NKMJ
Namık Kemal Tıp Dergisi
Namık Kemal Medical Journal

Research Article /Araştırma Makalesi
Doi: https://doi.org/10.37696/nkmj.660762 e-ISSN: 2587-0262

A NOVEL APPROACH TO MACHINE LEARNING APPLICATION TO PROTECTION PRIVACY DATA IN HEALTHCARE: FEDERATED LEARNING

Sağlık Alanında Veri Mahremiyetinin Korunmasına Yönelik Makine Öğrenmesi Uygulamalarına Yeni Bir Yaklaşım: Federe Öğrenme

Ahmet Ali SÜZEN[1], Mehmet Ali ŞİMŞEK[2]

[1]Isparta University of Applied Sciences, Department of Computer Technologies, Isparta, TURKEY.
[2]Tekirdag Namik Kemal University, TBMYO, Department of Computer Technologies, Tekirdag, TURKEY.

Abstract

Aim: Today, data banks contain unpredictable data. Together with the advances in data science, large data offer the potential to better understand the causes of diseases. This potential results from the processing, analysis or modeling of machine learning algorithms. Various data sets stored in different institutions are not always shared directly due to privacy and legal concerns. This problem limits the full use of large data in health research. Federated learning is aimed at developing artificial intelligence systems based on both high accuracy and data privacy.

Materials and Methods: In this study, a federated learning approach was proposed in order to access any data and develop machine learning applications without sharing personal information within the scope of data privacy. Firstly, the structure of the Federated learner has been studied. It was then determined how federated learning should be used in machine learning models in different health applications.

Results: In federated learning, the model is trained on local computers and its updates are transferred to a central server. The updated model is then transferred to local models. In this way, the central model is trained without seeing the data.

Conclusion: It is necessary to make machine learning models in which confidentiality is applied with data obtained from health. For this, federated learning must be integrated into traditional machine learning applications. Thus, high performance is envisaged to be achieved with big data where data confidentiality is adopted.

Keywords: Privacy, federated learning, personal data, machine learning, healthcare.

Öz

Amaç: Günümüzde veri bankalarını tahmin edilmeyecek büyüklükte veriler içermektedir. Veri bilimindeki gelişmelerle birlikte büyük veriler hastalıklarının oluşum sebeplerini daha iyi anlama potansiyeli sunmaktadır. Bu potansiyel verilerin işlenmesi, analiz edilmesi veya makine öğrenmesi algoritmaları ile modellenmesi sonucunda ortaya çıkmaktadır. Farklı kurumlarda depolanan çeşitli veri kümeleri gizlilik ve yasal kaygılar nedeniyle her zaman doğrudan paylaşılmamaktadır. Bu sorunda sağlık araştırmalarında büyük verilerin tam olarak kullanılmasını sınırlamaktadır. Federe öğrenme hem yüksek doğruluk hem de veri mahremiyetine göre yapay zekâ sistemlerinin geliştirilmesi amaçlanmaktadır.

Materyal ve Metot: Bu çalışmada veri mahremiyeti kapsamında kişisel bilgiler paylaşılmadan, herhangi bir veriye erişmek ve makine öğrenmesi uygulamaları geliştirebilmek için federe öğrenme yöntemi önerilmiştir. Öncelikle federe öğrenmeni yapısı incelenmiştir. Daha sonra federe öğrenmesin farklı sağlık uygulamalarındaki makine öğrenmesi modellerine nasıl kullanılması gerektiği belirlenmiştir.

Bulgular: Federe öğrenmede model, yerel bilgisayarlarda eğitilerek merkezi bir sunucuya güncellemeleri aktarılmaktadır. Yerelden gelen güncellemeler merkezi modeli günceller. Daha sonra güncellenmiş model yerel modellere aktarılır. Bu sayede merkezi model veriyi görmeden eğitilmektedir.

Sonuç: Sağlıktan elde edilen veriler ile gizliliğin uygulandığı makine öğrenme modellerinin geliştirilmesi gerekir. Bunun için geleneksel makine öğrenme uygulamalarına federe öğrenmenin entegre edilmesi gereklidir. Böylece veri gizliliğin benimsendiği büyük veriler ile yüksek performans elde edilmesi öngörülmektedir.

