

# Federated Learning

Makine öğrenme modellerini eğitme şeklimiz son yıllarda çok yol kat etti.

Geleneksel bir yaklaşım, tüm verileri merkezi bir sunucuda toplamak ve modeli eğitmek için kullanmaktı. Ancak bu yöntem, kolay olsa da, veri gizliliği ile ilgili endişeleri artırdı ve çok değerli ancak hassas verilere erişilemedi.

Bu sorunu ele almak için AI modelleri merkezi olmayan bir yaklaşıma geçmeye başladı ve "federe öğrenme" adı verilen yeni bir kavram ortaya çıktı. 1

## Federated Learning nedir?

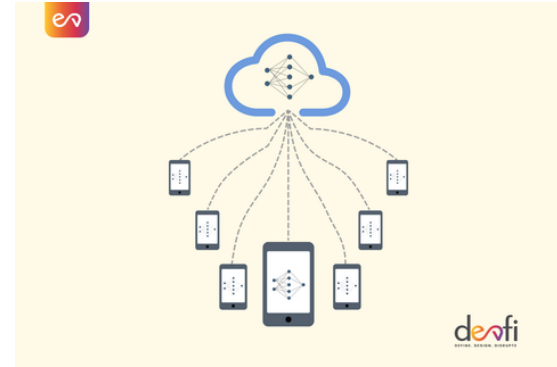
Federated Learning (işbirlikçi öğrenme) merkezi olmayan bir yaklaşımla eğitim yapan bir makine öğrenimi modelleri. Uç cihazlardan global sunuculara veri alışverişi gerektirmez. Bunun yerine, kenar cihazlarındaki ham veriler, modeli yerel olarak eğitmek ve veri gizliliğini artırmak için kullanılır. Nihai model, yerel güncellemeler toplanarak ortak bir şekilde oluşturulur

## Federated Learning Avantajları ?

**Gizlilik:** Verilerin eğitim için merkezi bir sunucuya gönderildiği geleneksel yöntemlerin aksine, federe öğrenme, eğitimin kenar cihazında yerel olarak gerçekleşmesine izin vererek potansiyel veri ihlallerini önler.(Görsel 0.1)

**Veri güvenliği:** Veri güvenliğini sağlamak için yalnızca şifreli model güncellemeleri merkezi sunucuyla paylaşılır. Ayrıca, Güvenli Toplama İlkesi gibi güvenli toplama teknikleri, yalnızca toplu sonuçların şifresini çözmeyi sağlar.

**Heterojen verilere erişim:** Birleşik öğrenme, birden fazla cihaza, yere ve kuruluşa yayılmış verilere erişimi garanti eder. Güvenlik ve gizliliği korurken finansal veya sağlık verileri gibi hassas veriler üzerinde modellerin eğitilmesini mümkün kılar. Daha fazla veri çeşitliliği sayesinde modeller daha genelleştirilebilir hale getirilebilir. 1



