağa bağlı her cihaz, bir daire üzerindeki noktalar gibi diğer iki cihaza bağlıdır. Birlikte, bir ring topolojisindeki cihazlara halka ağı denir. Bir ring ağında, veri paketleri hedeflerine ulaşana kadar bir cihazdan diğerine geçer. Çoğu ring topolojisi, paketlerin tek yönlü bir ring ağı olarak adlandırılan yalnızca bir yönde hareket etmesine izin verir [38].

Federe öğrenme, her bir uç nokta tarafından veri yerine model parametreleri değişimi ile gizliliği koruyan yaygın kullanılan bir dağıtık derin öğrenme çerçevesidir. Ancak, federede öğrenme yüksek iletişim maliyetleriyle karşılaşır, çünkü eğitim sürecinde önemli sayıda model parametresinin defalarca iletilmesi gereklidir ve iletişim ağının bant genişliği sınırlı olduğunda bu yöntem etkin olmaz. Yang ve ark. (2021) yaptıkları bir çalışmadan federede öğrenme sürecinde iletişim maliyetini azaltmak için RingFed adında yeni bir çerçeve önermişlerdir. Önerilen RingFed'de, orijinal federede öğrenmedeki gibi merkezi sunucu ile her uç nokta arasında parametre iletimi yerine, güncellenmiş parametreler sırayla her uç nokta arasında iletilir ve sadece sonuç merkezi sunucuya iletilir, böylece iletişim maliyeti önemli ölçüde azalır [40]. Şekil 2.12'de ring topolojisi şeması sunulmuştur.

Ring topolojisinin avantajları arasında, tüm verilerin tek yönde akarak paket çarpışma olasılığını azaltması, her iş istasyonu arasındaki ağ bağlantısını kontrol etmek için bir ağ sunucusuna gerek olmaması, verilerin iş istasyonları arasında yüksek hızlarda aktarılabilmesi ve ağın performansını etkilemeden ek iş istasyonlarının eklenmesi sayılabilir. Ancak, bu topolojinin dezavantajları da bulunmaktadır. Örneğin, ağ üzerinden aktarılan tüm verilerin ağdaki her bir iş istasyonundan geçmesi gerekmekte, bu da onu bir yıldız topolojisine göre daha yavaş hale getirebilmektedir. Ayrıca, bir iş istasyonunun kapanması durumunda tüm ağın etkileneceği bir yapıya sahiptir. Bunun yanı sıra, her bir iş istasyonunu ağa bağlamak için gereken donanımın, Ethernet kartlarından ve hub'lardan/anahtarlardan daha pahalı olduğu unutulmamalıdır.



Şekil 2.12. Ring topolojisi.

3. BÖLÜM

DENEYSEL ÇALIŞMALAR VE BULGULAR

Bu çalışmada, medikal verilerin sınıflandırılmasında federe öğrenme yapısında derin öğrenme mimarilerinden evrişimli sinir ağları kullanılmıştır. Hızlı yakınsama ve yüksek doğruluk elde etmek amacıyla önceki bölümde detayları sunulan FedBest algoritması incelenmiş, doğrulama amacıyla literatürde yaygın kullanılan FedAvg yöntemi ile kıyaslanmıştır. Çalışmada kullanılan CNN yapısına ait detaylar Tablo 3.1'de verilmiştir. Modelin eğitimi sırasında genelleme kabiliyetini artırmak amacıyla Callbacks, Regularization ve Dropout gibi yaygın teknikler kullanılmıştır. Aşırı öğrenmeyi önlemek için model katmanlarında Regularization (ağırlık azaltma) L2 (1e-4), Droupout=0,20 düzenleme teknikleri kullanılmıştır.

- Callbacks ile Modelcheckpoint yapılarak validasyon doğruluğu ‘max’ olduğunda yerel modeller kaydedilmiş ve yerel eğitim sonrası küresel model güncellemesinde bu kaydedilen yerel model güncellemeleri kullanılmıştır.

- Model performansını iyileştirmek için Batchsize sayısı (128) kullanılmıştır.

Tablo 3.1. CNN modelinin yapısı ve parametre sayısı.

Layer(type)	**Output Shape**	**#parameters**
conv2d(CONV2D)	(None,26,26,28)	784
Max_pooling2d(MaxPooling2D)	(None,13,13,28)	0
Conv2d_1(CONV2D)	(None,11,11,56)	14168
Max_pooling2d_1(MaxPooling2D)	(None,5,5,56)	0
Conv2d_2(CONV2D)	(None,3,3,56)	28280
flatten (Flatten)	(None,504)	0
dense (Dense)	(None,56)	28280
dense_1(Dense)	(None,10)	570
Droupout (Droupout)	(None,10)	0
Total parameters:	-	72,082
Trainable parameters:	-	72,082
Non-trainable parameters:	-	0

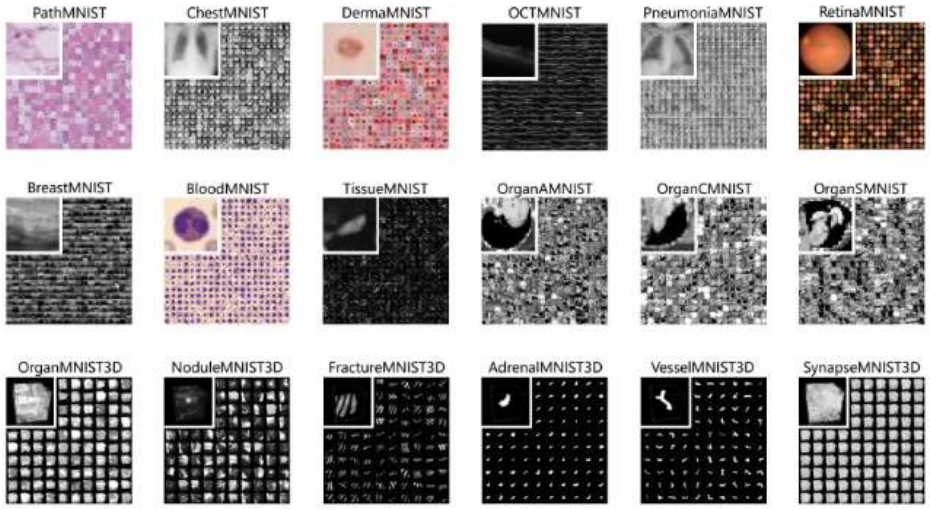
3.1 Çalışmada Kullanılan Medikal Veri Setleri

Bu bölümde bu çalışmada kullanılan veri setleri ile ilgili bilgi verilmiştir.

3.1.1 MedMNIST

Şekil 3.1' de verilen MedMNIST, standartlaştırılmış biyomedikal görüntüler için geniş ölçekli bir MNIST benzeri veri kümesidir ve 2B için 12 veri kümesi ve 3B için 6 veri kümesi içermektedir. MedMNIST, farklı veri ölçeklerinde (100'den 100.000'e kadar) ve farklı görevlerde (ikili / çok sınıflı, ordinal regresyon ve çok etiketli) 2B ve 3B görüntüler üzerinde sınıflandırma yapmak için tasarlanmıştır. Tüm görüntüler, kullanıcılar için herhangi bir arka plan bilgisi gerektirmeden, ilgili sınıflandırma etiketleriyle birlikte 28

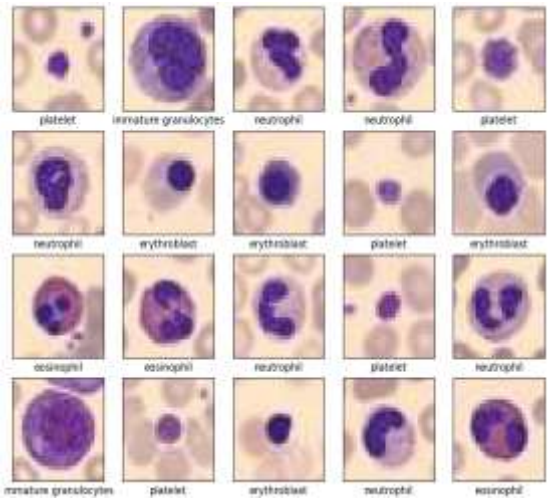
x 28 (2B) veya 28 x 28 x 28 (3B) boyutlarına önceden boyutlandırılmıştır. Biyomedikal görüntülerdeki temel veri modalitelerini kapsayan Toplamda 708.069 adet 2B görüntü ve 9.998 adet 3B görüntü içermektedir [41].



Şekil 3.1. MedMNIST 'e genel bakış [41].

3.1.1.1. BloodMNIST

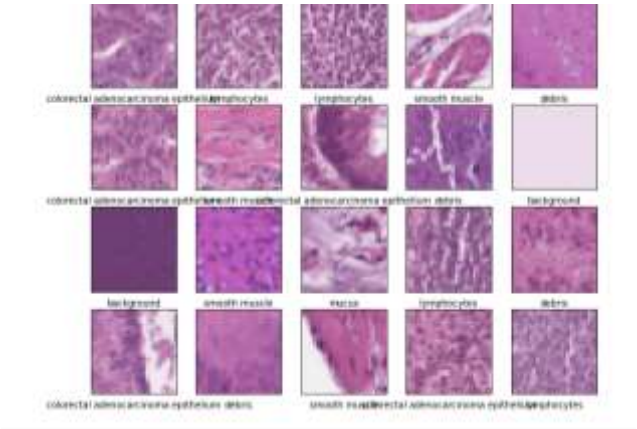
BloodMNIST veri kümesi, enfeksiyon, hematolojik ya da onkolojik hastalığı olmayan ve kan toplama anında herhangi bir farmakolojik tedavi görmeyen bireylerin normal hücrelerinden elde edilen bir veri kümesidir. Toplam 17.092 görüntü içermektedir ve 8 sınıfa ayrılmıştır. Kaynak veri kümesi eğitim, doğrulama ve test seti olmak üzere 7:1:2 oranında bölünmüştür. Kaynak görüntülerin çözünürlüğü $3 \times 360 \times 363$ pikseldir ve merkezden kırpılarak $3 \times 200 \times 200$ boyutlarına indirgenmiş, ardından $3 \times 28 \times 28$ boyutlarına yeniden boyutlandırılmıştır.Şekil 3.2'de BloodMNIST veri seti çoklu sınıf örnekleri sunulmuştur [41].



Şekil 3.2. BloodMNIST veri seti çoklu sınıf örnekleri.

3.1.1.2. PathMNIST

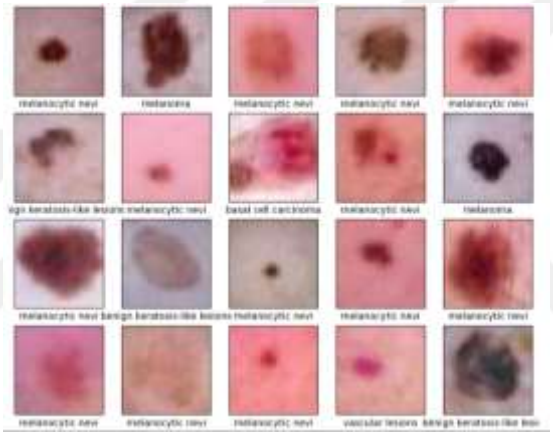
PathMNIST, kolorektal kanser histoloji slaytlarından sağkalım tahminine yönelik 100.000 adet görüntü yaması (NCT-CRC-HE-100K) ve farklı bir klinik merkezden sağlanan 7.180 adet görüntü yaması (CRC-VAL-HE-7K) içeren bir veri setidir. Veri seti, 9 farklı doku türünden oluşur ve çok sınıflı sınıflandırma görevini içerir. Kaynak görüntüleri 3 × 224 × 224 piksel boyutundan 3 × 28 × 28 piksele yeniden boyutlandırılmıştır. NCT-CRC-HE-100K 9:1 oranında eğitim ve doğrulama setlerine ayrılmıştır. CRC-VAL-HE-7K test seti olarak kullanılmaktadır. Şekil 3.3'te PathMNIST veri seti çoklu sınıf örnekleri sunulmuştur [41].