Anahtar Kelimeler: Gizlilik, federe öğrenme, kişisel veri, makine öğrenmesi, sağlık kuruluşu.

INTRODUCTION

The technologies we use every day, such as phones, tablets, computers, or the Internet of things, contain rich data sources[1]. These devices have different sensors that can produce large amounts of data[2]. It is estimated that terabytes of data are generated daily from devices and sensors. In recent years, with the

Corresponding Author / Sorumlu Yazar:

Ahmet Ali SÜZEN
Adres: Isparta University of Applied Sciences, Department of Computer Technologies, Isparta / TURKEY.
E-posta: ahmetsuzen@isparta.edu.tr

Article History / Makale Geçmişi:

Date Received / Geliş Tarihi: 17.12.2019
Date Accepted / Kabul Tarihi: 17.02.2020

help of big data artificial intelligence (machine learning and deep learning) techniques, great breakthroughs have emerged[3]. Through artificial intelligence applications, it is provided to make inferences, decisions and discover effective insights on these data. As a result, these applied users have a positive impact on cost, service quality and growth values[4]. More data is needed to improve the performance and accuracy of the developed systems. This need may lead to situations that violate the privacy of the private data of the users. The reason for this is based on a centralized education approach in which artificial intelligence applications training and test data are accessible. In other words, artificial intelligence application cannot be utilized without obtaining data. Studies show that the applications where personal privacy is most effective is healthcare[5].

Artificial intelligence applications are developing day by day and spreading in all areas of life. The expectations of the field of medicine from artificial intelligence technology and the studies to date are artificial intelligence applications that perform clinical diagnostic procedures and can offer treatment recommendations[6-8]. Supportive vector machines[9-11], artificial neural networks[12], deep neural networks[13-14] and machine learning[15-16] methods are generally preferred for artificial intelligence applications in medicine. For the training of the model to be realized in artificial intelligence applications, data sets with high validity and reliability are needed. The success rate of the model to be developed depends on the excess and accuracy of the data in the data set used in the training of the model. In the Declaration of Ethical Thoughts Regarding Health Databases of the World Medical Association (WMA), “all recorded information regarding the physical and mental health of the individual” is defined as personal health data[17-18]. These are referred to as “medical data” in Convention 108 and the Data Protection Directive. It was also stated that medical data considered sensitive data can only be processed with the consent of the patient and the hospital or provided that they provide the necessary assurance in the domestic law of the member states[19].

In traditional artificial intelligence applications, the training of the model takes place on computers with data. In such applications, sensitive data is shared. A distributed path is required to run the learning algorithm to protect sensitive data[20]. Federated learning is the right solution to this problem. The algorithm that uses data directly in the federated learning model must be run on local computers. The resulting updates are calculated based on locally available training data and sent to a server. In this way, privacy is prioritized. Also, in the development of models with large data, transmitting updates compared to transmitting data directly is seen as an advantage in terms of costs [21].

In this study, federated learning structure is examined, and solutions are proposed for the application of this learning style to machine learning systems to be realized in the field of health where data privacy is priority.

In this study, federated learning is explained in terms of horizontal, vertical and transfer learning types. As application-oriented, modeling of federated learning with deep neural networks based on current health data are addressed. Thus, a block chain can be established between newly established research centers of big data research centers. In this way, the center can transfer the experiences of the artificial intelligence models

it developed to the local. Likewise, the data obtained from the local centers can be transferred to the center while staying local. In line with the studies, educating the distributed data from a centralized system necessitates data privacy. It is also seen that the application of the federated learning paradigm to artificial intelligence models would mean the safe processing of sensitive health data.

FEDERATED LEARNING

Federated learning is a distributed collaborative machine learning approach, where a centralized model is learned by collecting locally-trained models in data-generating clients as shown in Figure 1[22]. It was originally proposed by Google to create learning models distributed across multiple devices[23-24].