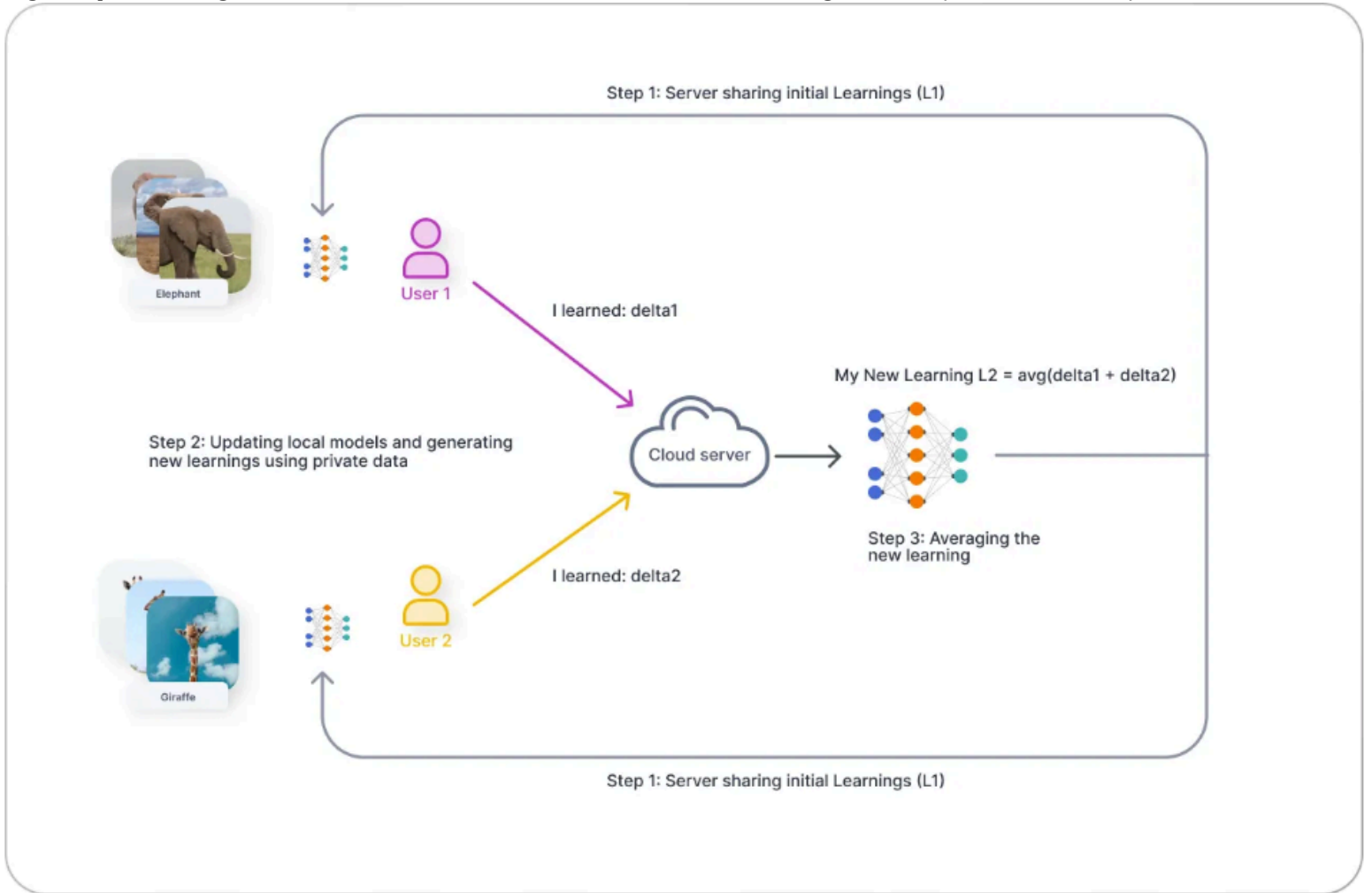
(Görsel 0.1)

## Federal öğrenme nasıl çalışır?

Genel bir temel model merkezi sunucuda saklanır. Bu modelin kopyaları istemci cihazlarla paylaşılır ve daha sonra modelleri ürettikleri yerel verilere göre eğitir. Zamanla, tek tek cihazlardaki modeller kişiselleştirilir ve daha iyi bir kullanıcı deneyimi sağlar.

Bir sonraki aşamada, yerel olarak eğitilmiş modellerden gelen güncellemeler (model parametreleri), güvenli toplama teknikleri kullanılarak merkezi sunucuda bulunan ana modelle paylaşılır. Bu model, yeni öğrenmeler oluşturmak için farklı girdileri birleştirir ve ortalamaları alır. Veriler çeşitli kaynaklardan toplandığından, modelin genelleştirilebilir hale gelmesi için daha geniş bir alan vardır.