Şekil 3.3. PathMNIST veri seti çoklu sınıf örnekleri.

3.1.1.3. DermaMNIST

DermaMNIST, yaygın pigmente cilt lezyonlarının çok kaynaklı dermatoskopik görüntülerinin büyük bir koleksiyonu olan HAM1000019,20,21 temel alınarak oluşturulmuştur. Veri kümesi, 7 farklı hastalığa ait sınıflandırılmış 10.015 dermatoskopik görüntü içermektedir ve çoklu sınıf sınıflandırma görevi olarak tanımlanmıştır. Görüntüler eğitim, doğrulama ve test setlerine 7:1:2 oranında bölünmüştür. Kaynak görüntülerin boyutu 3 × 600 × 450'dir ve 3 × 28 × 28 boyutuna yeniden boyutlandırılmıştır. Şekil 3.4'te DermaMNIST veri seti çoklu sınıf örnekleri sunulmuştur [41].



Şekil 3.4. DermaMNIST veri seti çoklu sınıf örnekleri.

Bu çalışmada kullanılacak BloodMNIST, PathMNIST ve DermaMNIST veri setlerinin uç noktalara dağıtılmadan önceki eğitim, doğrulama ve test veri setleri miktarları Tablo 3.2'de verilmiştir.

Tablo 3.2. BloodMNIST, PathMNIST ve DermaMNIST eğitim, doğrulama ve test veri sayıları.

Veri Seti	Eğitim	Doğrulama	Test
BloodMNIST	11959	1712	3421
PathMNIST	89996	10004	7180
DermaMNIST	7007	1003	2005

3.2. MedMNIST Veri Seti Deney Sonuçları

Bu bölümde MedMNIST veri seti içerisindeki BloodMNIST, PathMNIST ve DermaMNIST veri setleri ile yapılan deney sonuçları sunulmuştur.

3.2.1. BloodMNIST Veri Seti Deney Sonuçları

Bu çalışmada, MedMNIST veri setlerinden biri olan BloodMNIST veri seti kullanılmıştır. Bu veri seti, model sınıflandırmasında federe öğrenme yaklaşımlarının performansını değerlendirmek için kullanılmıştır. Çalışma kapsamında, toplamda dört adet uç nokta (client) oluşturulmuştur. Her bir uç noktaya eşit miktarda eğitim verisi dağıtılmış ve dağıtım sonrası uç noktalardaki yerel model eğitiminde kullanılmak üzere eğitim, doğrulama ve test veri setleri, 7:1:2 oranında bölümlendirilmiştir. BloodMNIST veri setlerinin uç noktalara dağıtıldıktan sonra her uç noktadaki eğitim, doğrulama ve test veri setleri miktarları Tablo 3.3'te verilmiştir.

Tablo 3.3. BloodMNIST eğitim, doğrulama ve test veri setleri miktarları.

Veri Seti	**Eğitim**	**Doğrulama**	**Test**
BloodMNIST	996	142	284

Federe öğrenme süreci için dört uç noktaya veriler karıştırlıp dağıtıldıktan sonra her uç noktaya başlangıç küresel model parametreleri gönderilmiştir. Yerel modellerin eğitim süreci, her bir uç noktadaki yerel modellerde toplamda 50 epoch (dönem) boyunca gerçekleştirilmiştir. Eğitim süreci tamamlanan uç noktalardaki yerel modellerin parametreleri merkezi sunucuya aktarılmış ve bu yerel modellerin parametreleri federe öğrenme yaklaşımları ile küresel model güncellenmiştir.

Federe öğrenme süreci üç eğitim turu boyunca tekrarlanmıştır. Her bir eğitim turu, uç noktaların merkezi sunucudan gönderilen model parametrelerini yerel verileri ile eğittiği ve eğitilen model parametrelerini merkezi sunucuya gönderip küresel modeli yeniden güncellediği bir dönemdir. Tablo 3.4'te, FedAvg ve önerilen FedBest federe öğrenme yaklaşımlarını kullanarak yerel modellerin ve her eğitim sonu güncellenen küresel modelin sınıflandırma sonuçları sunulmuştur.

Tablo 3.4. BloodMNIST veri seti deney sonuçları.

Uç Noktalar		***Initial CNN model***	***2.tur FedAvg***	***2.tur FedBest***	***3.tur FedAvg***	***3.tur FedBest***
1	**Train acc:**	0,8464	0,8705	0,8835	0,8665	0,9127
	Test acc:	0,7711	0,8451	0,8275	0,8239	0,8169
2	**Train acc:**	0,7691	0,8343	0,8815	0,8685	0,8906
	Test acc:	0,7465	0,7711	0,8063	0,8204	0,8345
3	**Train acc:**	0,8183	0,8544	0,8484	0,8785	0,9016
	Test acc:	0,8134	0,8169	0,8134	0,8345	0,8275
4	**Train acc:**	0,7982	0,8183	0,8333	0,8765	0,8835
	Test acc:	0,7606	0,7923	0,8169	0,8310	0,8275
Best:	**Train acc:**	0,8464	0,8705	0,8835	0,8785	0,9127
	Test acc:	0,8134	0,8451	0,8275	0,8345	0,8345
Mean:	**Train acc:**	0,8080	0,8443	0,8616	0,8725	0,8971
	Test acc:	0,7729	0,8063	0,8134	0,8274	0,8275
Std:	**Train acc:**	0,0326	0,0228	0,0248	0,0058	0,0127
	Test acc:	0,0288	0,0319	0,0088	0,0064	0,0072
Küresel Model Update	**Test Acc:**	**FedAvg:** 0,3768 **FedBest:** 0,7394	0,7570	0,8451	0,8451	0,8486

Sonuçlar analiz edildiğinde, ilk eğitim turu senaryosunda dört uç nokta kendi yerel verileri ile merkezi sunucudan gelen CNN model parametrelerini eğitmiştir. Eğitilen yerel model parametreleri merkezi sunucuya gönderilmiştir. Sunucuya gelen yerel modeller ortak test veri kümesi ile test edilmiş ve uç nokta 3'ten gelen yerel model en yüksek test doğruluk oranına sahip olduğu görülmüştür (%81,34). İlk eğitim turu sonrası dört uç noktadan gelen yerel model parametrelerinin FedAvg yaklaşımı kullanılarak ortalaması

alınmış ve küresel model bu parametrelerle güncellenmiştir. İlk eğitim turu sonrası güncellenen küresel model ortak test verileriyle ölçüldüğünde küresel model performansı, %37,68 test doğruluk oranında hesaplanmıştır. FedBest yaklaşımı kullanılarak uç nokta 3'ün eğittiği yerel model parametreleri kullanılarak küresel model güncellenmiş, ilk eğitim sonrası FedBest yaklaşımıyla güncellenen küresel model performansı %73,94 test doğruluğu oranında hesaplanmıştır.

İkinci eğitim turundan önce merkezi sunucu, FedAvg ve FedBest yaklaşımı ile güncellenen model parametreleri tekrar dört uç noktaya göndermiş ve güncellenen model uç noktalardaki yerel verilerle tekrar eğitilmiştir. FedAvg yaklaşımı senaryosunda, uç nokta 1, uç nokta 2, uç nokta 3 ve uç nokta 4'ün eğittiği yerel model test doğruluk oranlarının ilk eğitim turundaki sonuçlarına göre arttığı gözlemlenmiştir. Uç nokta 1 yerel modelinin test doğruluk oranı %84,51'e, uç nokta 2 yerel modelinin test doğruluk oranı %77,11'e, uç nokta 3 yerel modelinin test doğruluk oranı %81,69'a ve uç nokta 4 yerel modelinin test doğruluk oranı %79,23'e ulaşmıştır. FedBest yaklaşımı senaryosunda, uç nokta 1 yerel modelinin test doğruluk oranı %82,75'e, uç nokta 2 yerel modelinin test doğruluk oranı %80,63'e, uç nokta 3 yerel modelinin test doğruluk oranı %81,34'e ve uç nokta 4 yerel modelinin test doğruluk oranı %81,69'a ulaşmıştır. Bu durumda, ikinci eğitim turu sonunda uç nokta 1' den gelen yerel modelin en yüksek test doğruluk oranına sahip olduğu görülmüştür (%81,34).

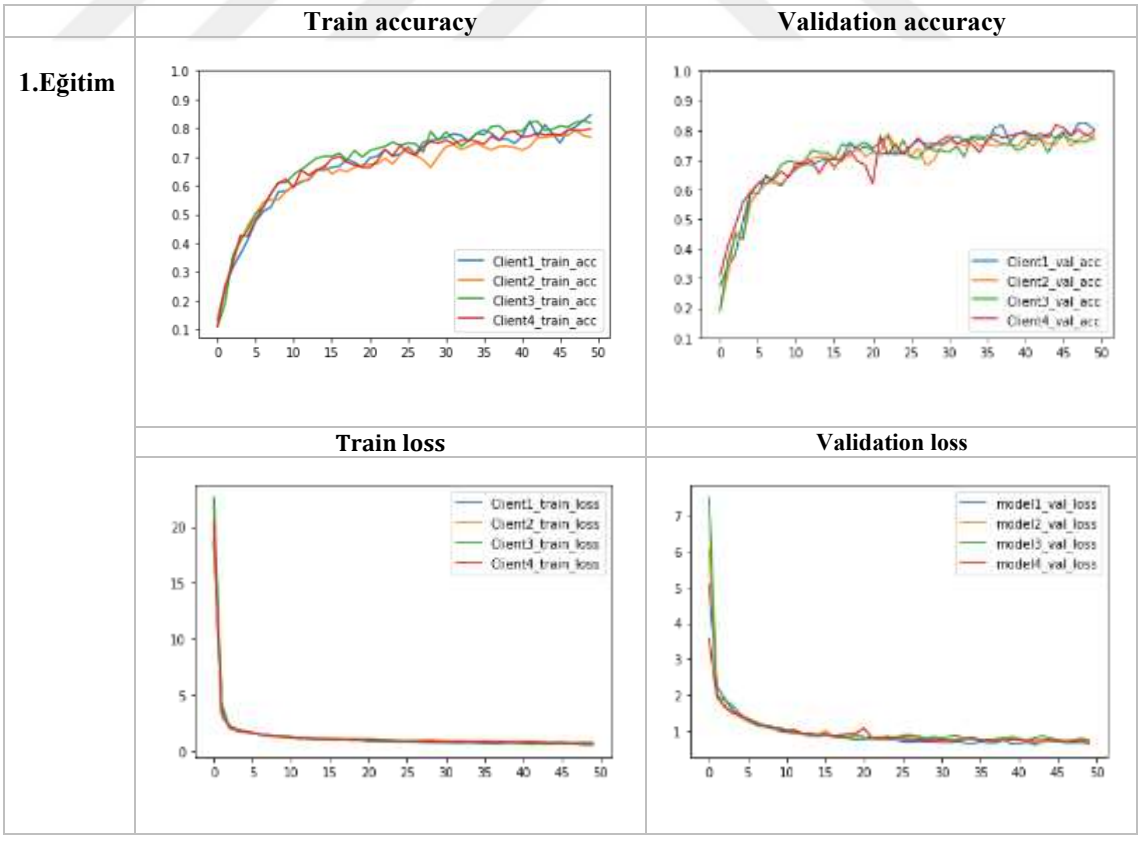
Üçüncü eğitim turundan önce FedAvg yaklaşımı ile güncellenen küresel model parametreleri uç noktalara gönderildikten sonra uç nokta 1 yerel modelinin test doğruluk oranı %82,39'a uç nokta 2 yerel modelinin test doğruluk oranı %82,04'e, uç nokta 3 yerel modelinin test doğruluk oranı %83,45'e ve uç nokta 4 yerel modelinin test doğruluk oranı %83,10'a ulaşmıştır. FedBest senaryosunda ise uç nokta 1 yerel modelinin test doğruluk oranı %81,69'a, uç nokta 2 yerel modelinin test doğruluk oranı %83,45'e, uç nokta 3 yerel modelinin test doğruluk oranı %82,75'e ve uç nokta 4 yerel modelinin test doğruluk oranı %82,75'e ulaşmıştır.