Generally, federated learning can be explained technically as follows: N data owner who wants to train a machine learning model, combining each with its own machine data {D_1, D_2, D_3, ⋯ D_N} is defined as {F_1, F_2, F_3, ⋯ F_N}. A conventional method uses D = D_1 U D_2 U D_3 ⋯ U D_N to assemble all data and train the M_{TOTAL} model, whereas a federated learning paradigm is a learning process where any F_i data owner does not show the data D_i to others with a M_{TOTAL} model cooperation in their communication. Additionally, the truth of M_{TOTAL} is shown as M_{FED}. M_{TOTAL} is a result very close to M_{FED} performance. Let's say that, formally, δ is a non-negative real number; if $|M_{FED} - M_{TOTAL}| < \delta$, it is suggested that the recommended federated learning algorithm has δ-truth loss [25].

Federated Learning offers greater privacy compared to approaches where data is collected and stored in a central location [26]. The integrated environment therefore introduces new challenges to existing privacy protection algorithms. Although there are various definitions of privacy in federated learning, it can often be divided into two as global and local privacy[27]. Global privacy requires that the model's updates in each training round are confidential from all third-party sources, except the central server. Local privacy is that model data updates are also hidden on the server [28-29].

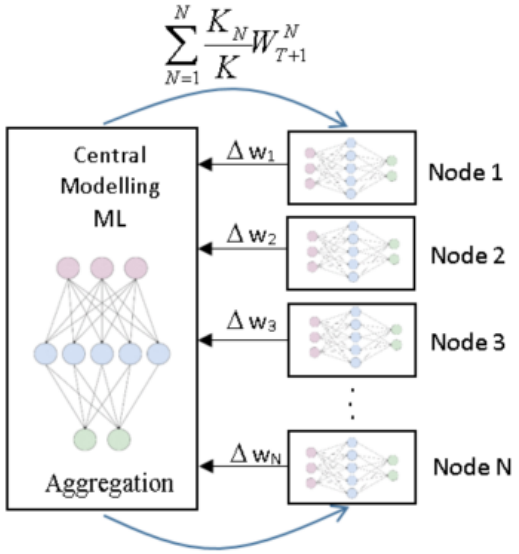

Figure 1. Structure of federated learning

Federated Learning seems to be most suitable for problems where the following situations apply [27]:

- Where task tags are derived from natural user interaction, so do not require human labeler.
- Where education data are sensitive to privacy.
- Where education data are too large to be collected centrally.

In addition, federated learning provides distributed learning through machine learning models. Federated learning is therefore distinguished form others by a few distinctive features. This explains the following challenges in federated learning:

- Too many users

- Unbalanced data point
- Different data distributions
- Communication to be slow and unstable communication

Federated Learning techniques are handled in 3 different frameworks to solve problems in different scenarios. These are respectively; Horizontal Federated Learning, Vertical Federated Learning and Federated Transfer Learning[27].

Horizontal Federated Learning

Horizontal learning is used in scenarios where the same property areas of the data sets share only the different area in the examples. The models are combined directly from edge models. For example, two regional hospitals may have very different patient groups in their region. Therefore, the intersection of patient characteristics is very small[30]. But due to the fact that the works are very similar property areas are the same. We can also explain horizontal federated learning mathematically as follows:

$$X_i = X_J, Y_i = Y_J, I_i \neq I_J, \forall D_i, D_J, i \neq j \quad (1)$$

Vertical Federated Learning

Vertical learning, also known as property-based learning, is used in scenarios where two data sets share the same instance ID field where the property fields are different. In this learning model, properties are combined to create a stronger property area for machine learning[27]. Homomorphic encryption is also used to ensure data privacy. If we go over the example given in the horizontal learning model where one is the hospital and the other is the school, the user sets are likely to include most of the users of the region. Therefore, the intersection of user areas is large. Likewise, the mathematical representation of the vertical learning model is given in Equation 2.

$$X_i \neq X_J, Y_i \neq Y_J, I_i = I_J, \forall D_i, D_J, i \neq j \quad (2)$$

Federated Transfer Learning

Federated transfer learning is used to improve performance and provide solutions when there are not many intersections in all properties or instances except for both learning styles. Federated transfer learning is an important extension of these, as it deals with problems that extend beyond the scope of other federated learning algorithms. Equation 3 is a mathematical representation of federated transfer learning [30].

$$X_i \neq X_J, Y_i \neq Y_J, I_i \neq I_J, \forall D_i, D_J, i \neq j \quad (3)$$

PRIVACY IN FEDERATED LEARNING

Considering the many attacks on machine learning methods, privacy is an important factor. Confidentiality is more important in federated learning machine learning models where data is in distributed centers. There are different aspects of data privacy for federated learning. First, it is necessary to determine what an attacker can detect by analyzing the model parameters of the data of all users participating in the optimization[31]. Given this broad availability, it appears that existing security will not be sufficient. In general, differential and k-anonymity mechanisms that ensure confidentiality are used. There are models aggregation, differential and cryptographic methods for data protection in federated learning[32].