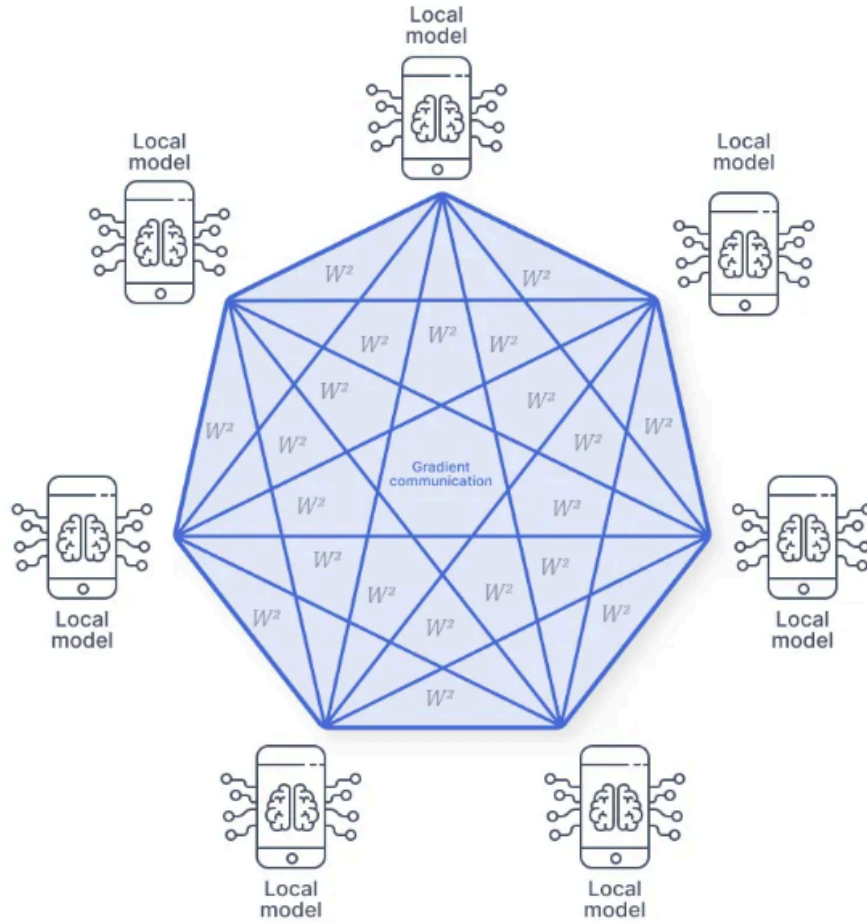
Merkezi model yeni parametreler üzerinde yeniden eğitildikten sonra, bir sonraki yineleme için istemci cihazlarla tekrar paylaşılır. Her döngüde, modeller çeşitli miktarda bilgi toplar ve gizlilik ihlalleri oluşturmadan daha da gelişir. ( Görsel 0.2 ) 1



## Merkezi olmayan Federated Learning

Merkezi olmayan federal öğrenme, öğrenmeyi koordine etmek için merkezi bir sunucu gerektirmez. Bunun yerine, model güncellemeleri yalnızca birbirine bağlı kenar cihazları arasında paylaşılır. Nihai model, bağlı kenar cihazlarının yerel güncellemelerini toplayarak bir kenar cihazında elde edilir.

