Federated Learning in Finance - FedFin

Pooja Prasad and Kristian Kersting
Technishe Universitat Darmstadt

November 2021

Contents

1 Need for a change in financial sector status quo

In today's volatile market environment and with growing complexity and size of available data generated from various sources and edge devices like smartphones and IoT devices, use of cutting-edge machine learning techniques has become a necessity for any organization than ever before. The organizations should start using machine learning technologies to harness the insights and benefits out of the humongous data available to them. This is true for the financial sector as well. Data enables better products and smarter models. This will not only improve their functionality and keep them up to date with the advancement across the globe but also help in increasing their ROI by reducing frauds, laundering, customer-churn and so on.

But, applying machine learning techniques in the financial sector is not easy due to the complex and private nature of the data in this sector. All the existing machine learning based solutions are applied in bits and pieces and its full capacity is not yet harnessed. There are several challenges that we will discuss below that need to be addressed to incorporate machine learning based efficient applications that can not only surpass the traditional methods but also enable financial sectors to reach new heights that were not achieved before.

2 Issues to tackle

In order to apply any classical machine learning algorithm, data needs to be present at one central location. There are several limitations using standard machine learning algorithms in the financial sector:

1. Data Privacy- As we are dealing with confidential financial data, data protection is of utmost importance. Financial Institutions want to keep their data within their physical boundaries, due to security, regulatory, and competitive risks. So, bringing the data to a common server to run ML algorithms is not feasible.

2. Complicated Administrative Procedures -Due to the complicated administrative procedures, even data integration between different departments of the same institution faces several challenges and resistance.

3. Ever-changing data sources and data- These financial systems have different types of data collected from hundreds of different information systems and often change more rapidly than these systems can be fully documented using metadata and painstakingly preprocessed by data scientists for the ML tasks using ETL tools.

4. Data Scarcity - Due to privacy concerns, owners are not always willing to share their sensitive yet useful data

5. Getting users' lawful consent for collecting their data and using them for training a model is not an easy task

6. Expensive collection, storage, and computation - Collecting and preserving the growing data securely is time consuming and costly. Training machine learning algorithms on billions of data is computation expensive

7. Non IID nature of data - Individual data is too small and does not represent the entire data distribution. Hence, classical distributed learning cannot be applied

How to solve the problem of fragmented and isolated data lawfully and securely is a major challenge for AI researchers and practitioners today.

3 What can be the solution?

One of the probable solution can be a technique that can help us apply machine learning on the private data without the data leaving the source. The above problems can be solved through Federated Learning with privacy enabled technologies.

3.1 Federated Learning

As given in Wikipedia, Federated Learning (also known as collaborative learning) is a machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging them.

There are various other definitions of Federated Learning but the core idea remains the same as above. Federated Learning covers wide range of methods to access decentralized and private data which was previously not available for classical machine learning.

Although the prototypical idea of FL dates back decades ago, to the early work of Mangasarian and Solodov in 1994, it was only brought to the forefront of deep learning after the seminal paper by McMahan et al. [10] from Google where they coined the term Federated Learning to create shared models from their customers' computing devices (clients) in order to improve the user experience on those devices.

"We advocate an alternative that leaves the training data distributed on the mobile devices, and learns a shared model by aggregating locally-computed updates. We term this decentralized approach Federated Learning." [10]

Federated Learning (FL) collaboratively learns a shared model while keeping the data residing on each client. The goal of FL is to enable edge devices to do state of the art machine learning without centralization of data and with privacy by default.

