International Journal of 3D Printing Technologies and Dijital Industry
Uluslararası 3B Yazıcı Teknolojileri ve Dijital Endüstri Dergisi

BÜYÜK VERİLERDE GİZLİLİK TABANLI YAKLAŞIM: FEDERE ÖĞRENME

Ahmet Ali Süzen[a*], Kıyas Kayaalp[a]

[a] Isparta Uygulamalı Bilimler Üniversitesi, Uluborlu Selahattin Karasoy Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, TÜRKİYE

[*]*Sorumlu Yazar: ahmetsuzen@isparta.edu.tr*

(Geliş/Received: 23.12.2019**; Düzeltme/Revised:** 24.12.2019**; Kabul/Accepted:** 29.12.2019**)**

ÖZET

Bu çalışmada dağıtık yapılardaki büyük verilerden gizlilik tabanlı makine öğrenmesi uygulamaları geliştirilmesi için federe öğrenme biçimi anlatılmıştır. Federe öğrenme eğitim verilerini yerelde tutarken, cep telefonları ve IoT (Internet of Things) cihazları gibi kaynakları kısıtlı uç aygıtların tahmin için paylaşılan bir model öğrenmesini sağlar. Federe öğrenme büyük ve heterojen ağlarda modellerin istatiksel eğitimlerini içerir. Bu dağıtık yapı içerisinde temel amaç toplam kayıp fonksiyon değerini minimize edebilmektir. Dağıtık yerel cihazlarda modelleri federe öğrenme ile eğitmedeki istatistiksel ve sistematik zorluklar, federe öğrenmenin gerçek dünyaya uygulanmasını zorlaştırmaktadır. Zorlukların çözümü ile ilgili yeni yaklaşımlar ve algoritmalar önerilmektedir. Elde edilen sonuçlar doğrultusunda federe öğrenmenin uygulanması ile merkezi yaklaşım, gizlilik, güvenlik, düzenleyici ve ekonomik olarak faydalar sağlayacağı öngörülmektedir.

Anahtar Kelimeler: Federe Öğrenme, Makine Öğrenmesi, Gizlilik, Büyük Veri.

A PRIVACY-BASED APPROACH IN BIG DATA: FEDERATED LEARNING

ABSTRACT

This study describes the Federated way of learning to develop privacy-based machine learning applications from large data in distributed structures. Federated learning allows learning a shared model for forecasting resource-restricted end devices, such as mobile phones and IoT (Internet of Things) devices, while keeping training data locally. Federated learning involves statistical training of models in large and heterogeneous networks. The main purpose of this distributed structure is to minimize the total loss function value. The statistical and systematic challenges in federated learning and training in distributed local devices make it difficult to apply federated learning to the real world. It has been proposed new approaches and algorithms for solving challenges. In lights with the results achieved, it is envisaged that the implementation of federated learning and the central approach will bring benefits in terms of privacy, security, regulatory and economic terms.

Keywords: Big Data, Federated Learning, Machine Learning, Privacy.

1. GİRİŞ

Gelişen internet teknolojileri (sosyal medya, web sayfaları, alışveriş siteleri vb.), Sanayi 4.0 devrimi (akıllı fabrikalar, nesnelerin interneti, siber-fiziksel sistemler) ve teknolojik gelişmelerle birlikte sürekli olarak veriler üretilmektedir [1-2]. Üretilen bu veriler; güvenlik, pazarlama, sağlık, ar-ge gibi birçok

sektörde kullanılmaktadır. Büyük veri olarak nitelendirilen bu verilerin kullanımında şirket bilgilerinin, kişiye özgü verilerin mahremiyeti büyük önem taşımaktadır [3].