Model Aggregation

It is a framework used to prevent communication of raw local data in federated learning. The developed general model is updated by collecting parameters from multiple locales (devices) each round. This is a typical stochastic gradient descent (SGD) learning algorithm. This framework applies to both model parameters between clients and metrics that the model exports as a result of local collection[33].

Cryptographic Methods

Cryptographic methods are widely used in machine learning algorithms that protect privacy such as homomorphic encryption and secure multiparty computation. In such methods, locally-trained updates are encrypted and sent to the server. The model on the server needs to decrypt it in order to use the received update. With such application, data privacy can be ensured[34].

Differential Privacy

Such frameworks generally add random noise to data or model parameters, providing privacy for individual data and protection against implication attacks in the model. Such systems reduce the success of the model in education due to noise in the learning process[35] (Figure 2).

Figure 2. Differential privacy process

We can explain the differential privacy by using the formula as follows. Let X be an array with hidden data and y be an array set with noisy values. The differential mechanism K differs as Ɛ-locally for all of $x_1, x_2, \ldots \in X_n$ and $y \in Y_n$ (Equation 4).

$$p[K(x) = y] <= e^{\varepsilon} p[K(x') = y] \quad (4)$$

Although said privacy mechanisms provide good privacy, it seems difficult to overcome the limitations of the approach. It may also be a good way to look for new approaches to protect the requirements of flexible privacy.

APPLICATION OF FEDERATED LEARNING IN HEALTH

Personal health data includes individual confidentiality, while scientific research data ensures confidentiality of data subjects only. When data comes from a variety of sources, they increase the difficulty of data analysts, making them obliged to comply with confidentiality regulations. The balance between medical data analysis and the protection of patient privacy has really become a difficult and urgent problem to solve. At this point, the dilemma of machine learning methods is solved by federated learning. Federated learning adapts to the broad ecosystem of machine learning models[36]. Table 1 shows the components and sub-components used in the implementation of federated learning systems[37].

Table 1. Federated learning components

FEDERATED LEARNING SYSTEMS			
Machine Learning Models	**Communication Architecture**	**Privacy Mechanism**	**Data Partitioning**
Decision Trees	Central	Differential Privacy	Horizontal
Neural Networks	Distributed	Cryptographic Methods	Vertical
Deep Neural Networks		Model Average	Hybrid

The application of federated learning to machine learning algorithms occurs in two ways. Training on device, which is the first part,

is applied as follows: In T=0 time, the device receives a trained model named W^0. With this model, the server also sends the mini-batch size (**b**), learning rate (**η**), number of trainings (**e**) and the required parameters. The model is trained on the device when data is collected in a sufficient amount. This model on the device can be shown as w^1 = model (x, y, b, e, η). Here w^1 is the new weights matrix calculated by the model. X and Y are input and destination outputs on the local device. New weights from local training are then shared with the server.

In the second part, the server collects locally produced trained weights from the devices. The update of the spherical weight matrix collected from n devices represented as W^{1n} takes place as in Equation 5.

$$g = g + \frac{\left(p^n * w^{1n}\right)}{N} \tag{5}$$

Where p^n is the number of data points used to obtain w^{1n} in device k. N is the sum of the number of data points in all devices. It considers a small portion of clients (Z) each round to update overall weights. Here nz is the number of clients and is calculated as nz = max (Z * N, 1). The server selects random nz clients and the overall weights are updated in this way. This can be considered as a mini mini-batch gradient descent. The server and local-based rough code of the federated averaging algorithm introduced by Google is as follows.