Sonuçlar incelendiğinde, FedAvg senaryosunda, ikinci eğitim ve üçüncü eğitim turundan sonra uç nokta yerel modellerin test doğruluk oranları artmıştır. FedBest senaryosunda da benzer şekilde, uç nokta yerel modellerinin test doğruluk oranlarının arttığı görülmektedir. İlk turda en yüksek yerel model test doğruluk oranına sahip olan uç nokta

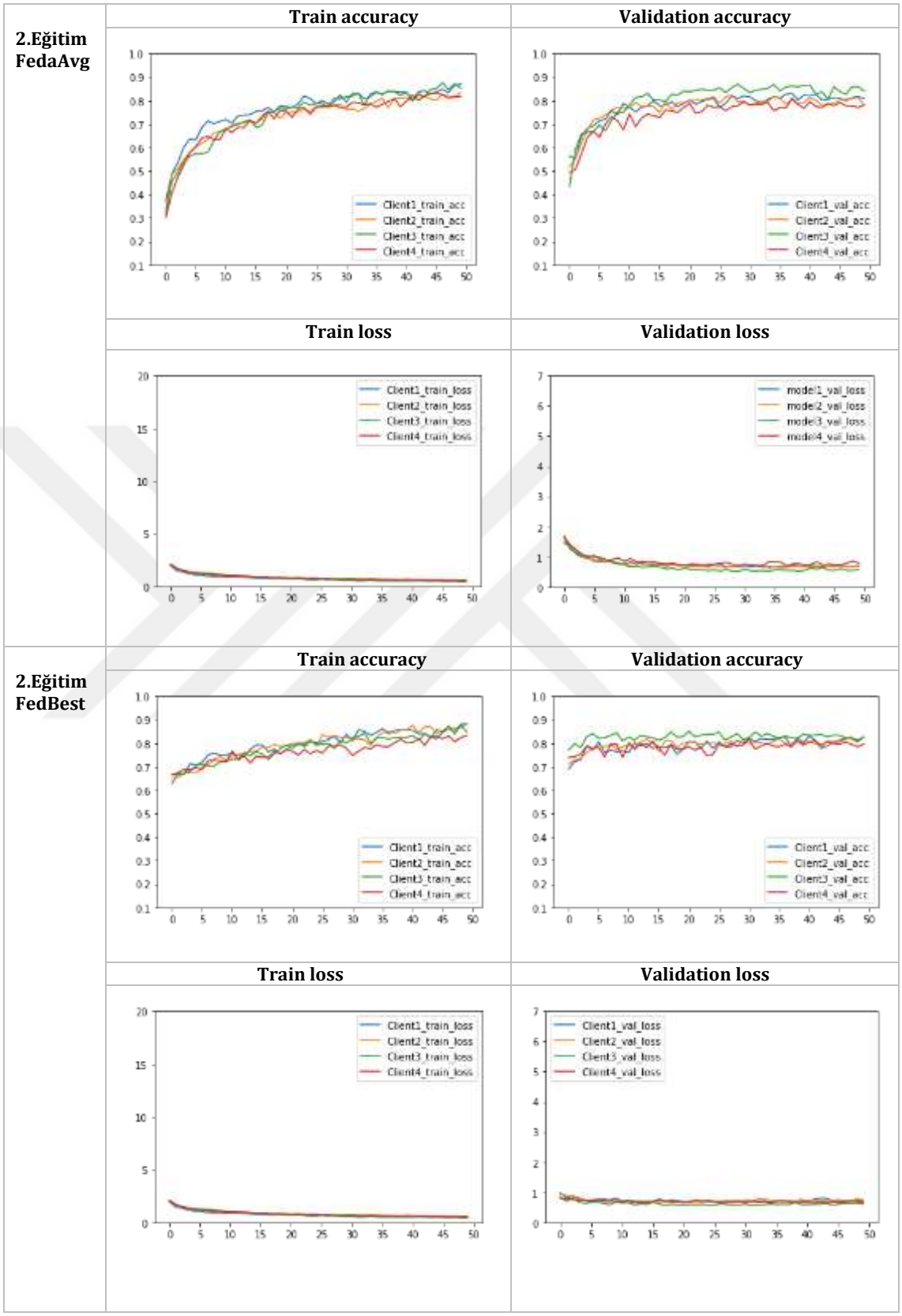
3 (%81,34), ikinci turda uç nokta 1 (%82,75), üçüncü eğitim turunda da uç nokta 2 (%83,45) olmuştur. Burdaki sonuçlara göre her eğitim sonrası en iyi (best) yerel model test doğruluk oranının arttığı görülmüştür.

Bu sonuçlar, BloodMNIST veri seti sınıflandırılmasında FedAvg ve FedBest yaklaşımlarının genel olarak iyi performans gösterdiğini ve FedBest yaklaşımının uç noktalardan en iyi performans gösteren modeli seçerek küresel modeli güncellediğinde eğitim sonrası küresel model test doğruluğu performansında daha iyi sonuçlar elde ettiği ve daha hızlı yakınsadığı görülmüştür.

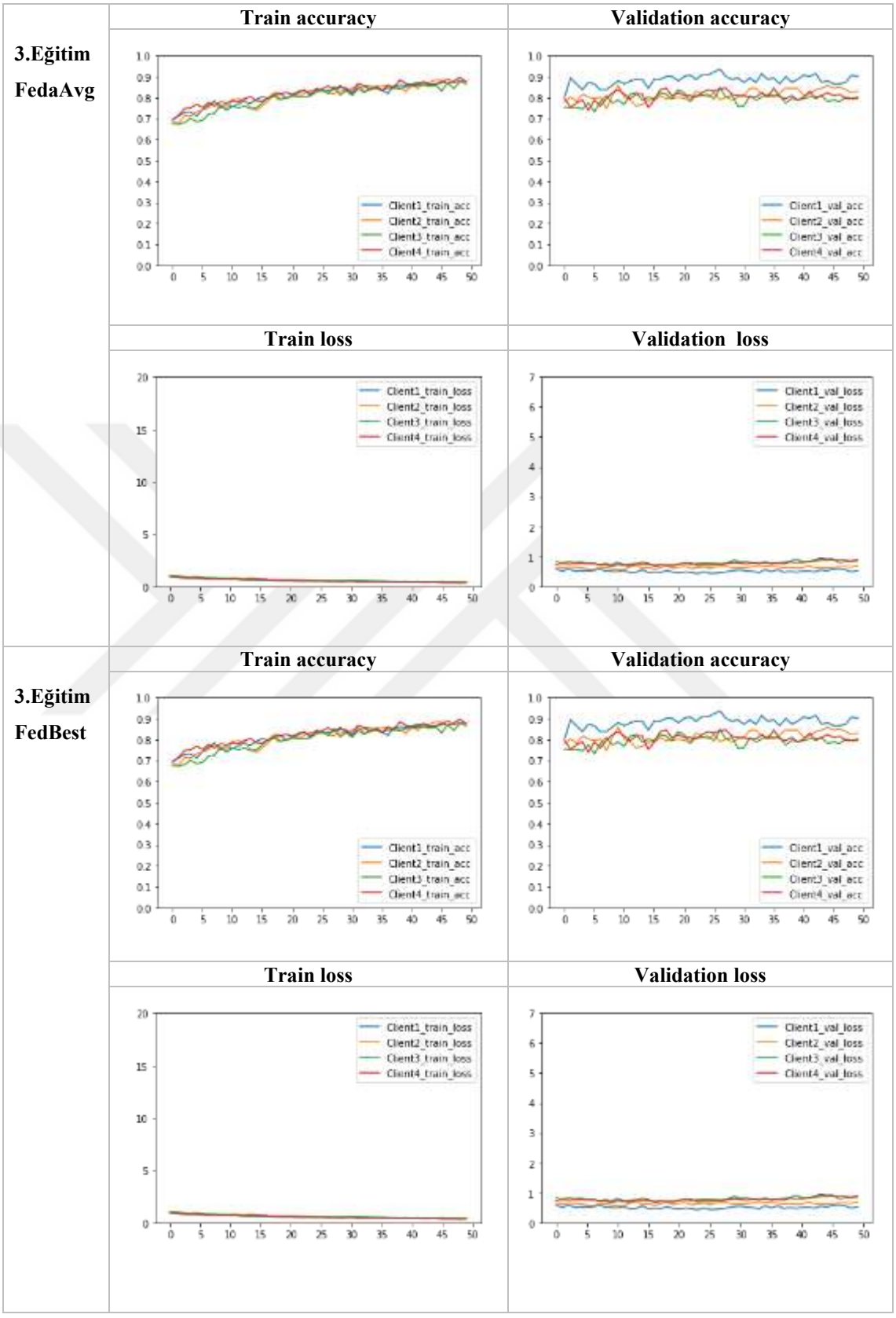
Şekil 3.5-3.7'de üç eğitim boyunca alınan uç noktalardaki yerel model performans sonuçlarının grafikleri sunulmaktadır. Grafikler, 50 epoch sonunda her uç noktanın yerel modelinin eğitim doğruluğu (train accuracy) ve kayıp değerlerini (train loss), ayrıca validasyon doğruluğu (validation accuracy) ve kayıp değerlerini (validation loss) göstermektedir. Grafikler, her uç noktanın eğitim sürecindeki performansını ve yerel modelin doğruluğu ile kayıp üzerindeki değişimleri takip etmemize olanak sağlamaktadır.



Şekil 3.5. Birinci eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri.



Şekil 3.6. İkinci eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri.



Şekil 3.7. Üçüncü eğitim sonu BloodMNIST veri seti deney sonuçları grafikleri.