Bilim insanları tarafından son 10 yılda yapay zekâ, makine öğrenmesi ve derin öğrenme konularında literatüre yeni algoritmalar, yeni çözüm yolları ve hibrit yöntemler kazandırılmış, aynı zamanda kazandırılmaya da devam etmektedir [4]. Bu gelişmeler yapay zekâ dünyası için yeni öngörülerin ve yeni kapıların açılmasına olanak sağlamaktadır. Büyük Veri, yapay zekâ, makine öğrenmesi ve derin öğrenmenin hammaddesidir [5]. Tahmin sistemleri, konuşma tanıma sistemleri, görüntü tanıma sistemleri, sohbet robotları gibi sistemler büyük miktardaki verilere ihtiyaç duymaktadır. İhtiyaç duyulan büyük verilerin toplanmasında kişisel verilerin mahremiyeti dikkat edilmesi gereken konulardan birisidir. Örneğin hastalıkların teşhis edilmesinde kullanılan kan testlerinin herkesle paylaşılması kişi mahremiyetini terstir. Ama doktorların elinde ne kadar çok veri bulunursa derin öğrenme yöntemleri ile de hastalıkların teşhisi bir o kadar kolaylaşmaktadır. Literatüre yeni kazandırılan "Federe Öğrenme" ile hem kişi mahremiyeti korunmakta, hem de ihtiyaç duyulan büyük veriler elde edilmektedir [6-7].

Bu çalışmada veri mahremiyeti tabanlı federe öğrenme yöntemi incelenmiştir. Federe öğrenme biçimi makine öğrenme uygulamalarında merkezi modelinin yerel modellerden, verilerini görmeden beslenmesidir. Yerel modeller kendi veri kümesi üzerinden modeli eğitir. Eğitilen modelin ağırlıkları ve özellikleri merkezi modele aktarılır. Merkezi model gelen parametrelere göre güncellenir. Güncelleme sonrası yeni parametreler yerel modellere aktarılır. Bu değerler dizisi sayesinde merkezi model verileri görmeden yüksek doğruluk ve performans ile çalışabilmektedir. Federe öğrenmede uygulamaları geliştirilirken hem merkezi hem de yerel deki parametrelerin gizliliği ve güvenliği önemlidir. Bunun için farklı gizlilik algoritmaları kullanılmaktadır. Özellikle veri mahremiyetinin önemli olduğu sağlık, eğitim, bankacılık gibi sektörlerde federe öğrenmenin uygulanması performanslı makine öğrenme modellerinin geliştirilmesine imkân sağlayacaktır.

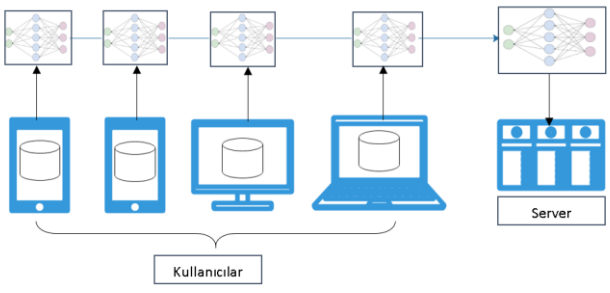
2. FEDERE ÖĞRENME

Federe Öğrenme kullanıcı verilerinin, kullanıcıların cihazlarından hiç çıkmadığı, eğitim sürecinin birçok kullanıcı arasında dağıtıldığı işbirlikçi bir makine öğrenmesi yöntemidir (Şekil 1). Google tarafından önerilen Federe Öğrenme; veri gizliliğini önlemek amacıyla birden fazla cihaza eğitim modeli dağıtılarak, eğitimin kullanıcı cihazlarında yapılmasıdır [8]. Klasik makine öğrenmesinde, eğitim verileri bir veri merkezinde toplanırken federe öğrenmede kişi bilgileri kullanıcı cihazlarında kalmaktadır.

Federe öğrenmede ki amaç beklenen ampirik kaybı en aza indirgeyen bir sinir ağı parametresinin vektörünü bulmaktadır [7].

$$L(w) = \sum_{D_t \in D} \sum_{(x,y) \in D_t} l(f(x,w), y)$$

Burada l(x,y) kayıp fonksiyonudur. Her i yerel katılımcı D_i veri kümesinde tutulur. Her yerel bilgisayar kendi veri kümesinde modeli öğrenir ve kayıp değerini en aza indirerek merkezi sunucuya gönderir[9].