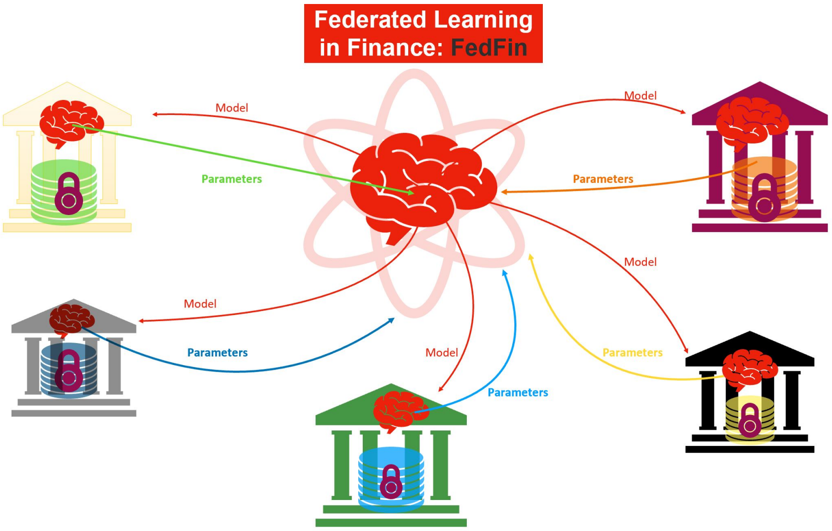


Figure 1: Federated Learning in Finance. The framework depicts a collaborative system where data has multiple shareholders such as financial institutions, governmental institutions, private institutions and public. They work together using private artificial intelligence and they all would have to collude to violate the data privacy.

3.2 Federated Learning Settings

We next discuss several different types of settings that can be used for federated learning.

- **Based on types of participating devices-** We have following 2 types:

  1. Cross-Device Federated Learning (CDFL) involves learning across user devices that have data created by a single user. Client devices can be a smart phone/ tablet/personal computer/IoT sensor. The central server coordinates with the clients in order to train the model. A data scientist creates a base ML model to begin with. The base model is stored in the cloud or server of the service provider. Each client device downloads the base model and improves it by learning from the data stored inside of them. Once the client side models are trained, only the individual model weights are sent to the coordinator server. The coordinator server has the secure aggregator that summarises the weights of the models as aggregated focused updates. Only this aggregated update is sent to the data scientist where he/she uses it to improve the initial base model. He/she tests/validates the model on new/unseen data locally available to them. If they are not happy with the performance, they will make some changes to the initial model and resend the model to the clients for retraining.Finally

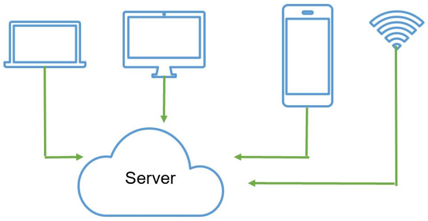


Figure 2: Cross-Device FL

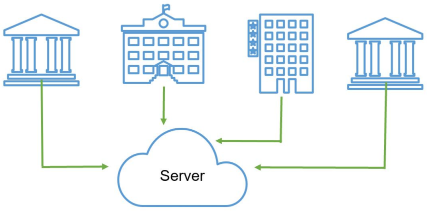


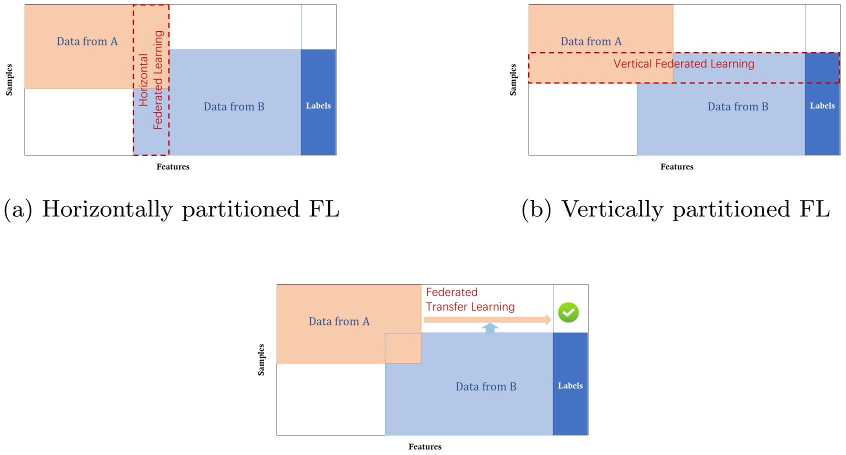
Figure 3: Cross-Silo FL

when the combined model performance is satisfactory, it is deployed at the client devices for inference on their respective data. For example, data from Bank apps installed on different users' phones that can be used to provide personalized investment recommendation is an example.(Fig. 2)

2. Cross-Silo Federated Learning (CSFL) learns across databases that contain data for many users. ML models are trained on data owned by different institutions. In Cross-silo Federated Learning the participant clients are not devices rather they are institutions like hospitals, banks, government institutions etc. We can have several institutions taking part in the training with the huge amount of data that they have. The institutions do not have to share or exchange data among each other or the central service provider. They can use Federated Learning to train and learn a combined model that's going to work well for every institute involved on their respective private data. For example, in China, the banking sector, specifically WeBank, are driving an open-source platform, capable of supporting Cross-Silo Federated Learning. Even our case that involves banks and other financial institutions is such an example.(Fig. 3)