3.2.2. PathMNIST Veri Seti Deney Sonuçları

Bu çalışmada, PathMNIST veri seti kullanılmıştır. Çalışma kapsamında, toplamda dört adet uç nokta (client) oluşturulmuştur. Her bir uç noktaya eşit miktarda eğitim veri seti dağıtılmış ve dağıtım sonrası uç noktalardaki yerel model eğitiminde kullanılmak üzere eğitim, doğrulama ve test veri setleri, 7:1:2 oranında bölümlendirilmiştir. PathMNIST veri setlerinin uç noktalara dağıtılan eğitim, doğrulama ve test veri setleri miktarları Tablo 3.5'te verilmiştir.

Tablo 3.5. PathMNIST eğitim, doğrulama ve test veri setleri miktarları.

Veri Seti	**Eğitim**	**Doğrulama**	**Test**
PathMNIST	7499	883	598

Yerel modellerin eğitim süreci, her bir uç noktadaki yerel modellerde toplamda 30 epoch (dönem) boyunca gerçekleştirilmiştir. Eğitim süreci tamamlanan uç noktalardaki yerel modellerin parametreleri merkezi sunucuya aktarılmış ve bu yerel modellerin parametreleri federe öğrenme yaklaşımları ile güncellenmiştir.

Federe öğrenme süreci üç eğitim turu boyunca tekrarlanmıştır. Tablo 3.6'da FedAvg ve önerilen FedBest federe öğrenme yaklaşımlarını kullanarak yerel modellerin ve her eğitim sonu güncellenen küresel modelin sınıflandırma sonuçları sunulmuştur.

Tablo 3.6. PathMNIST veri seti deney sonuçları.

Uç Noktalar		***Initial CNN model***	***2.tur FedAvg***	***2.tur FedBest***	***3.tur FedAvg***	***3.tur FedBest***
1	**Train acc:**	0,7289	0,8222	0,8065	0,9075	0,9127
	Test acc:	0,6388	0,6656	0,7993	0,6940	0,8169
2	**Train acc:**	0,5279	0,8182	0,8121	0,8995	0,8906
	Test acc:	0,5635	0,6756	0,7609	0,7174	0,8345
3	**Train acc:**	0,6554	0,7906	0,8092	0,8903	0,9016
	Test acc:	0,6739	0,7375	0,6973	0,7023	0,8275
4	**Train acc:**	0,6765	0,8252	0,7825	0,8848	0,8835
	Test acc:	0,6756	0,6823	0,6890	0,7207	0,8275
Best:	**Train acc:**	0,7289	0,8252	0,8121	0,9075	0,9127
	Test acc:	0,6756	0,7375	0,7993	0,7207	0,8345
Mean:	**Train acc:**	0,6554	0,8140	0,8025	0,8955	0,8971
	Test acc:	0,6379	0,6902	0,7366	0,7086	0,8266
Std:	**Train acc:**	0,0853	0,0158	0,0135	0,0100	0,0127
	Test acc:	0,0524	0,0322	0,0527	0,0126	0,0072
Küresel Model Update	**Test Acc**	**FedAvg:** 0,1405 **FedBest:** 0,6806	0,6221	0,7074	0,7993	

Sonuçlar analiz edildiğinde, ilk eğitim turu sonrası dört uç noktadan gelen model parametrelerinin FedAvg yaklaşımıyla ortalaması alınarak küresel model güncellenmiştir. Güncellenen küresel modelin ortak test verileriyle ölçülen performansı %14,05 doğruluk oranında hesaplanmıştır. FedBest yaklaşımı ile uç nokta 4'ün eğittiği

yerel model parametreleri kullanılarak küresel model güncellenmiş olup ilk eğitim sonrası küresel model performansı %68,06 doğruluk oranında hesaplanmıştır.

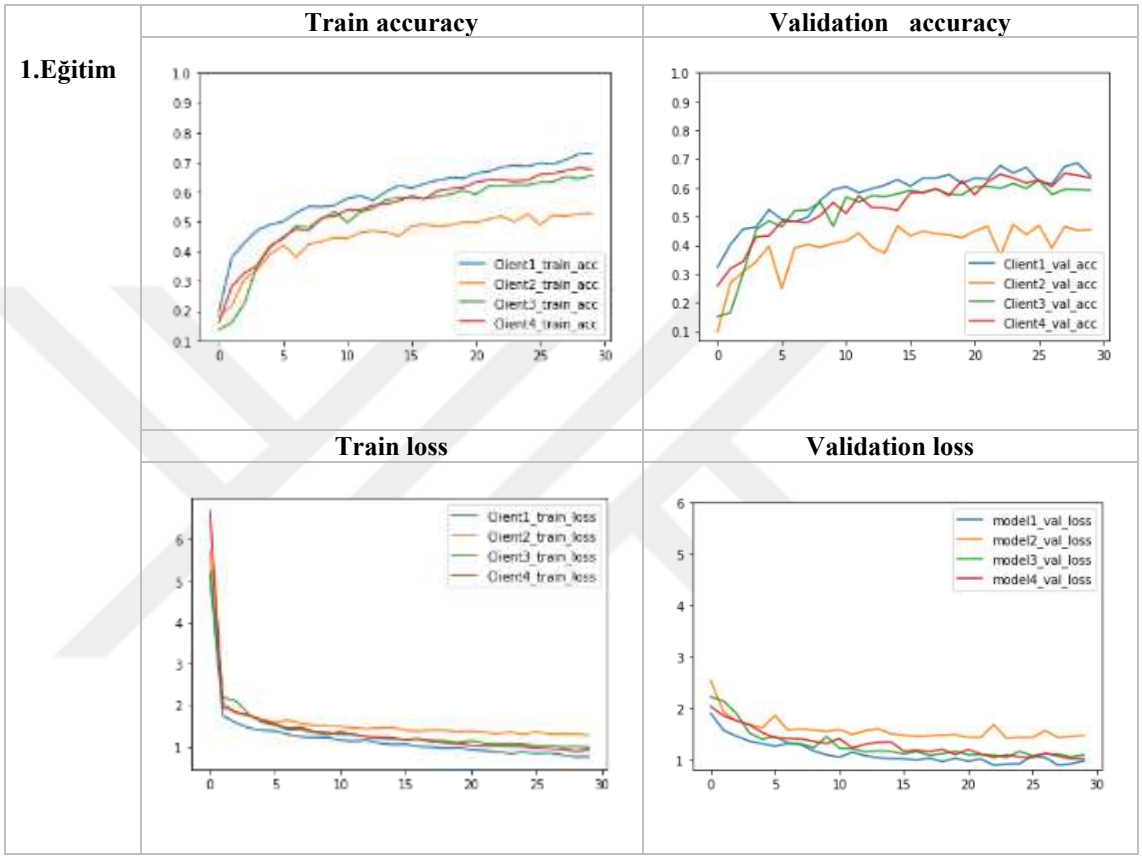
İkinci eğitim turundan önce merkezi sunucu, FedAvg ve FedBest yaklaşımı ile güncellenen model parametreleri tekrar dört uç noktaya göndermiş ve güncellenen model uç noktalardaki yerel verilerle tekrar eğitilmiştir. FedAvg senaryosunda, uç nokta 1 yerel modelinin, uç nokta 2 yerel modelinin, uç nokta 3 yerel modelinin ve uç nokta 4 yerel modelinin test doğruluk oranlarının ilk eğitim turundaki sonuçlarına göre arttığı gözlemlenmiştir. Uç nokta 1 yerel modelinin test doğruluk oranı %66,56'ya, uç nokta 2 yerel modelinin test doğruluk oranı %67,56'ya, uç nokta 3 yerel modelinin test doğruluk oranı %73,75'e ve uç nokta 4 yerel modelinin test doğruluk oranı %68,23'e ulaşmıştır. FedBest senaryosunda, uç nokta 1 yerel modelinin, uç nokta 2 yerel modelinin, uç nokta 3 yerel modelinin ve uç nokta 4 yerel modelinin test doğruluk oranlarının ilk eğitim turundaki sonuçlarına göre arttığı gözlemlenmiştir. Uç nokta 1 yerel modelinin test doğruluk oranı %79,93'e, uç nokta 2 yerel modelinin test doğruluk oranı %76,09'a, uç nokta 3 yerel modelinin test doğruluk oranı %69,73'e ve uç noktanın 4 yerel modelinin test doğruluk oranı %68,90'a ulaşmıştır. ikinci eğitim turu sonunda uç nokta 1' den gelen yerel modelin en yüksek test (best) doğruluk oranına sahip olduğu görülmüştür (%67,56).

Üçüncü eğitim FedAvg senaryosunda uç nokta 1 yerel modelinin test doğruluk oranı %69.40'a uç noktanın 2 yerel modelinin test doğruluk oranı %71,74'e, uç nokta 3 yerel modelinin test doğruluk oranı %70.23'e ve uç nokta 4 yerel modelinin test doğruluk oranı %72,07'ye ulaşmıştır. FedBest senaryosunda ise uç nokta1 yerel modelinin test doğruluk oranı %81,69'a, uç nokta 2 yerel modelinin test doğruluk oranı %83,45'e, uç nokta 3 yerel modelinin test doğruluk oranı %82,75'e ve uç nokta 4 yerel modelinin test doğruluk oranı %82,75'e ulaşmıştır.

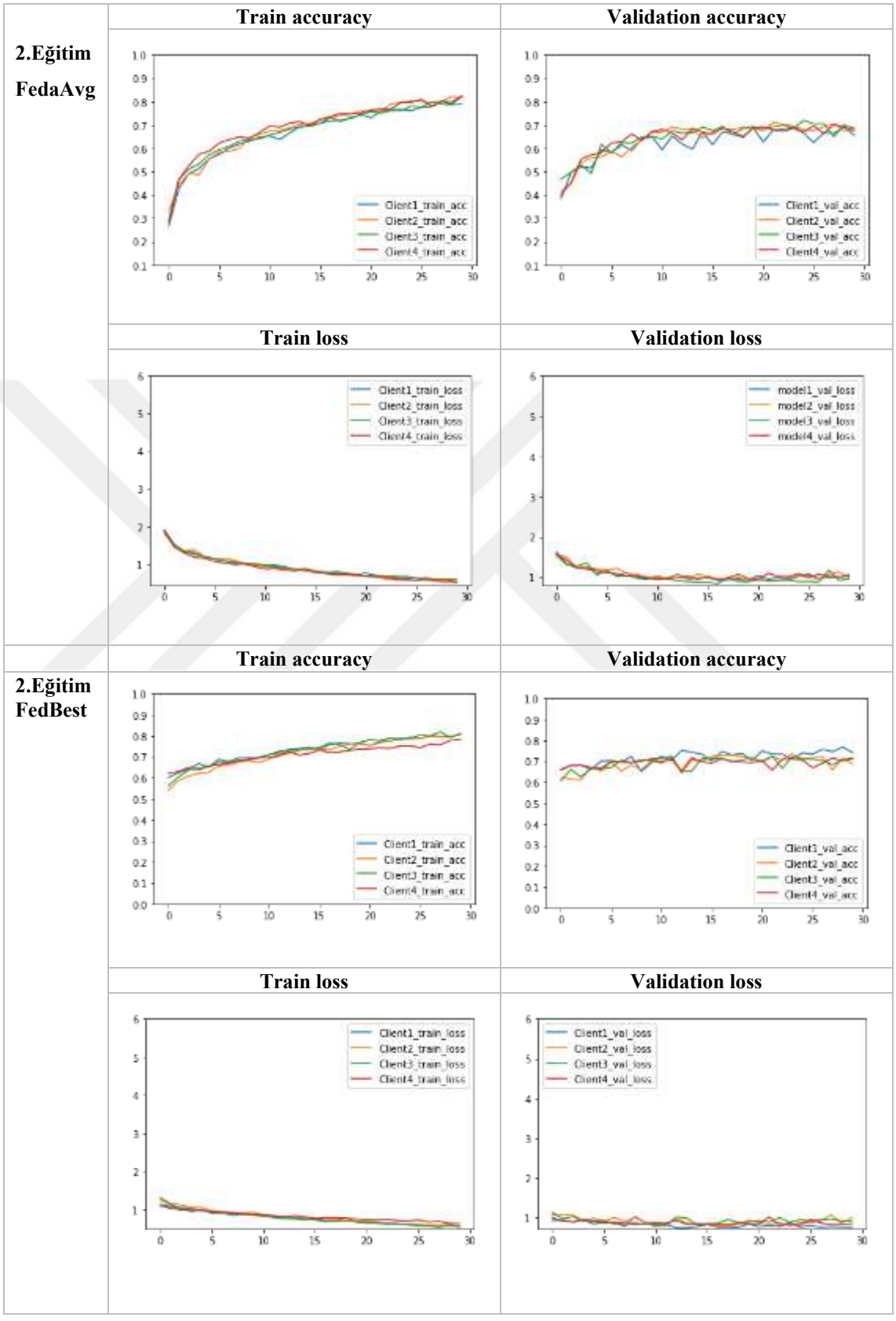
Bu sonuçlar, PathMNIST veri seti sınıflandırılmasında FedAvg ve FedBest yaklaşımlarının genel olarak iyi performans gösterdiğini ve FedBest yaklaşımının uç noktalardan en iyi performans gösteren modeli seçerek küresel modeli güncellediğinde eğitim sonrası küresel model test doğruluğu performansında daha iyi sonuçlar elde ettiği ve daha hızlı yakınsadığı görülmüştür.