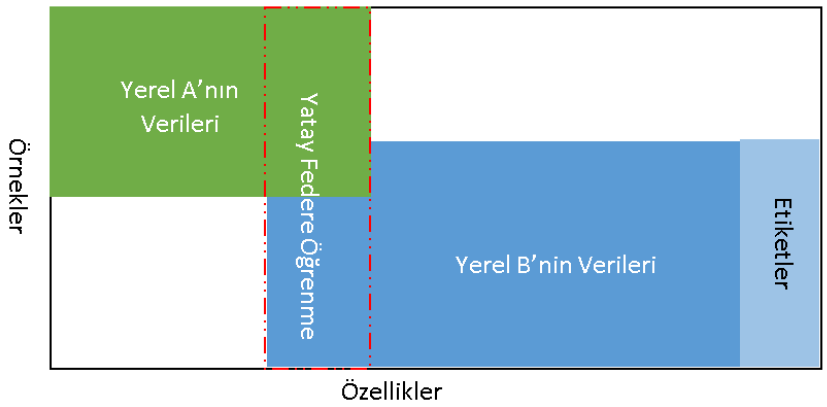
Şekil 1. Federe öğrenme yapısı.

2.1. Federe Öğrenme Türleri

Federe Öğrenmede problemlerin çözümü, Yatay, Dikey ve Federe Transfer öğrenmeleri ile gerçekleştirilir.

2.1.1. Yatay Federe Öğrenme

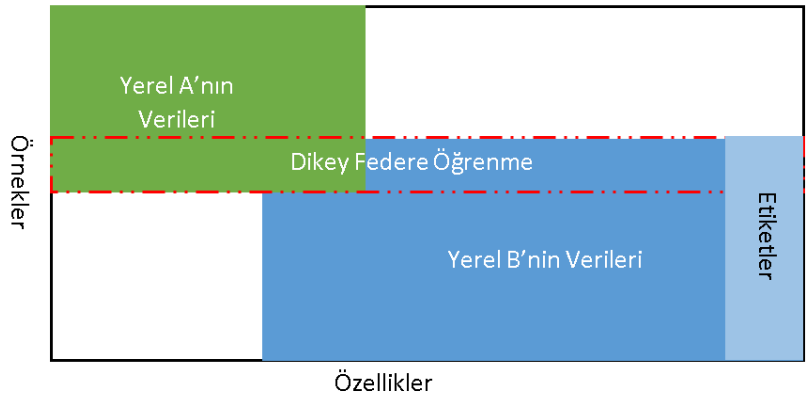
İki veri kümesinin aynı özellik alanını paylaştığı ancak örneklerde farklı senaryoların olduğu durumlarda Yatay Federe Öğrenme yöntemi kullanılır (Şekil 2). Örnek olarak iki banka kendi şubelerinde çok farklı kullanıcı gruplarına sahip olabilir ve kullanıcıların kesişimi çok küçüktür [10]. Bununla birlikte, işleri çok benzer, bu nedenle de kaydedilen kullanıcı özellikleri aynıdır. Bu gibi durumlarda, yatay bir Federe öğrenme modeli oluşturulabilir [11].



Şekil 2. Yatay federe öğrenme modeli.

2.1.2. Dikey federe öğrenme

İki veri kümesinin aynı kullanıcıları paylaştığı ancak özellik alanında farklı olduğu durumlarda Dikey Federe Öğrenme yöntemi kullanılır (Şekil 3). Örnek olarak, aynı müşterilere sahip bir banka ve bir e-ticaret firması olsun. Banka kullanıcılarının gelir ve harcama davranışını ve kredi notunu, e-ticaret firması ise kullanıcılarının alışveriş tarama ve satın alma geçmişini kaydettiğinden, kullanıcı öznitellikleri birbirinden farklıdır. Bu nedenle müşterilerin oluşturduğu veri kümesinin boyutu çok büyüktür. Dikey Federe Öğrenme yöntemi, bu farklı özellikleri şifreli olarak bir araya getirerek, müşterilerin gelir durumuna uygun alışveriş önerileri sunabilen bir hesaplama sürecidir [5,10].

