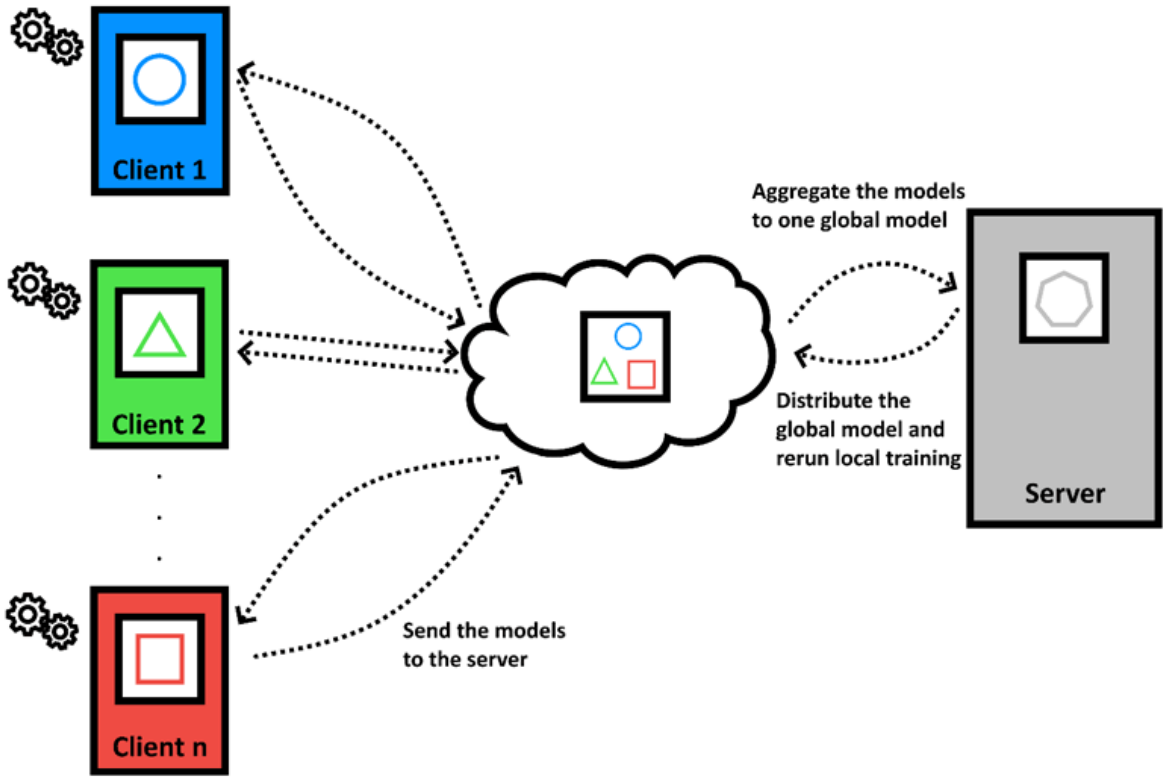
FEDERATED LEARNING ÇALIŞMA MANTIĞI



Federated Learning çalışma mantığı basitçe ;

- Her bir client, serverdaki giriş modelini serverdan alır.

- Her bir client, kendi lokallerindeki veri setleri ile lokal modellerini eğitir.

- Eğitilmiş lokal modellerinin parametrelerini server'a gönderirler.

- Server'da toplanan model parametreleri birleştirilir ve bir modele indirgenir. Buna global model denir.

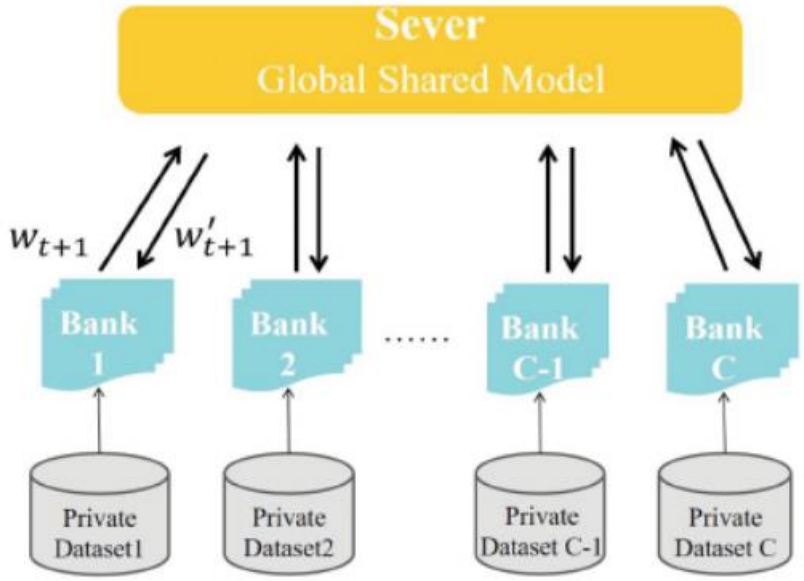
- Global model tekrar clientların lokallerine gönderilir.