In the FedAvg algorithm given in Algorithm 1, the central parameter server in the model is started with the weight w0. Once started, the parameter communicates simultaneously with the server and local devices. As t ∈ [1, .., t], it continues as follows as a general communication sequence. Central Model w_{t-1}, is shared with a sub-set S_t randomly selected from the user pool *K* with a participation rate C. Each user k ∈ S_t performs one or more training rounds through local targets data by using mini-batch stochastic gradient descent (SGD) with a local learning rate **η.** S_t users send model updates back to w_t, k, $k \in S$ parameter servers after local training is completed. The server calculates the average model based on updates of local users based on $w_{t,k}$, $k \in S_t$ [28].

Algorithm 1. Federated averaging (FedAvg) algorithm

1	**Server executes**	1	**ClientUpdate**(*k*,*w*):
2	initialize w_0	2	β← (split P_K into batches of size β)
3	**for** each round *t=1,2,* ….. **do**	3	**for** each local epoch *i* from *1* to E **do**
4	$m \leftarrow$ max (*C.K*,1)	4	**for** batch b ∈ β do
5	$S_t \leftarrow$(random set of *m* client)	5	$w \leftarrow w - n\nabla l(w;b)$
6	**for** each $k \in S_t$ **in parallel do**	6	return *w* to server
7	$w^k_{t+1} \leftarrow$ ClientUpdate(k,w_t)		
8	$w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w^k_{t+1}$		

In Figure 1, there are 3 different concepts of health care institutions. These 3 organizations cannot share patients' cases to protect data privacy. A machine learning model involving all healthcare organizations must be within the framework of federated learning. In the sample model, let the training iteration be 500. Each organization trains the model 5 times with the data set owned by its local model. Local models develop a little more each iteration. Local error and accuracy values are calculated in the last step. The results are collected in the central model. The results collected at each iteration are also sent to all local models. The entire process is repeated 500 times and the models improve themselves a little. Federal learning protects the privacy of data sets in each healthcare facility. At the same time, a machine learning model is produced that will benefit all organizations. This shared machine learning model also generates statistics of common cases.

Federated learning is a good way to connect all health care institutions as in the model shown in Figure 3. Institutions share their experiences with each other with the guarantee of confidentiality of data. As a result, the performance of machine learning models will be significantly improved by the large medical data set formed. In these studies, federated learning systems and patient similarity learning, hospitalization prediction and mortality were estimated[38-39].

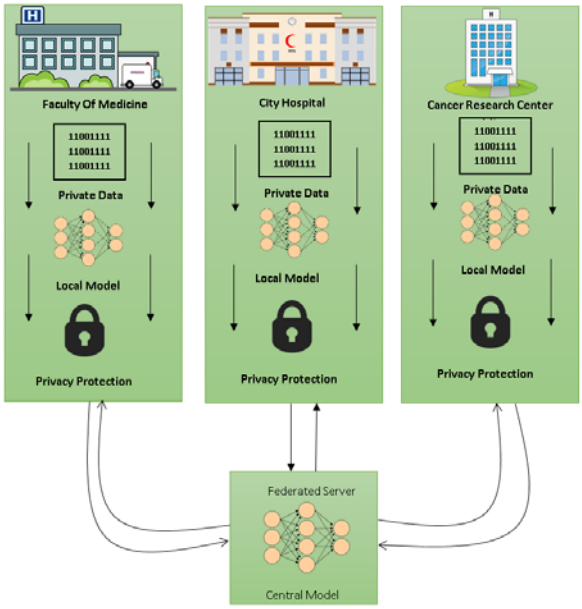

Figure 3. An example federated learning architecture for health institutions

Many companies are conducting scientific research for the application of federated learning to machine learning methods and its development. TensorFlow, one of Google's most popular deep-learning libraries in the world, includes federated learning. Likewise, PyTorch from Facebook has started to adopt a federated learning approach for privacy protection. When the studies are examined, the tools used for federated learning are listed as follows:[37].

- PySyft: Developed to protect the privacy of deep learning [40]. Model training is performed using federated learning, differential secrecy, and multilateral computing. PySyft is a python library.
- TensorFlow Federated (TFF): Open source framework for machine learning. TFF has been developed to facilitate open research and experiments with Federated Learning[41]. This library has two interfaces called the Federated Learning API and the Federated Learning Core.
- Federated AI Technology Enabler (FATE): An open source project developed by Webank. This library supports secure computing with machine learning algorithms such as logistic regression in federated learning, tree-based algorithms, deep learning, and transfer learning[42].
- Tensor/IO: Machine learning library for devices (OS, Android, and React native applications)[43].
- Functional Federated Learning in Erlang (ffl-erl): Open source application for federated learning in Erlang[44].