- **Based on data partitions** - Qiang Yang et al.[14] categorized federated learning based on the distribution characteristics of the data in following 3 types:

  1. Horizontally partitioned Federated Learning (HFL): Data is distributed in different silos containing the same feature space and different samples.(Fig. 4a)
  2. Vertically partitioned Federated Learning (VFL): Data is distributed in different silos containing different feature spaces and the same samples.(Fig. 4b)
  3. Federated Transfer Learning (FTL): Data is distributed in different silos containing different feature spaces and different samples.(Fig. 4c)



(a) Horizontally partitioned FL

(b) Vertically partitioned FL

(c) Federated Transfer Learning

Figure 4: FL based on data partitions.

In [11] authors propose a HFL method using neural networks named continual horizontal federated learning (CHFL), a continual learning approach to improve the performance of HFL by taking advantage of unique features of each client. CHFL splits the network into two columns corresponding to common features and unique features, respectively. It jointly trains the first column by using common features through vanilla HFL and locally trains the second column by using unique features and leveraging the knowledge of the first one via lateral connections without interfering with the federated training of it. We conduct experiments on various real world datasets and show that CHFL greatly outperforms vanilla HFL that only uses common features and local learning that uses all features that each client has.

3.3 Advantages of Federated Learning

Federated Learning solves various problems that we face in Centralized Learning regime. Some of the advantages of using Federated Learning over classical machine learning are:

1. Data Privacy- Privacy of the sensitive data is preserved as data never leaves the owner's system.

2. Computationally less expensive - Since the training of the model is distributed among several systems/devices, the computation cost is comparatively low than standard machine learning.

3. Data Scarcity is resolved - Since data owners no longer need to share their private data, they are more comfortable to participate in the learning

4. Non IID nature of data - Individual data is too small and does not represent the entire data distribution. Hence, classical distributed learning cannot be applied.

5. All the participating clients/systems get a smarter, more updated model to be run on their local data. They are able to get their customized model trained on their local data without them having to share the data with anyone.

Disclaimer: The federated learning idea proposed by Google was to build machine learning models based on data that are distributed across multiple devices. Although, data remains in the participating devices, the final model is made available locally to the participants. Since, this model was trained by sharing weights between different parties, inverting the model to retrieve insights about the underlying training data is possible. Hence, in practice, privacy may still be compromised. Hence, there are different privacy-preserving federated learning settings discussed next.

3.4 Advanced Federated Learning Settings

There are several categories of privacy and security preserving federated learning, out of which we discuss the main three categories namely,

- **Encryption Based Federated Learning** - This setting mainly uses cryptography. Homomorphic Encryption, Secret Sharing and Secure Multi Party are some of the examples.

  1. Homomorphic Encryption - allows users to perform computations on its encrypted data without first decrypting it. These resulting computations are left in an encrypted form which, when decrypted, result in an identical output to that produced had the operations been performed on the unencrypted data. As shown in the fig on left, 2 parties encrypt their data namely X and Y and send them to the coordinator to do aggregate computation. The coordinator performs the computation on encrypted data and send them back the result which when decrypted by both parties gives the expected result. Secure Aggregation with Homomorphic Encryption protects gradients or model inversion attacks from untrusted server. The Clients own the symmetric key used for encryption and decryption. In this type of setting, there is a tradeoff between model performance and privacy protection and hence not scalable for large data owners.(Fig. 5)

  2. Secure Multi-party Computation - SMC is one of the promising privacy preserving technique that can be applied for use cases involving several institutions trying to solve a common problem. In order to