- Süreç beklenen başarım noktasına gelene kadar devam eder.

Federated Learning'te ortak sunucu olması şart değildir. Clientlar ortak sunucu kullanmadan kendi aralarında model ağırlıklarını paylaşarak da iş birlikçi model geliştirebilirler.

[1] FFD: A Federated Learning Based Method for Credit Card Fraud Detection

Çalışmada *Federated fraud detection* adını verdikleri framework farklı bankaların ortak bir modeli işbirliği içinde öğrenmesine ve aynı zamanda çarpık tüm eğitim verilerini kendi özel veritabanlarında tutmasına olanak tanıyor.



Kredi kartı dolandırıcılığının tespitine yönelik geleneksel makine öğrenimi modelleri, genellikle bireysel bankalar tarafından kendi özel veri kümeleriyle eğitilir. Geleneksel makine öğreniminden farklı olarak, birleştirilmiş öğrenme, paylaşılan bir modelin işbirlikçi bir şekilde öğrenilmesine olanak sağlar.

1) Katılımcı bankalar makinelerine sunucuda bulunan ortak(global) modeli merkezi sunucudan indirir.

2) Her bir banka lokaldeki verilerini sunucudan gelen model ile eğitir. Böylece her bir bankanın lokal modelleri oluşmuş olur.

3) Bankalar oluşan lokal modelleri tekrardan sunucuya şifreli iletişim kullanarak gönderir.

4) Sunucuda biriken "C" sayıda model bir optimizasyon stratejisi ile sunucuda birleştirilir ve tek bir model elde edilmiş olur.

5) Süreç yakınsayana kadar tekrarlanır.

Federated Learning, her bir bankanın dolandırıcılık ve yasal işlemlere ilişkin daha iyi kalıpları öğrenmesine yardımcı olmakla kalmıyor, aynı zamanda veri kümelerinin gizliliğini ve güvenliğini de koruyor.

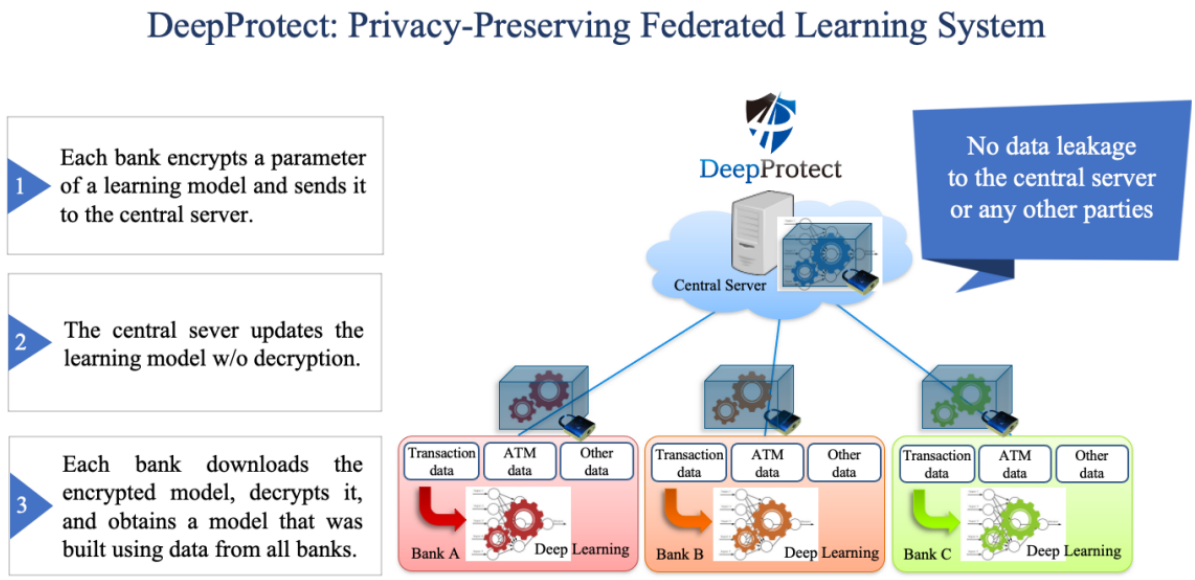
Federated Learning yapısında her banka lokal modellerini istediği eğitim sayısı ile veya istediği değişkenler ile eğitebilir.