Şekil 3.8-3.10'da üç eğitim boyunca alınan uç noktalardaki yerel model performans sonuçlarının grafikleri sunulmaktadır. Grafikler, gösterilen 30 epoch sonunda her uç

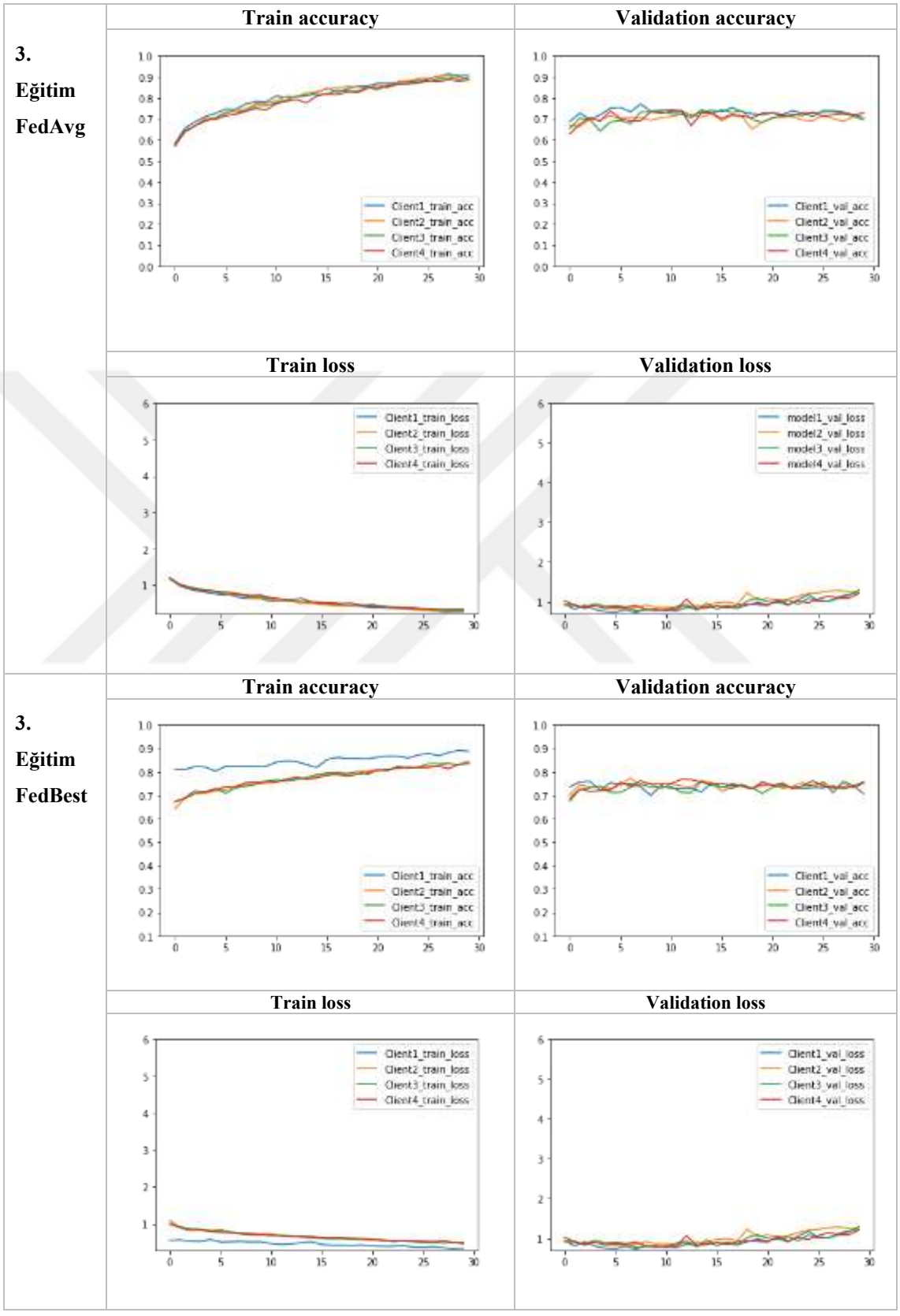
noktanın yerel modelinin eğitim doğruluğu (train accuracy) ve kayıp değerlerini (train loss), ayrıca validasyon doğruluğu (validation accuracy) ve kayıp değerlerini (validation loss) göstermektedir. Grafikler, her uç noktanın eğitim sürecindeki performansını ve yerel modelin doğruluğu ile kayıp üzerindeki değişimleri takip etmemize olanak sağlamaktadır.



Şekil 3.8. Birinci eğitim sonu PathMNIST veri seti deney sonuçları grafikleri.



Şekil 3.9. İkinci eğitim sonu PathMNIST veri seti deney sonuçları grafikleri.



Şekil 3.10. Üçüncü eğitim sonu PathMNIST veri seti deney sonuçları grafikleri.

3.2.3. DermaMNIST Veri Seti Deney Sonuçları

Bu çalışmada, DermaMNIST veri seti kullanılmıştır. Çalışma kapsamında, toplamda dört adet uç nokta (client) oluşturulmuştur. Her bir uç noktaya eşit miktarda eğitim veri seti dağıtılmış ve dağıtım sonrası uç noktalardaki yerel model eğitiminde kullanılmak üzere eğitim, doğrulama ve test veri setleri, 7:1:2 oranında bölümlendirilmiştir. DermaMNIST veri setlerinin uç noktalara dağıtılmadan önceki eğitim, doğrulama ve test veri setleri miktarları Tablo 3.7'de verilmiştir.

Tablo 3.7. DermaMNIST eğitim, doğrulama ve test veri setleri miktarları.

Veri Seti	**Eğitim**	**Doğrulama**	**Test**
BloodMNIST	583	83	167

Yerel modellerin eğitim süreci, her bir uç noktadaki yerel modellerde toplamda 10 epoch (dönem) boyunca gerçekleştirilmiştir. Eğitim süreci tamamlanan uç noktalardaki yerel modellerin parametreleri merkezi sunucuya aktarılmış ve bu yerel modellerin parametreleri federe öğrenme yaklaşımları ile güncellenmiştir.

Federe öğrenme süreci üç eğitim turu boyunca tekrarlanmıştır. Tablo 3.8'de, FedAvg ve önerilen FedBest federe öğrenme yaklaşımlarını kullanarak yerel modellerin ve her eğitim sonu güncellenen küresel modelin sınıflandırma sonuçları sunulmuştur.

Tablo 3.8. DermaMNIST veri seti deney sonuçları.

Uç Noktalar		***Initial CNN model***	***2.tur FedAvg***	***2.tur FedBest***	***3.tur FedAvg***	***3.tur FedBest***
1	**Train acc:**	0,7873	0,7787	0,7993	0,7513	0,8268
	Test acc:	0,6766	0,6766	0,6168	0,6766	0,7246
2	**Train acc:**	0,7770	0,8370	0,8268	0,7788	0,8483
	Test acc:	0,6766	0,6766	0,6407	0,6946	0,6886
3	**Train acc:**	0,7581	0,7719	0,8062	0,8316	0,8276
	Test acc:	0,6766	0,6527	0,6826	0,6108	0,5928
4	**Train acc:**	0,7822	0,7702	0,7890	0,7959	0,8370
	Test acc:	0,7186	0,6228	0,6647	0,6467	0,7066
Best:	**Train acc:**	0,7873	0,8370	0,8268	0,8316	0,8483
	Test acc:	0,7186	0,6766	0,6826	0,6946	0,7246
Mean:	**Train acc:**	0,7761	0,7719	0,7993	0,7894	0,8349
	Test acc:	0,6871	0,6571	0,6512	0,6571	0,6781
Std:	**Train acc:**	0,0127	0,0319	0,0159	0,0336	0,0100
	Test acc:	0,0210	0,0255	0,0286	0,0366	0,0587
Küresel Model Update	**Test Acc**	**FedAvg:** 0,6707 **FedBest:** 0,6826	0,6946	0,7186	0,7186	0,7305

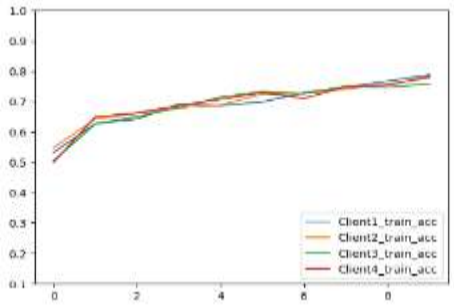
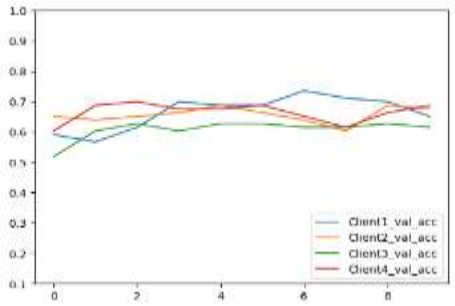
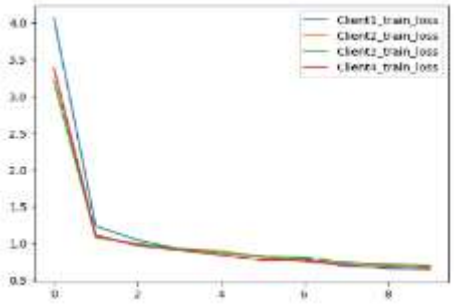
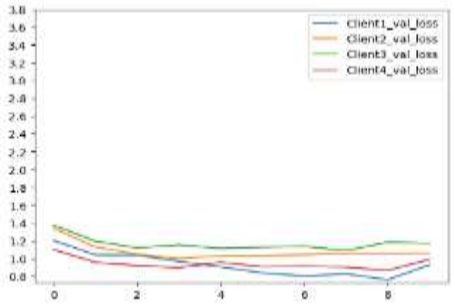
Sonuçlar analiz edildiğinde, ilk eğitim sonrası dört uç noktadan gelen yerel model parametreleri FedAvg yaklaşımı ile ortalaması alınarak küresel model güncellenmiştir. Güncellenen küresel modelin performansı %67,07 olarak bulunmuştur. İlk eğitim turu sonrası uç nokta 4'ten gelen yerel modelin en yüksek test doğruluk oranına sahip olduğu görülmüştür (%71,86). FedBest yaklaşımında uç nokta 4'ün eğittiği yerel model

parametreleri kullanılarak küresel model güncellenmiş olup ilk eğitim sonrası küresel model %68,26 oranında doğruluk elde etmiştir.