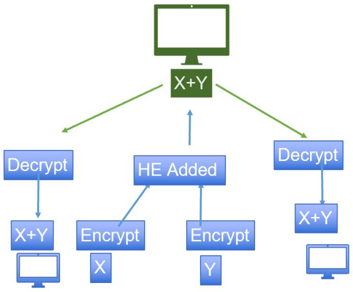


Figure 5: Process of Homomorphic Encryption

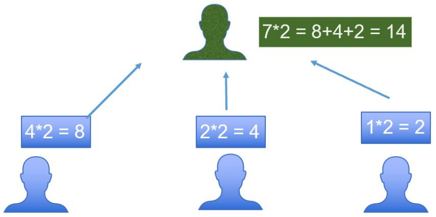


Figure 6: Secure Multi-party Computation

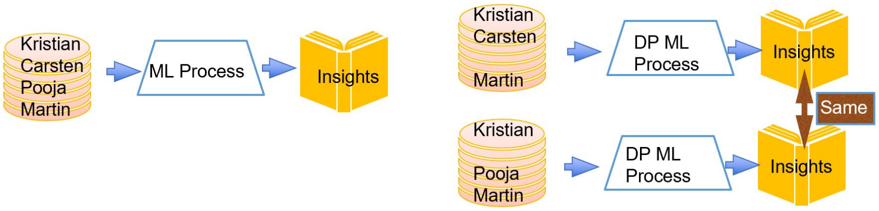


Figure 7: Differential Privacy.

explain Secure Multi Party Computation in simple way, let us say we have some data which we want to perform an operation on. In this case, let's say our data is the number 7 and the operation is multiplication by 2. How can we get a third party to complete this operation without knowledge of the data? Well, By using Secure Multi-Party Computation, Instead of dealing with data as a whole, we can split it into multiple parts, perform the operation, and combine each result back together. Traditionally, cryptography was about concealing content, while this new type of computation and protocol is about concealing partial information about data while computing with the data from many sources. These works require participants' data to be secretly-shared among non-colluding servers and correctly producing outputs. This type of setting retains the original accuracy and achieve a high privacy.(Fig. 6)

- **Perturbation Based Federated Learning** - This setting adds noise to the original data, allowing statistical information calculated from perturbed data to be statistically indistinguishable from original data. Differential privacy is one of the example.

    1. Differential Privacy - [1] proposed a technique for learning and a re-

fined analysis of privacy protection for deep neural networks at a modest cost in software complexity, training efficiency and model quality within the framework of differential privacy. To explain in simple words, suppose we have a ML process that takes some database as input, and returns some output.To make a process differentially private, typically, we add some randomness, or noise, in some places. What exactly we do, and how much noise we add, depends on which process we are modifying.Now, remove somebody from the database, and run the new process on it. If the new process is differentially private, then the two outputs are basically the same- meaning similarly distributed. This must be true no matter who we remove, and what database we had in the first place.You might ask, What does this has to do with privacy? Well, suppose someone is trying to figure out whether their target-say myself or Carsten is in the original data. By looking at the output, they can't be hundred percent certain of anything. Sure, it could have come from a database with their target in it. But it could also have come from the exact same database, without the target. Both options have a similar probability, so there's not much the attacker can say.In one word, uncertainty in the process means uncertainty for the attacker, which means better privacy.(Fig. 7)

There are several recent research using differential privacy. [7] has introduced Differentiable Privacy using Fourier transformation that can be applied on financial data.

4 Rethink the future of Financial Sector

Several use cases where state of the art privacy-preserving artificial intelligence technologies can enable new leaps in capabilities of financial services are:

1. Central AML (anti-money-laundering) Surveillance Utility - Development of "collective intelligence" to protect financial institutions against money laundering, terrorist financing and other systematic threats, particularly threats employing transactions across multiple institutions that would otherwise be difficult to detect for any one institution.

   Benefits:

   (a) Replaces current fragmented cross-institution AML solutions which are not very efficient and effective enough and lack standardization and normalization.

   (b) Increases financial inclusion as institutions and regulators become more confident in servicing customers with limited financial histories, or from more risk-prone areas

   (c) Positive impact through cost savings in managing AML and potential revenue uplift from targeting untapped markets

Challenges:

   (a) Security and regulatory environment are the major challenges that need to be addressed before a centralized solution is build to detect money laundering patterns using data across multiple financial institutions.

   (b) One of the many tasks in AML in federated setting is to build a network graph representing money laundering patterns that span across different banks using decentralized data . The easy way to do this is via a central instance that pools the data in one place and implements this. But, this is not necessarily safe from a data security standpoint. Building a network graph using data located at different locations abiding to security is an open problem.

2. Central Claims Fraud Detection Framework - Fraud is a systemic issue as malicious actors often target multiple institutions with similar methods. Developing a central fraud detection framework with collective intelligence through which all insurance claims were routed through before payments were made will allow institutions to dramatically reduce the financial loss due to fraud.

   Benefits:

   (a) Improved and efficient claims experience to customers as a central intelligent system will reduce false positives and thus reduce the processing time of claims for customers in general.