[2] Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks

Çalışmada Japonya'daki 5 banka (Chiba Bank, Ltd., MUFG Bank, Ltd., Chugoku Bank, Ltd., Sumitomo Mitsui Trust Bank, Ltd., ve Iyo Bank, Ltd.) bir araya gelerek federated learning yapısını oluşturmaktadır. Yapılan deneylerde, iki tür mali dolandırıcılığı tespit etmek için makine öğrenimi modelleri geliştirilmiştir.

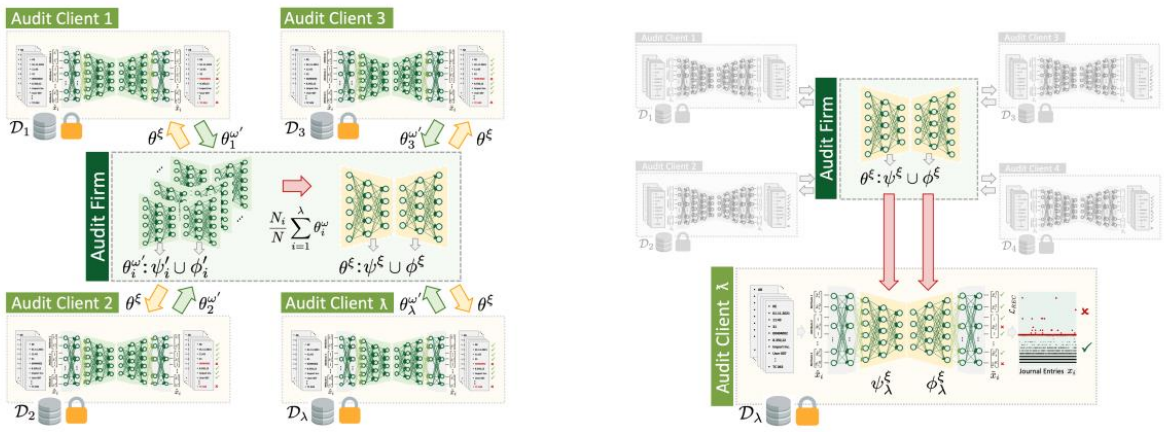
- Müşterilerin/mağdurların hesaplarındaki hileli işlemleri tespit etmek
- Suçluların banka hesaplarını tespit etmek.

Çalışma sonuçları Federated Learning sisteminin, tek bir bankanın veri seti kullanılarak oluşturulan model tarafından tespit edilemeyen dolandırıcılıkları tespit ettiğini gösteriyor.



Şekilde'de görüldüğü üzere veriler her bankanın kendi sistemindedir ve sadece modeller sunucuya gönderilmektedir. Çalışmada ek güvenlik önlemi olarak model parametreleri sunucuya gönderilirken homomorfik şifreleme uygulanmıştır.

[3] Federated and Privacy-Preserving Learning of Accounting Data in Financial Statement Audits



(a) Federated Training Setup **(b) Federated Inference Setup**

Yukarıdaki çalışmada clientlar muhasebe verilerindeki anormallikleri tespit etmektedir. Aynı mantık ile (a) 'da gözüktüğü gibi ilk etapta serverdan model alınmakta ardından lokalde tekrardan eğitilmektedir. Bu sürecin sonunda ise (b)'de gözüktüğü gibi herhangi bir client son geliştirilen global modeli alarak ürününde kullanabilir.

DİĞER LİTERATÜR ÇALIŞMALARI

[4] Federated learning model for credit card fraud detection with data balancing techniques

[5] Credit Card Fraud Detection Using Federated Learning Techniques

[6] Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms

[7] A Privacy-Preserving Hybrid Federated Learning Framework for Financial Crime Detection

[8] Federated Continual Learning to Detect Accounting Anomalies in Financial Auditing

[9] Federated Learning for Fraud Detection in Accounting and Auditing

Yapılan bütün çalışmalarda ana mantık aynıdır. Veri gizliliği korunarak, herhangi bir veri paylaşımı yapılmadan sadece model parametrelerinin paylaşılması ile birlikte işbirlikçi model geliştirme esasına dayanır.