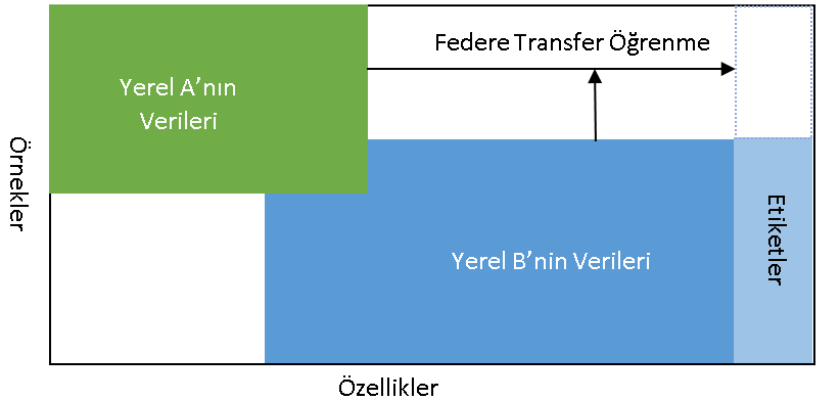


Şekil 3. Dikey federe öğrenme modeli.

2.1.3. Federe transfer öğrenme

İki veri kümesinin hem kullanıcı hem de özellik alanlarının farklı olduğu durumlarda Federe Transfer Öğrenme yöntemi kullanılır (Şekil 4). Türkiye'de bulunan bir banka ile Çin'de bulunan bir e-ticaret firmasının hem kullanıcıları farklı hem de öznitelikleri farklıdır. Bu iki firmanın kullanıcı gruplarının kesişimi çok az sayıdadır. Ayrıca banka ve e-ticaret firması farklı sektörlere hizmet verdiği için öznitelik kesişimi de çok azdır. Bu gibi az sayıdaki verilerin kullanılabileceği federe öğrenmede, etkili çözümlerin

sunulabilmesi ve model performanslarının artırılması için Federe Transfer Öğrenme yöntemi kullanılır [10-12].



Şekil 4. Federe transfer öğrenme modeli.

2.2. Model Geliştirme

Öncelikle en basit hali ile federe öğrenme aşağıdaki basamaklarda anlatıldığı gibi çalışmaktadır.

- Yerel cihazlar merkezi makine öğrenme modelini indirir.
- Kullanıcı makine öğrenme modeliyle bağlantılı uygulamayı kullanırken veriler üretilir.
- Kullanıcı uygulama ile daha fazla etkileşime girmeye başladığında, kullanıcı kullanımına göre daha iyi tahminleri alır.
- Yerel Model, merkezi sunucuyla zamanlanmış senkronizasyon için hazır olduğunda, yereldeki güncellemeler model sunucuya gönderilir.
- Tüm yerellerden gelen modeller toplanır ve modelin en son eğitiminden daha gelişmiş bir modelini oluşturmak için birleşik ortalama işlevi kullanılır.
- Merkezi model eğitildikten sonra geliştirilmiş modelin güncellemeleri yerel katılımcılarında kullanması için aktarılır.