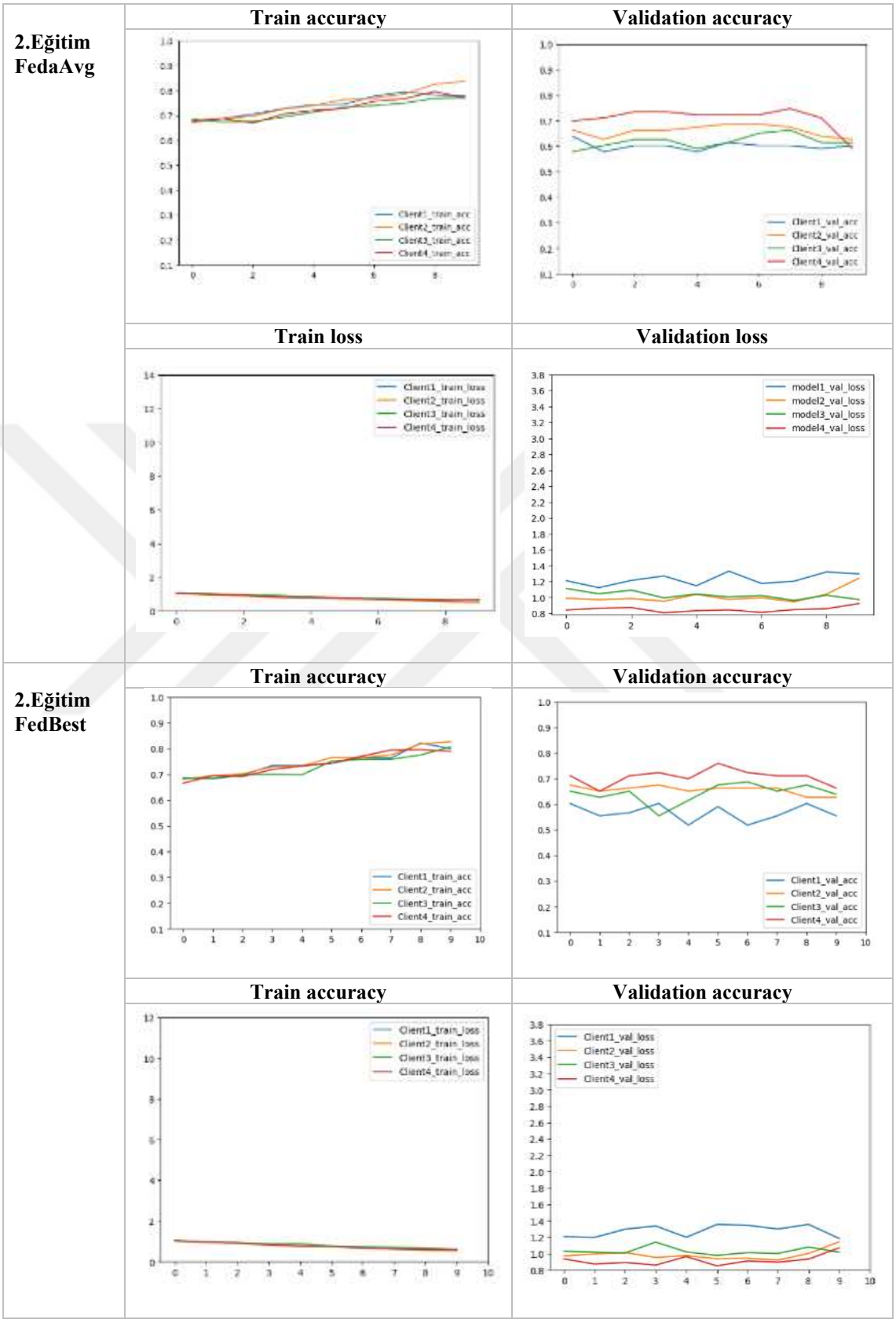
İkinci eğitim senaryosundan önce ilk eğitim turunden elde edilen uç noktalardaki yerel model parametreleriyle federe öğrenme yaklaşımlarında olan FedAvg ve FedBest ile küresel model güncellenmiştir. FedAvg senaryosunda, Uç nokta 1 yerel modelinin, uç nokta 2 yerel modelinin, uç nokta 3 yerel modelinin ve uç nokta 4 yerel modelinin test doğruluk oranları ilk eğitim turundaki sonuçlarına göre arttığı gözlemlenmiştir. Uç nokta 1 yerel modelinin test doğruluk oranı %67,66'ya, uç nokta 2 yerel modelinin test doğruluk oranı %67,66'ya, uç nokta 3 yerel modelinin test doğruluk oranı %65,27'e ve uç nokta 4 yerel modelinin test doğruluk oranı %62,28'e ulaşmıştır. FedBest senaryosunda, uç nokta 1 yerel modelinin, uç nokta 2 yerel modelinin, uç nokta 3 yerel modelinin ve uç nokta 4 yerel modelinin test doğruluk oranlarının ilk eğitim turundaki sonuçlarına göre arttığı gözlemlenmiştir. Uç nokta 1 yerel modelinin test doğruluk oranı %61,68'e, uç nokta 2 yerel modelinin test doğruluk oranı %64,07'ye, uç nokta 3 yerel modelinin test doğruluk oranı %68,26'ya ve uç nokta 4 yerel modelinin test doğruluk oranı %66,47'ye ulaşmıştır. Bu durumda, ikinci eğitim sonunda uç nokta 1' den gelen modelin en yüksek test doğruluk oranına sahip olduğu görülmüştür (%67,56).

Üçüncü eğitim FedAvg senaryosunda, uç nokta 1 yerel modelinin test doğruluk oranı %67,66'a uç nokta 2 yerel modelinin test doğruluk oranı %69,46'a, uç nokta 3 yerel modelinin test doğruluk oranı %61.08'e ve uç nokta 4 yerel modelinin test doğruluk oranı %64,67'ye ulaşmıştır. FedBest senaryosunda ise uç nokta 1 yerel modelinin test doğruluk oranı %72,46'a, uç nokta 2 yerel modelinin test doğruluk oranı %68,86'ya, uç nokta 3 yerel modelinin test doğruluk oranı %59,28'e ve uç nokta 4 yerel modelinin test doğruluk oranı %70,66'ya ulaşmıştır.

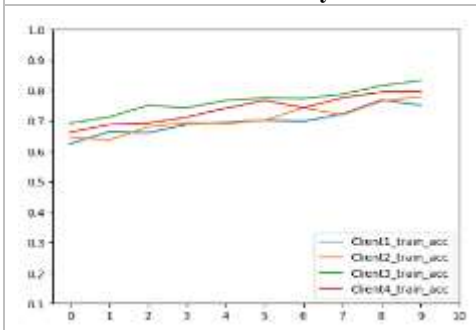
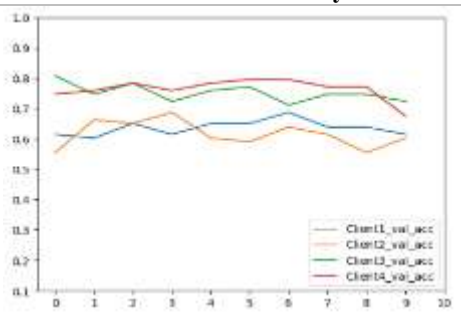
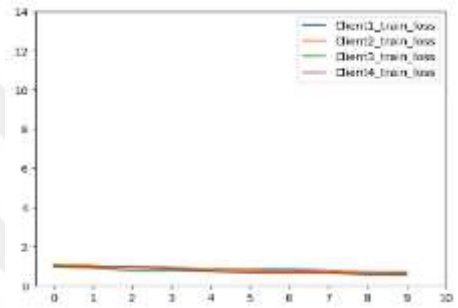
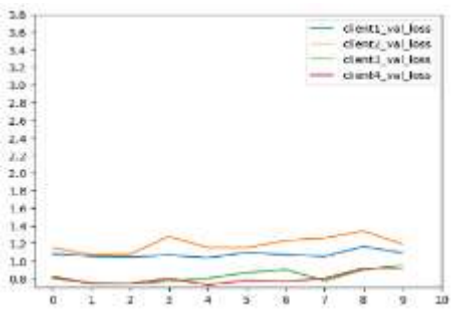
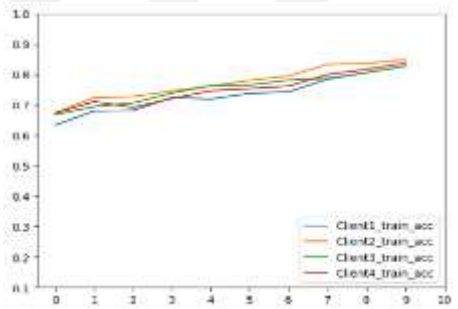
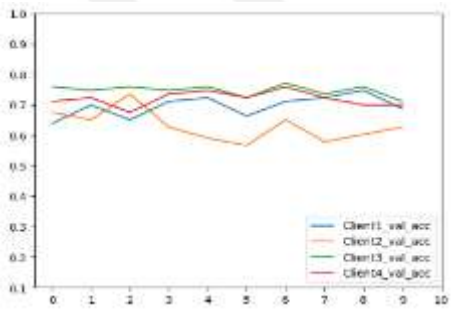
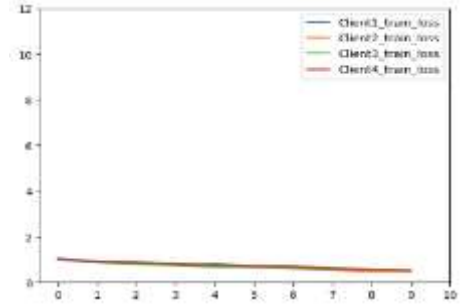
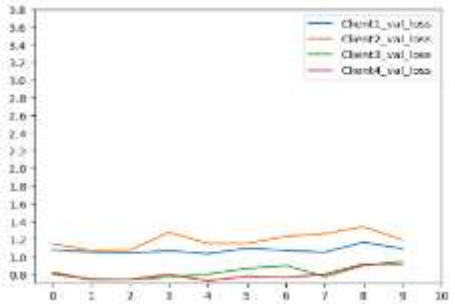
Şekil 3.11-3.13'te üç eğitim boyunca alınan uç noktalardaki yerel model performans sonuçlarının grafikleri sunulmaktadır. Grafikler, gösterilen 30 epoch sonunda her uç noktanın yerel modelinin eğitim doğruluğu (train accuracy) ve kayıp değerlerini (train loss), ayrıca validasyon doğruluğu (validation accuracy) ve kayıp değerlerini (validation loss) göstermektedir. Grafikler, her uç noktanın eğitim sürecindeki performansını ve yerel modelin doğruluğu ile kayıp üzerindeki değişimleri takip etmemize olanak sağlamaktadır.