CONCLUSION

The processing logic of federated learning can be summarized as follows. A subset of the current client that downloads the current model is selected. Client in subset is trained with local data and calculates updated model. Model updates are sent from the requested client to the server. In the final step, the server aggregates the updates according to the average to create an improved model. Privacy mechanisms are used to transfer updates and parameters in federated learning.

One of the advantages of federated learning is minimizing central data collection. In fact, this is a distributed optimization problem. Therefore, federated learning is an area of ongoing research. The application of federated learning has some challenges under discussion. These

challenges are grouped into communication, heterogeneity, and privacy. Communication in federated learning can cause a slowdown in local computations that networks created by a large number of devices. Likewise, devices can constitute a heterogeneous structure that has differences in storage, communication capabilities (4G, 5G, WIFI, LAN) and power variability. Finally, there are privacy problems in updating weights trained on local devices and protecting local data.

The most important point in federated practices is not to store the personal information of the patients, but to store the learning information of the model that learns their diseases on the servers. With the spread of such practices, learning and medical service will be separated from each other. As a result, artificial intelligence applications based on federated learning paradigm will contribute to increase patient quality of life, decrease morbidity, and perhaps eliminate early mortality.

References

1. Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464-467). IEEE.
2. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.
3. Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the Internet of Things with edge computing. IEEE Network, 32(1), 96-101.
4. Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.
5. Shakeel, P. M., Baskar, S., Dhulipala, V. S., Mishra, S., & Jaber, M. M. (2018). Maintaining security and privacy in health care system using learning based deep-Q-networks. Journal of medical systems, 42(10), 186.
6. Demirhan A., Kılıç Y. A., Güler İ. Tıpta Yapay Zekâ Uygulamaları. Yoğun Bakım Dergisi 2010;9(1):31-41.
7. Lisboa P.J.G. A Review Of Evidence Of Health Benefit From Artificial Neural Networks İn Medical İntervention. Neural Networks 15, p 11-39, 2002.
8. Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. Nature Medicine, 25(1), 44–56. doi:10.1038/s41591-018-0300-7
9. Hashem, E. M., & Mabrouk, M. S. (2014). A study of support vector machine algorithm for liver disease diagnosis. American Journal of Intelligent Systems, 4(1), 9-14.
10. Ulagamuthalvi, V., & Sridharan, D. (2012, March). Automatic identification of ultrasound liver cancer tumor using support vector machine. In International Conference on Emerging Trends in Computer and Electronics Engineering (pp. 41-43).
11. Xian, G. M. (2010). An identification method of malignant and benign liver tumors from ultrasonography based on GLCM texture features and fuzzy SVM. Expert Systems with Applications, 37(10), 6737-6741.
12. Chu, F., Xie, W., & Wang, L. (2004, June). Gene selection and cancer classification using a fuzzy neural network. In IEEE Annual Meeting of the Fuzzy Information, 2004. Processing NAFIPS'04. (Vol. 2, pp. 555-559). IEEE.
13. Li, W., Jia, F., & Hu, Q. (2015). Automatic segmentation of liver tumor in CT images with deep convolutional neural networks. Journal of Computer and Communications, 3(11), 146.
14. Chaudhary, K., Poirion, O. B., Lu, L., & Garmire, L. X. (2018). Deep learning–based multi-omics integration robustly predicts survival in liver cancer. Clinical Cancer Research, 24(6), 1248-1259.
15. Ye, Q. H., Qin, L. X., Forgues, M., He, P., Kim, J. W., Peng, A. C., ... & Ma, Z. C. (2003). Predicting hepatitis B virus–positive metastatic hepatocellular carcinomas using gene expression profiling and supervised machine learning. Nature medicine, 9(4), 416.
16. Li, Y., Hara, S., & Shimura, K. (2006, August). A machine learning approach for locating boundaries of liver tumors in ct images. In 18th International Conference on Pattern Recognition (ICPR'06) (Vol. 1, pp. 400-403). IEEE.
17. Sağlıkla İlgili Uluslararası Belgeler, TTB Yayınları, 2. Baskı, 2009, s:177
18. İzgi, M. C. (2014). Mahremiyet kavramı bağlamında kişisel sağlık verileri The concept of privacy in the context of personal health data. Türkiye Biyoetik Dergisi, (s 1), 1.
19. Dülger, M. V. (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 1(2), 43-80.
20. Hartmann, F., Suh, S., Komarzewski, A., Smith, T. D., & Segall, I. (2019). Federated Learning for Ranking Browser History Suggestions. arXiv preprint arXiv:1911.11807.
21. Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.
22. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 12.
23. H. Brendan McMahan, Eider Moore, Daniel Ramage, and Blaise Agüera y Arcas. (2016). Federated learning of deep networks using model averaging. CoRR abs/1602.05629 (2016). arxiv:1602.05629 http://arxiv.org/abs/1602.05629.
24. Gang Liang and Sudarshan S. Chawathe. (2004). Privacy-preserving inter-database operations. In International Conference on Intelligence and Security Informatics. Springer, 66–82.
25. Arivazhagan, M. G., Aggarwal, V., Singh, A. K., & Choudhary, S. (2019). Federated Learning with Personalization Layers. arXiv preprint arXiv:1912.00818.
26. Niknam, S., Dhillon, H. S., & Reed, J. H. (2019). Federated learning for wireless communications: Motivation, opportunities and challenges. arXiv preprint arXiv:1908.06847.
27. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 12.
28. Leroy, D., Coucke, A., Lavril, T., Gisselbrecht, T., & Dureau, J. (2019, May). Federated learning for keyword spotting. In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 6341-6345). IEEE.