Federe öğrenmede genel olarak veri sahibi ve model sahibi olmak üzere 2 ana varlık bulunmaktadır. Sunucu merkezi modelin eğitim sürecini ve öğrenme hızı gibi hiperparametrelerini yerel modellere belirtir. N = {1, . . . , N}'de her biri özel bir veri kümesi $D_{i\in N}$ olan N veri sahibi kümesini belirtir. Her veri sahibi veri kümesi D_i'yi kullanarak yerel bir model olan W_i'yi eğitmek ve yerel model parametrelerini merkezi sunucuya aktarmak için kullanılır. Sunucuya aktarılmadan önce, $w_i^t = \arg\min L(w_i^t)$ kayıp fonksiyonunu en aza indiren uygun parametreyi bulmak için eğitim t kadar yenilenir. Daha sonra toplanan yerel model parametreleri merkezi bir W_g oluşturmak için $w = \cup_{i\in N} W_i$ olarak toplanır. Yapılan bu işlem W_t modelini eğitmek için kullanılan geleneksel merkezi eğitimden farklıdır. Merkezi model yerel modellerden gelen güncellemeleri topladıktan sonra merkezi kayıp fonksiyonunu en aza indirmek için $L(w_G^t) = \frac{1}{n}\sum_{i=2}^{n} L(w_i^t)$ olarak uygular. İstenilen değer bulununcaya kadar eğitim yerel ve merkezi olarak tekrarlanır. Son adımda merkezi modelin W_g'si yerel modellere gönderir. Federe öğrenmenin uygulanış biçimi için kaba kod Algoritma 1'de verilmiştir.

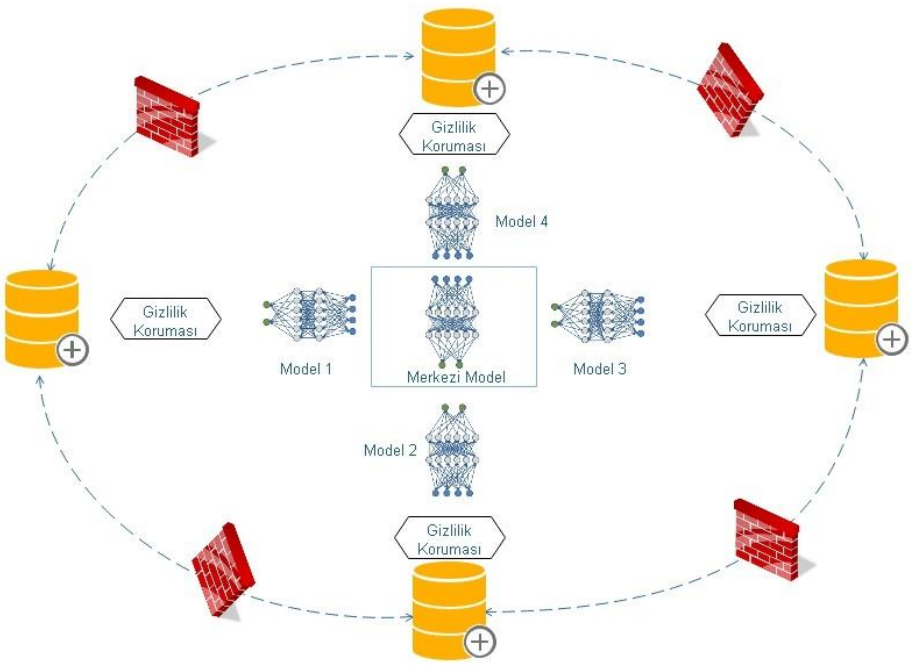
Algoritma 1. Federe öğrenme.

[Yerel]	**[Sunucu]**

B= yerel minibatch boyutu
m= yerel katılımcı sayısı
E= eğitim turu
η = öğrenme oranı
Başla
$w_0 \leftarrow$ rastgele başlatma
{İletişim Boyunca}
for *t*=1,..,*T*,...**do**
$S_t \leftarrow$ (*rastgele alt küme- max (C x K,1) katılımcı*)
{ Her katılımcı için yerel optimizasyon }
for *katılımcı* $k \in S_t$ **do**
yerel ağırlıkları başlat: $w_{t,k} \leftarrow w_{t-1}$
for *epoch* $e \in [1,E]$ **do**
Yerel verileri böl, B ($\frac{B}{n_k}$ B yığınları)
for *yığın* $b \in B$ **do**
$w_{t,k} \leftarrow w_{t-k} - \eta_{local} \Delta l\,(w_{t,k}; b)$
end for
end for
end for
{Merkezi Ortalama}
$w_t \leftarrow \sum_{k \epsilon S_t} \frac{n_k}{n} w_{t,k}$
end for
	Başla w_0
	for *her t* = 0,1,... **do**
	m ← max ($[C \cdot K]$, 1)
	S_t = rastgele m katılımcı ayarla
	for *her katılımcı için* $k \in S_t$ ***in parallel do***
	$w_{t+1}^k = \text{YerelGuncelle}(k, w_t)$
	$w_{t+1} = \sum_{k \epsilon St} \frac{n_k}{n_\sigma} w_{t+1}^k, \quad n_\sigma = \sum_{k \epsilon St} n_k$