	Train accuracy	Validation accuracy
1.Eğitim		
	Train loss	**Validation loss**
		

Şekil 3.11. Birinci eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri.



Şekil 3.12. İkinci eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri.

3. Eğitim FedAvg	**Train accuracy**	**Validation accuracy**
		
	Train loss	**Validation loss**
		
3. Eğitim FedBest	**Train accuracy**	**Validation accuracy**
		
	Train accuracy	**Validation accuracy**
		

Şekil 3.13. Üçüncü eğitim sonu DermaMNIST veri seti deney sonuçları grafikleri.

3.3. İletişim Topolojisinin Performans Üzerindeki Etkisi

Daha önceki çalışmada, her bir uç noktanın doğrudan merkezi sunucu ile iletişim kurduğu star topoloji iletişim şeklinin kullanılmıştır. Bu iletişim şeklinde, uç noktalar, verilerini merkezi sunucuya gönderir ve model güncellemeleri de merkezi sunucu tarafından yönetilir. Bu yaklaşım, uç noktaların merkezi sunucunun tüm veri ve model parametrelerini kontrol ettiği bir yapıyı ifade eder.

Ring topolojisi, uç noktaların dairesel bir yapıda birbirleriyle iletişim kurduğu bir yapıyı ifade eder. Bu çalışmada, veri uç noktalarının doğrudan merkezi sunucuyla iletişim kurmak yerine, birbirleriyle iletişim kurarak modelin güncellenmesine olanak sağlayan ring topolojisi incelenmiştir. Star topolojisi kullanılarak yapılan model güncellemeleriyle ring topolojisi kullanılarak yapılan model güncellemelerinin yakınsama üzerindeki etkisi karşılaştırılmıştır. İki farklı iletişim topolojisinin uç nokta yerel model doğrulukları üzerindeki etkisini karşılaştırmak için elde edilen sonuçlar Tablo 3.9-3.11'de sunulmuştur.

Tablo 3.9. BloodMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar.

BloodMNIST	**FedAvg**		**FedBest**	
Uç Nokta	Star	Ring	Star	Ring
1	0,8239	0,8415	0,8169	0,8803
2	0,8204	0,5458	0,8345	0,8592
3	0,8345	0,8204	0,8275	0,8592
4	0,8310	0,7782	0,8275	0,8803

Tablo 3.9'daki verilere göre, BloodMNIST veri seti üzerinde Star ve Ring topolojilerinin uç noktaların model doğrulukları üzerinde farklı etkileri görülmüştür. Uç nokta 1 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %82,39 iken, Ring topolojisinde FedBest kullanıldığında %84,15'e yükselmiştir. Ring topolojisi, uç nokta 1'in model doğruluğunu artırmıştır. Uç nokta 2 için, Star topolojisinde FedAvg

kullanıldığında model doğruluk oranı %82,04 iken, Ring topolojisinde FedBest kullanıldığında %54,58'e düşmüştür. Bu durumda, Ring topolojisi kullanımı uç nokta 2'nin model doğruluğunu düşürmüştür. Uç nokta 3 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %83,45 iken, Ring topolojisinde FedBest kullanıldığında %82,04'e düşmüştür. Ring topolojisi, uç nokta 3'ün model doğruluğunu az miktarda düşürmüştür. Uç nokta 4 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %83,10 iken, Ring topolojisinde FedBest kullanıldığında %77,82'ye düşmüştür. Ring topolojisi uç nokta 4'ün model doğruluğunu düşürmüştür.

Tablo 3.10. PathMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar.

PathMNIST	**FedAvg**		**FedBest**	
Uç Nokta	Star	Ring	Star	Ring
1	0,6940	0,7191	0,8169	0,7090
2	0,7174	0,7124	0,8345	0,7308
3	0,7023	0,7124	0,8275	0,7241
4	0,7207	0,7074	0,8275	0,7241

Tablodaki 3.10’ daki verilere göre, FedAvg ve FedBest algoritmalarının Star ve Ring topolojileri altında uç noktaların model doğrulukları üzerinde farklı etkileri görülmüştür. Uç nokta 1 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %69,40 iken, Ring topolojisinde %71,91'e yükselmiştir. Ring topolojisi, uç nokta 1'in model doğruluğunu artırmıştır. Ancak, FedBest yaklaşımı kullanıldığında Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde edilmiştir. Uç nokta 2 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %71,74 iken, Ring topolojisinde de %71,24 hesaplanmıştır. FedBest yaklaşımı kullanıldığında ise Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde edilmiştir. Uç nokta 3 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %70,23 iken, Ring topolojisinde %71,24'e yükselmiştir. FedBest yaklaşımı kullanıldığında ise Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde

edilmiştir. Uç nokta 4 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %72,07 iken, Ring topolojisinde %70,74'e düşmüştür. FedBest yaklaşımı kullanıldığında ise Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde edilmiştir. Sonuç olarak, Ring topolojisinin genel olarak model doğruluğunu artırdığı görülse de FedBest yaklaşımı kullanıldığında Star topolojisi daha yüksek model doğruluğu sağlamıştır.

Tablo 3.11. DermaMNIST veri setinde Star ve Ring Topolojileri ile elde edilen sonuçlar.

DermaMNIST	**FedAvg**		**FedBest**	
Uç Nokta	Star	Ring	Star	Ring
1	0,6766	0,6048	0,7246	0,6527
2	0,6946	0,6287	0,6886	0,6108
3	0,6108	0,6347	0,5928	0,6108
4	0,6467	0,6467	0,7066	0,6527

Tablo 3.11'deki verilere göre, DermaMNIST veri seti üzerinde FedAvg ve FedBest algoritmalarının Star ve Ring topolojileri altında uç noktaların model doğrulukları üzerinde farklı etkileri görülmüştür. Uç nokta 1 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %67,66 iken, Ring topolojisinde %60,48'e düşmüştür. FedBest yaklaşımı kullanıldığında ise Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde edilmiştir. Uç nokta 2 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %69,46 iken, Ring topolojisinde %62,87'e düşmüştür. FedBest yaklaşımı kullanıldığında ise Star topolojisinde Ring topolojisine göre daha yüksek bir model doğruluğu elde edilmiştir. Uç nokta 3 için, Star topolojisinde FedAvg kullanıldığında model doğruluk oranı %61,08 iken, Ring topolojisinde %63,47'ye yükselmiştir. Ring topolojisi, uç nokta 3'te her iki yaklaşım için model doğruluğunu artırmıştır. Uç nokta 4 için, Star topolojisinde FedAvg kullanıldığında

model doğruluk oranı %64,67 iken, Ring topolojisinde de %64,67 olarak hesaplanmıştır. Ring topolojisi, FedAvg yaklaşımında uç nokta 4'ün model doğruluğunu değiştirmemiştir.

Tabloda verilen üç farklı veri seti (BloodMNIST, PathMNIST, DermaMNIST) üzerindeki sonuçlar incelendiğinde, BloodMNIST verisetinde Ring topolojisi altında FedBest yaklaşımının kullanılması tüm uç noktalarda daha yüksek model doğruluğu sağlamıştır. PathMNIST ve DermaMNIST veri setlerinde ise Star topolojisi altında FedBest yaklaşımı kullanıldığında, bazı uç noktaların model doğruluklarında belirgin bir artış görülmüştür. Star ve Ring topolojisinde FedBest yaklaşımının kullanılması model doğruluğunda genel anlamda daha iyi sonuçlar vermiştir.

4. BÖLÜM

TARTIŞMA-SONUÇ ve ÖNERİLER

4.1.Tartışma

Veri paylaşımının uygun olmadığı senaryolarda, Federe öğrenme, medikal verilerin sınıflandırılmasında etkili bir yöntemdir. Bu çalışmada, FedAvg ve FedBest algoritmalarının medikal veri sınıflandırması üzerindeki performansları karşılaştırılmıştır. Ayrıca, iletişim topolojisi olarak Star ve Ring topolojileri altında FedAvg ve FedBest yöntemleri kullanılarak medikal veri sınıflandırma performansı üzerindeki etkileri karşılaştırılmıştır.

FedAvg, federe öğrenme için yaygın olarak kullanılan bir algoritmadır. Bu algoritma, uç noktaların güncellediği yerel model parametrelerinin ortalamalarını alarak merkezi sunucudaki küresel modeli günceller. Bu şekilde, farklı uç noktaların bilgileri birleştirilir ve küresel bir model elde edilir. FedAvg, küresel bir modelin güncellenmesinde etkili olmasına rağmen, performans açısından bazı zorluklarla karşılaşabilir. Özellikle, tüm uç noktaların küresel model güncellemesinde kullanılması, performansı düşük olan yerel modellerin güncellemeye katılımından kaynaklı olarak küresel modelin genel performansını düşürebilir. FedBest, FedAvg'ye kıyasla küresel model performansını geliştirmeyi sunan bir algoritmadır. Bu algoritma, yerel uç noktaların performansını değerlendirerek en iyi performansı gösteren modeli seçer ve küresel modele entegre eder. Böylece, daha iyi bir genelleme yeteneği elde edilir. FedBest, en iyi modellerin seçilmesi sayesinde daha etkili sonuçlar elde edilebilir.

İletişim topolojileri olarak Star ve Ring topolojileri, federe öğrenme algoritmalarında uç noktaların nasıl iletişim kuracağını belirler. Star topolojisinde, tüm uç noktalar merkezi bir sunucu ile doğrudan iletişim kurar ve model güncellemeleri merkezi sunucu tarafından yönetilir. Ring topolojisinde ise, uç noktalar birbirleriyle dairesel bir yapıda iletişim kurar, yani her uç nokta komşusu ile veri ve model güncellemelerini paylaşır. Star topolojisi, basit ve kolay yönetilebilir olması nedeniyle yaygın olarak kullanılır. Merkezi sunucu üzerinden yönetildiği için tüm uç noktaların model güncellemelerini toplayarak küresel modeli güncellemesi daha kolaydır. Ancak yüksek iletişim maliyeti ve merkezi sunucuya olan bağımlılığı dezavantajları vardır. Ring topolojisi ise, doğrudan uç noktalar arasında iletişim sayesinde iletişim maliyetini düşürür ve merkezi sunucuya olan bağımlılığı azaltır. Bu nedenle daha büyük ve heterojen veri setleri için daha etkili olabilir. Ancak doğrudan iletişim nedeniyle zamanlama ve senkronizasyon zorlukları ortaya çıkabilir.

4.2 Sonuç ve Öneriler

Bu çalışmada, federe öğrenme algoritmaları FedAvg ve FedBest'in medikal veri sınıflandırması üzerindeki performansını değerlendirilmiştir. Deneylerimizde, her iki algoritmanın da iyi sonuçlar verdiğini görülmüştür. Ancak, FedBest'in daha iyi performans gösterdiği ve daha yüksek bir doğruluk oranı sağladığı tespit edilmiştir. Bu bulgular ışığında, medikal veri sınıflandırmasında federe öğrenme yöntemlerinin etkili olduğu sonucuna varılmıştır. Veri gizliliğini koruyarak birden çok uç noktanın verilerinden yararlanmak, daha genel ve güncel bir küresel modelin oluşturulmasını sağlamıştır. FedBest yaklaşımı ile en iyi performans gösteren modelin seçilmesi ve küresel modele entegrasyonu sayesinde daha iyi sonuçlar elde edilmiştir.