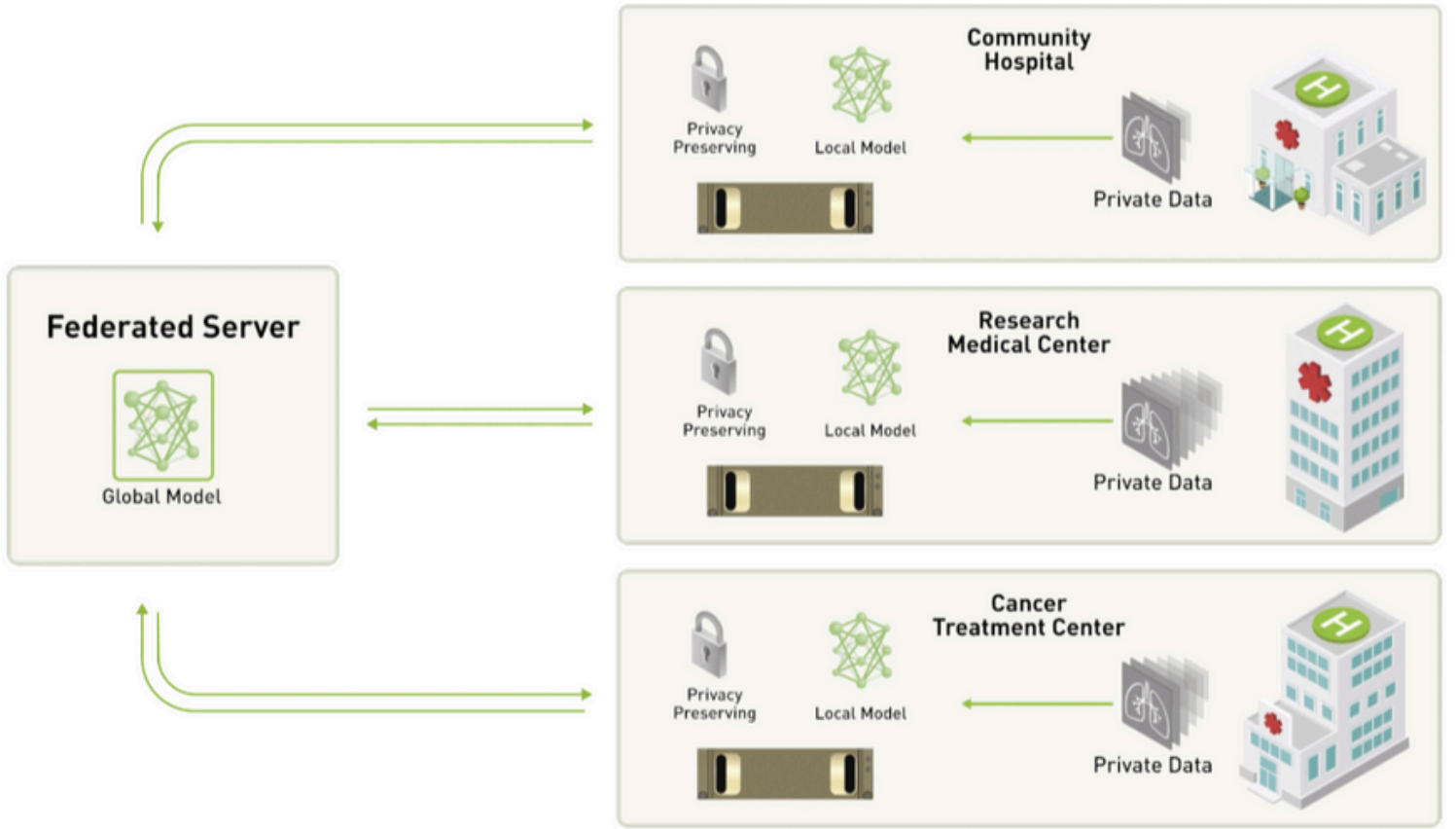
Bu yaklaşım, tek noktalı bir arıza olasılığını önler; ancak, modelin doğruluğu tamamen kenar cihazlarının ağ topolojisine bağlıdır.(Görsel 0.3) 1



## Heterojen federe öğrenme

Heterojen federe öğrenme, cep telefonları, bilgisayarlar veya IoT (Nesnelerin İnterneti) cihazları gibi heterojen istemcilere sahip olmayı içerir. Bu cihazlar donanım, yazılım, hesaplama özellikleri ve veri türleri açısından farklılık gösterebilir.

HeteroFL, yerel modellerin ' niteliklerinin ana modelinkine benzediğini varsayan ortak Federe Öğrenme stratejilerine yanıt olarak geliştirilmiştir. Ancak gerçek dünyada, çok nadiren olur. HeteroFL, çok çeşitli yerel modeller üzerinde eğitim aldıktan sonra çıkarım için tek bir küresel model oluşturabilir. 1



## Kaynakça

1. <https://www.v7labs.com/blog/federated-learning>
2. : <https://towardsdatascience.com/how-federated-learning-is-going-to-revolutionize-ai-6e0ab580420>
3. [https://www.researchgate.net/figure/Decentralized-Federated-Learning-Environments\\_fig1\\_34438657](https://www.researchgate.net/figure/Decentralized-Federated-Learning-Environments_fig1_34438657)