2.3. Gizlilik

Federe öğrenmedeki en önemli motivasyon, makine öğrenmelerinin klasik yöntemle geliştirilmesinden kaynaklı gizlilik endişesidir. Federe öğrenme yönteminde veriler yerel bilgisayarı terk etmediği için büyük bir eksikliği gidereceği öngörülmektedir. Her ne kadar verileri yerelde kalsa da sunucuya gönderilen güncellemelerden verilerin tekrardan yapılandırılabileceği düşünülmektedir (Şekil 5). Bundan dolayı federe öğrenme biçiminde gizlilik algoritmaları yaklaşımları geliştirilmektedir. Yaygın olarak federe öğrenmede gizlilik yaklaşımı 3 farklı güvenlik modeli ile sağlanmaktadır.



Şekil 5. Federe öğrenme modelinde gizlilik.

Güvenli Toplama*:* Birden fazla tarafın toplu olarak hesaplamalar yapmasını sağlayan ve bilgi girişinde bulunan tarafların bilgilerinin diğer taraflarca bilinmemesini sağlayan bir şifreleme kümesidir [13]. Gizli Paylaşım mekanizması, kimlik doğrulamalı şifrelemeyle yerel güncellemelerin iletimi için de kullanılır. Güvenli toplama güvenli müzayede, gizlilik korumalı tahmin ve kıyaslama, güvenli tedarik zinciri yönetimi, e-oylama gibi birçok uygulama kullanılmaktadır [14].

Diferansiyel Gizlilik / K-anonimlik: Diferansiyel gizlilik, kalabalık veriler ile çalışan algoritmaların mahremiyet garantisi için yaygın olarak kullanılan bir standarttır. Bir genelleme yöntemi olan bu güvenlik modelinde gelen verilere gürültü eklenir. Diğer taraftan bilgilerin kimden geldiği bilgisi gizlenerek veri güvenliği sağlanır [15-16]. Diferansiyel gizlilik için gürültü eklemenin farklı yaklaşımları; giriş pertürbasyonu, çıkış pertürbasyonu, üstel mekanizma ve objektif pertürbasyon olarak kategorize edilebilirler. Makine öğrenme modellerinde diferansiyel gizliliğin uygulanmasında öncelikle merkezi bir veri kümesi üzerinde eğitilmiş modellere odaklanmıştır [17].

Homomorfik Şifreleme: Kullanıcıların verilerinin gizliliği, makine öğrenimi sürecinde şifreleme mekanizmalarının değişimi yoluyla sağlanan bir modeldir [18]. Aynı zamanda homomorfik şifrelemen, yerel bilgisayardaki verileri sunuculara gönderirken güvenliğini sağlamak için şifrelenen verinin sunucuya gönderilmesi, işlenmesi ve şifreli olarak geri gönderilmesi sürecidir. Bu süreci en verimli kullanan Brakerski / Fan-Vercauteren (BFV) ve Cheon-Kim-Kim-Song (CKKS) şemalarıdır [19-21].

2.4. Federe Öğrenme Uygulamaları

Federe Öğrenme yöntemlerinin uygulama alanlarına bakıldığında çok kullanıcılı mobil servislerinin kullanıldığı görülmektedir. Federe öğrenme modeline göre yapılan çalışmalar aşağıdaki gibi özetlenmiştir.