FedAvg ve FedBest yaklaşımlarının da seçilen iletişim topolojisine göre model performansına farklı etkileri görülmüştür. FedBest, en iyi performansa sahip uç noktanın bilgisini daha fazla değerlendirerek Star topolojisinde daha iyi sonuçlar elde etmiştir. Medikal veri sınıflandırmasında kullanılacak olan iletişim topolojisi ve algoritmanın seçimi; veri dağılımı, iletişim maliyeti ve diğer faktörlere bağlı olarak yapılmalıdır.

Medikal veri sınıflandırması için federe öğrenme yaklaşımları kullanılmasının devam etmesi ve özellikle FedBest'in daha geniş çapta değerlendirilmesi, ileriye dönük olarak, federe öğrenme yaklaşımlarının daha fazla veri seti ve farklı medikal uygulamalarda test edilmesi ve iyileştirilmesi önemlidir. Böylece medikal alanda daha etkili ve güvenilir sınıflandırma modelleri elde edilebilir. Bu çalışmada federe öğrenme yöntemleri, medikal veri sınıflandırmasında etkili bir yaklaşım sunmuştur. FedAvg ve FedBest gibi algoritmalar, medikal verilerin gizliliğini koruyarak daha iyi sonuçlar elde etmek için değerlendirilmelidir. Bu çalışmanın bulguları, gelecekteki çalışmalara ışık tutacak ve daha iyi medikal veri sınıflandırma modellerinin geliştirilmesine katkıda bulunacaktır.

KAYNAKÇA

Büyüknacar, Y., Canbay,Y., 2021. Federe öğrenme ve veri mahremiyeti. **Nobel Yayınları**, **Cilt (**3): 59-77.

Kelvin., 2020. Introduction to federated learning and challenges. (Web sayfası: **https://towardsdatascience.com/introduction-to-federated-learning-and-challenges-ea7e02f260ca**), (Erişim tarihi: 10 Mayıs 2021).

Demirhan, A., Kılıç, Y. A., İnan, G., 2010. Tıpta yapay zekâ uygulamaları. **Yoğun Bakım Dergisi, 9** (1): 31-41

Szegedi, G., Kiss, P., Horváth, T., 2019. Evolutionary Federated Learning on EEG-data. **ITAT**, pp. 71-78.

Lee, J., Sun, J., Wang, F., Wang, S., Jun, C. H.,Jiang, X., 2018. Privacy-preserving patient similarity learning in a federated environment: development and analysis. **JMIR medical informatics**, **6**(2): e7744.

Huang, L., Yin, Y., Fu, Z., Zhang, S., Deng, H., Liu, D.,2020. LoAdaBoost: Loss based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data. **Plos one, 15**(4): e0230706.

Nazir, S., Kaleem, M., 2023. Federated Learning for Medical Image Analysis with Deep Neural Networks. **Diagnostics, 13**(9): 1532.

Kumar, R., Khan, A. A., Kumar, J., Golilarz, N. A., Zhang, S., Ting, Y., Zheng, C., Wang, W., 2021. Blockchain-federated-learning and deep learning models for covid-19 detection using ct imaging. **IEEE Sensors Journal, 21**(14):16301-16314.

Price, W. N.,Cohen, I. G., 2019. Privacy in the age of medical big data. **Nature medicine, 25**(1): 37-43.

Lee, J. S., Darcy, K. M., Hu, H., Casablanca, Y., Conrads, T. P., Dalgard, C. L., ... & Shriver, C. D.,2019. From discovery to practice and survivorship: building a national real-world data learning healthcare framework for military and veteran cancer patients. **Clinical Pharmacology & Therapeutics, 106**(1): 52-57.

Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., ... & Feng, A., 2019. Privacy-preserving federated brain tumour segmentation. In Machine Learning in Medical Imaging: 10th International Workshop, MLMI 2019, Held in Conjunction with MICCAI 2019, Shenzhen, China, October 13, 2019. **Springer International Publishing, Proceedings 10**, pp. 133-141.

Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., Bakas, S., 2019. Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In Brainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries: 4th International Workshop, BrainLes 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 16, 2018, Revised Selected Papers, **Springer International Publishing**, **Part I 4**, pp. 92-104.

Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W., & Ilie-Zudor, E., 2018. Chained anomaly detection models for federated learning: An intrusion detection case study. **Applied Sciences, 8**(12): 2663.

Roth, H. R., Chang, K., Singh, P., Neumark, N., Li, W., Gupta, V., ... & Kalpathy-Cramer, J., 2020. Federated learning for breast density classification: A real-world implementation. In Domain Adaptation and Representation Transfer, and Distributed and Collaborative Learning: Second MICCAI Workshop, DART 2020, and First MICCAI Workshop, DCL 2020, Held in Conjunction with MICCAI 2020, Lima, Peru, October 4–8, 2020, **Springer International Publishing, Proceedings 2**, pp. 181-191.

Ju, C., Gao, D., Mane, R., Tan, B., Liu, Y., Guan, C., 2020. Federated transfer learning for EEG signal classification. **2020 42nd annual international conference of the IEEE engineering in medicine & biology society (EMBC)**, pp. 3040-3045.

Bdair, T., Navab, N., Albarqouni, S., 2021. FedPerl: semi-supervised peer learning for skin lesion classification. **International Conference on Medical Image Computing and Computer-Assisted Intervention**, pp. 336-346.

Wang, J., Liu, Q., Liang, H., Joshi, G., Poor, H. V., 2020. Tackling the objective inconsistency problem in heterogeneous federated optimization. **Advances in neural information processing systems, 33**: 7611-7623.

Jatain, D., Singh, V., Dahiya, N., 2022. A contemplative perspective on federated machine learning: Taxonomy, threats & vulnerability assessment and challenges. **Journal of King Saud University-Computer and Information Sciences, 34**(9): 6681-6698.

Nergiz, M.,2022. İşbirlikçi Yapay Zekâ Konsepti: Federe Öğrenmeye Genel Bir Bakış. **Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 13**(2): 279-286.

Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., Liu, X., He, B., 2021. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. **IEEE Transactions on Knowledge and Data Engineering.**

McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B., 2017. Communication-efficient learning of deep networks from decentralized data. **Artificial intelligence and statistics, PLMR,** pp. 1273-1282.

Flower aggregation algorithms. (Web sayfası: **https://flower.dev/docs/**) (Erişim tarihi: Ağustos 2023).

Isik-Polat, E., Polat, G., Kocyigit, A., & Temizel, A., 2021. Evaluation and analysis of different aggregation and hyperparameter selection methods for federated brain tumor segmentation. **International MICCAI Brainlesion Workshop**, pp. 405-419.

Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., Smith, V., 2020. Federated optimization in heterogeneous networks. **Proceedings of Machine learning and systems, 2**:429-450.

Asad, M., Moustafa, A., Ito, T., 2020. FedOpt: Towards communication efficiency and privacy preservation in federated learning. **Applied Sciences, 10**(8):2864.

Reddi, S., Charles, Z., Zaheer, M., Garrett, Z., Rush, K., Konečný, J., Kumar, S., McMahan, H. B.,2020. Adaptive federated optimization. **arXiv preprint,** arXiv:2003.00295.

Süzen, A. A., & Kayaalp, K., 2019. Büyük Verilerde Gizlilik Tabanlı Yaklaşım: Federe Öğrenme. **International Journal of 3d Printing Technologies and Digital Industry, 3**(3): 297-304.

Dou, Q., So, T. Y., Jiang, M., Liu, Q., Vardhanabhuti, V., Kaissis, G., ... & Heng, P. A., 2021. Federated deep learning for detecting COVID-19 lung abnormalities in CT: a privacy-preserving multinational validation study. **NPJ digital medicine, 4**(1): 60.

Li, X., Gu, Y., Dvornek, N., Staib, L. H., Ventola, P., Duncan, J. S., 2020. Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation: ABIDE results. **Medical Image Analysis, 65**:101765.

Huang, L., Shea, A. L., Qian, H., Masurkar, A., Deng, H., Liu, D., 2019. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. **Journal of biomedical informatics, 99**: 103291.

Garcia Bernal, D.,2020. Decentralizing Large-Scale Natural Language Processing with Federated Learning.

Imteaj, A.,Amini, M. H., 2022. Leveraging asynchronous federated learning to predict customers financial distress. **Intelligent Systems with Applications, 14:** 200064.

Long, G., Tan, Y., Jiang, J., Zhang, C., 2020. Federated learning for open banking. **Federated Learning: Privacy and Incentive**, pp. 240-254.

Li, J., Cui, T., Yang, K., Yuan, R., He, L., Li, M., 2021. Demand forecasting of e-commerce enterprises based on horizontal federated learning from the perspective of sustainable development. **Sustainability, 13**(23):13050.

Behavioral Informatics & Interaction Computation Lab (BIIC) (Web sayfası: **https://biic.ee.nthu.edu.tw/blog-detail.php?id=2**)(Erişim Tarihi: 14.06.2023).

Tüfekçi, M., Karpat, F., 2019. Derin Öğrenme Mimarilerinden Konvolüsyonel Sinir Ağları (CNN) Üzerinde Görüntü İşleme-Sınıflandırma Kabiliyetininin Arttırılmasına Yönelik Yapılan Çalışmaların İncelenmesi. **International Conference on Human-Computer Interaction, Optimization and Robotic Applications**, pp. 28-31.

Wu, J., Drew, S., Dong, F., Zhu, Z., Zhou, J., 2023. Topology-aware Federated Learning in Edge Computing: A Comprehensive Survey. **arXiv preprint,** arXiv:2302.02573.

Hope, C., 2023.Star topology and Ring topology, 2023 (Web sayfası: **https://www.computerhope.com/**) (Erişim tarihi: Ağustos 2023).

Wu, J., Drew, S., Dong, F., Zhu, Z., Zhou, J.,2023. Topology-aware Federated Learning in Edge Computing: A Comprehensive Survey. **arXiv preprint,** arXiv:2302.02573.

Yang, G., Mu, K., Song, C., Yang, Z., Gong, T., 2021. Ringfed: Reducing communication costs in federated learning on non-iid data. **arXiv preprint,** arXiv:2107.08873.

Yang, J., Shi, R., Wei, D., Liu, Z., Zhao, L., Ke, B., Pfister, H., Ni, B., 2023. MedMNIST v2-A large-scale lightweight benchmark for 2D and 3D biomedical image classification. **Scientific Data, 10**(1):41.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı: Beyza Nur AKŞİT

Uyruğu: Türkiye (T.C)

EĞİTİM

Derece	**Kurum**	**Mezuniyet Tarihi**
Yüksek Lisans	Erciyes Üniversitesi, Bilgisayar Mühendisliği	2023
Lisans	Erciyes Üniversitesi, Bilgisayar Mühendisliği	2019
Lise	Mustafa Eminoğlu Anadolu Lisesi, Kayseri	2014

İŞ DENEYİMLERİ

Yıl	**Kurum**	**Görev**
2021-Halen	Aksaray Üniversitesi	Araştırma Görevlisi

YABANCI DİL

İngilizce