29. Nilsson, A., Smith, S., Ulm, G., Gustavsson, E., & Jirstrand, M. (2018, December). A performance evaluation of federated learning algorithms. In Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning (pp. 1-8). ACM.
30. Qian, Y., Hu, L., Chen, J., Guan, X., Hassan, M. M., & Alelaiwi, A. (2019). Privacy-aware service placement for mobile edge computing via federated learning. Information Sciences, 505, 562-570.
31. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2019). Federated learning: Challenges, methods, and future directions. arXiv preprint arXiv:1908.07873.
32. Nishio, T. and R. Yonetani, "Client Selection for Federated Learning with Heterogeneous Resources in Mobile Edge," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7. doi: 10.1109/ICC.2019.8761315
33. Dwork, C. and A. Roth. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9:211–407, 2014.
34. Li, Q., Wen, Z., & He, B. (2019). Federated learning systems: Vision, hype and reality for data privacy and protection. arXiv preprint arXiv:1907.09693.
35. McMahan, H. B., Moore, E., Ramage, D., & y Arcas, B. A. (2016). Federated learning of deep networks using model averaging.
36. Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., & Zhou, Y. (2019, November). A hybrid approach to privacy-preserving federated learning. In Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security (pp. 1-11). ACM.
37. Xu, J., & Wang, F. (2019). Federated Learning for Healthcare Informatics. arXiv preprint arXiv:1911.06270.
38. Li Huang and Dianbo Liu. Patient clustering improves efficiency of federated machine learning to predict mortality and hospital stay time using distributed electronic medical records. arXiv preprint arXiv:1903.09296, 2019
39. Yejin Kim, Jimeng Sun, Hwanjo Yu, and Xiaoqian Jiang. Federated tensor factorization for computational phenotyping. In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 887–895. ACM, 2017.
40. Theo Ryffel, Andrew Trask, Morten Dahl, Bobby Wagner, Jason Mancuso, Daniel Rueckert, and Jonathan Passerat-Palmbach, (2018). A generic framework for privacy preserving deep learning. arXiv preprint arXiv:1811.04017.
41. Google, (2019). Tensorflow federated. https://www.tensorflow.org/federated
42. Webank's AI, (2019). Federated ai technology enabler. https://www.fedai.org/cn/
43. doc.ai. Declarative, on-device machine learning for ios, android, and react native. https://github.com/doc-ai/tensorio, 2019.
44. Gregor Ulm, Emil Gustavsson, and Mats Jirstrand. Functional federated learning in erlang (ffl-erl). In International Workshop on Functional and Constraint Logic Programming, pages 162–178. Springer, 2018.