Google Klavye (Gboard), 2018'de 1 milyardan fazla kurulumu olan mobil cihazlar için sanal bir klavyedir. Gboard, hem metin otomatik düzeltme, bir sonraki kelime tahmini ve kelime tamamlama gibi yazma özelliklerini hem de emoji, GIF'ler ve çıkartmalar ifade özelliklerini içerir. Öncelikle, bir kullanıcının mobil cihazına yazdıklarının çoğuna erişebilen bir klavye uygulaması olarak Gboard, kullanıcının gizliliğine saygı göstermektedir [22].

Fransız şirketi Owkin, tıp ve biyoloji araştırmaları için yapay zeka ve makine öğrenmesini kullanan bir Fransız-Amerikan ortaklığıdır. Kendi tescilli platformu olan Owkin Socrates'te, hastalıklar ve tedavi sonuçlarıyla ilgili biyobelirteçleri ve mekanizmaları keşfetmek için biyomedikal görüntüleri, genomikleri ve klinik verileri entegre etmek için makine öğrenme teknolojisini kullanmaktadır. Şirket, sağlık kurumları ile bilimsel işbirlikleri geliştirmekte ve ilaç firmalarıyla ortaklıklar kurmaktadır. Owkin, tıbbi verilerle ilgili paylaşılan sorunların üstesinden gelmek için gizlilik ve güvenliği korurken, dağıtılmış verilerden toplu zekâyı inşa etmek için sağlık hizmetlerinde Federe Öğrenmeye dayalı biyomedikal makine öğrenme modellerini geliştirilmiştir [23].

Nvidia ve King's College Londra'daki yapay zekâ araştırmacıları, beyin tümörü segmentasyonunda bir sinir ağını eğitmek için federe öğrenmeyi kullandılar. Bu teknik, hasta mahremiyetini korurken, hastaneler ve araştırmacılar arasında veri paylaşımına izin verebilmektedir. Geliştirilen model, beyin tümörü olan 285 hastanın BraTS görüntülerinden elde edilen verileri kullanmaktadır [24].

Firefox URL çubuğunu geliştirmek için Federe Öğrenmeyi kullanmıştır. Yaklaşık 360.000 kullanıcı ile yapılan çalışmada, Firefox URL çubuğu, kullanıcılar bir arama sorgusu yazdığında önerileri gösterir. Bu önerilerin bir kısmı doğrudan bir arama motoru tarafından sağlanmaktadır. Diğerleri, kullanıcının geçmişine, yer imlerine veya açık sekmelerine bağlı olarak Firefox tarafından üretilir [25].

3. SONUÇ

Bu çalışmada dağıtık uç veri kaynaklarının işbirlikçi eğitim modeli ile eğitilmesi için federe öğrenme biçimi incelenmiştir. Federe öğrenme modelinin geleneksel makine öğrenme uygulamalarına uygulanması ele alınmıştır. Federe Öğrenmenin gerçek dünyada uygulanmasında bazı zorluklar bulunur. Federe Öğrenmeye dâhil olan cihazların bağlantı sorunları, model eğitim süreleri, eksik güncellemeler,

farklı model sürümleri öğrenme sürecini olumsuz yönde etkilemektedir. Federe sistemin tam koordine edilememesi, eğitim modeli oluşturulurken iyi bir hipotezin kurulamaması ve kullanıcılardan gelen verilerin şifresiz gelmesi de kullanıcının kimliğinin açığa çıkmasına neden olabilir. Tüm bu sorunların çözümü için farklı algoritmalar ve yaklaşımlar önerilmektedir. İlerleyen çalışmalarda federe öğrenmesi uygulanmasında problemlerin aşılacağı öngörülmektedir.

KAYNAKLAR

1 . Yıldız, A., Endüstri 4.0 ve akıllı fabrikalar. Sakarya University Journal of Science, Vol. 22, Issue 2, Pages 546-556. 2018. DOI: 10.16984/saufenbilder.321957

2 . Lee, J., Bagheri, B., & Kao, H. A., A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing letters, Issue 3, Pages 18-23, 2015.

3 . Zhou, K., Liu, T., & Zhou, L., Industry 4.0: Towards future industrial opportunities and challenges. In 2015 12th International conference on fuzzy systems and knowledge discovery (FSKD) Pages 2147-2152. 2015. IEEE.

4 . Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., & Kudlur, M, Tensorflow: A system for large-scale machine learning. In 12th {USENIX} Symposium on Operating Systems Design and Implementation, Pages 265-283, 2016.

5 . Kayaalp, K., Süzen A.A., Derin Öğrenme ve Türkiyedeki Uygulamaları, Yayın Yeri: IKSAD International Publishing House, Basım sayısı:1, Sayfa sayısı:92, ISBN:978-605-7510-53-2, 2018.

6 . Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D., & Shmatikov, V., How to backdoor federated learning. arXiv preprint arXiv:1807.00459.2018.

7 . Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D., Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.2016.

8 . Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., & Ramage, D., Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604.2018.

9 . Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X., & Chen, M., In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. IEEE Network, Vol. 33 Issue 5, Pages 156-165. 2019.

10 . Yang, Q., Liu, Y., Chen, T., & Tong, Y., Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), Vol. 10, Issue 2, Pages 12, 2019.

11 . Nock, R., Hardy, S., Henecka, W., Ivey-Law, H., Patrini, G., Smith, G., & Thorne, B., Entity Resolution and Federated Learning get a Federated Resolution. arXiv preprint arXiv:1803.04035.2018.

12 . Liu, B., Wang, L., Liu, M., & Xu, C., Lifelong federated reinforcement learning: a learning architecture for navigation in cloud robotic systems. arXiv preprint arXiv:1901.06455.2019.

13 . Pettai, M., & Laud, P., Combining differential privacy and secure multiparty computation. In Proceedings of the 31st Annual Computer Security Applications Conference, Pages 421-430, 2015. ACM.

14 . Bayatbabolghani, F., & Blanton, M., Secure Multi-Party Computation. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Pages 2157-2159, ACM.2018.

15 . Choudhury, O., Gkoulalas-Divanis, A., Salonidis, T., Sylla, I., Park, Y., Hsu, G., & Das, A., Differential Privacy-enabled Federated Learning for Sensitive Health Data. arXiv preprint arXiv:1910.02578. 2019.

16 . Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L., Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 308-318). ACM.2016.

17 . Yang, Y., Zhang, Z., Miklau, G., Winslett, M., & Xiao, X., Differential privacy in data publication and analysis. In Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data, 601-606. ACM.2012.

18 . Aslett, L. J., Esperança, P. M., & Holmes, C. C., A review of homomorphic encryption and software tools for encrypted statistical machine learning. arXiv preprint arXiv:1508.06574, 2015.

19 . Brakerski, Z., Fully homomorphic encryption without modulus switching from classical GapSVP. In Advances in cryptology–crypto 2012, Pages 868–886. Springer, Berlin, Heidelberg, 2012.

20 . Fan, J., & Vercauteren, F., Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive, 2012, 144, 2012.

21 . Cheon, J. H., Kim, A., Kim, M., & Song, Y., Homomorphic encryption for arithmetic of approximate numbers. In International Conference on the Theory and Application of Cryptology and Information Security, Pages 409–437. 2017. Springer, Cham.

22 . Yang, T., Andrew, G., Eichner, H., Sun, H., Li, W., Kong, N., & Beaufays, F., Applied federated learning: Improving google keyboard query suggestions. arXiv preprint arXiv:1812.02903. 2018.

23 . İnternet : Galtier, M. N., & Marini, C., Substra: a framework for privacy-preserving, traceable and collaborative Machine Learning. arXiv preprint arXiv:1910.11567. 2019.

24 . İnternet: Johnson, K., Erişim adresi: https://venturebeat.com/2019/10/13/nvidia-uses-federated-learning-to-create-medical-imaging-ai/ Aralık, 12, 2019

25 . Federated Learning for FirefoxErişim adresi: https://florian.github.io/federated-learning-firefox/ Aralık 10, 2019