   (b) Reduced cost of handling claims for insurers as the framework more efficiently identifies the frauds and removes the need of manual fraud investigation.

   (c) Reducing fraud losses as the central system will accurately identify the frauds and blacklist the malicious actors across the entire insurance environment.

   Challenges:

   (a) Since the current process relies heavily on manual intervention and human judgement, fully automating the fraud prevention process is difficult.

   (b) IoT connectivity for insured goods (e.g. homes, vehicles etc.) is not available for financial institutions to fully utilize the high volume of customers data

3. Privacy Protected Surveillance - Face recognition system without disclosing people faces or identifiable features can be used by the financial institution to enable extra security on their already existing system. This framework can be used to identify the identity of person doing online transactions in real time.

   Benefits:

   (a) The privacy protected surveillance system can not only save financial institutions to avoid unethical transactions but can also help government avoid problems as big as threat to country's financial and payment systems from criminal exploitation or even threat to national security. One of the recent example of such incident is US unemployment fraud of around 400 billion dollar during pandemic according to the report by Axios. Over 400 billion dollars have been paid improperly and stolen due to fraudulent activities from Covid-19 unemployment and other pandemic relief programs in US. This staggering amount is almost 50 percent of unemployment monies paid out.It is one of the massive fraud incident reported in recent years.
   (b) Since the data of the users will be protected, privacy rules and regulations are applied.

   Challenges:

   (a) The current financial and governmental systems still rely on manual and paper based systems in majorities of the activities. The system will take time to reach to a level where state-of-the-art private artificial intelligence can be applied
   (b) Large number of institutions like financial, governmental, private need to collaborate to achieve the private protected survellance system

4. Federated Auto ML Solution for Financial Services - Imagine a scenario where finance specialists are given a choice to build their own state-of-the-art Machine Learning models to validate their hypothesis using Auto-ML solutions designed specifically for financial data from different banks and other financial institutions. Sber AI lab team [12] present an AutoML system called LightAutoML developed for a large European financial services company and its ecosystem satisfying the set of idiosyncratic requirements that this ecosystem has for AutoML solutions. Although, this framework was based on centralized data system, but the idea can be extended to federated decentralized data setting. One of the recent work on hyperparameter tuning in federated setting by Khodak, Mikhail, et al [6] can be extended along with Different.iable architecture search [9] for building an auto-ML solution in federated setting for financial institutions.

   Benefits:

   (a) Domain specific AutoML solution in federated settings that not only builds production-level high-quality Machine Learning models to be able to work with large and different types of data but also build large number of models to validate various hypothesis.
   (b) Give financial experts a framework to test their hypothesis without going deep in coding.

   Challenges:

    (a) Useful when an ML model should be built quickly with limited resources. When there is plenty of time to build a model using top data science talent working on complex problems requiring non- standard solutions, and careful fine-tuning of the model parameters, humans can outperform AutoML solutions.

    (b) Auto-ML in federated setting for financial environment needs to incorporate privacy preserving techniques to avoid any private data leakage.

5. Anomaly Detection - There is an increase in online financial activities during this pandemic hit era and this has also given more opportunities for financial frauds. Current methods of financial fraud detection of financial institutions are slow and inefficient. Finding the new patterns in transaction data could not only be helpful to detect any new money laundering scenarios or frauds like fraudulent credit card transactions by analyzing customer's transactions history using cross-device federated learning setting and also help to prevent them. [8] propose a fundamentally different model-based method, iForest, that explicitly isolates anomalies instead of profiles normal points and exploit sub-sampling to an extent that is not feasible in existing methods.

   Benefits:

    (a) Identifying anomaly in financial activities not only help financial institutions save a lot of money but will also help them avoid any further monetary and time loss by preventing the fraud.

    (b) Make financial system more sophisticated and secure from any financial malicious damage

   Challenges:

    (a) One of the major challenge why the centralized anomaly detection framework is not yet achieved is due to the private nature of data involved for building such a framework

6. Federated Financial Causal Discovery - Discovery of cause and effect relations among the concerned variables is one of the most fundamental problem in machine learning. If we are able to find the causal relations we can excavate the generation process behind the data and can predict for future The recent paper from Gao et al. [5] has developed a gradient-based learning framework, namely DAG-shared Federated Causal Discovery that enables to learn Directed Acyclic Graphs from decentralized data in order to infer causal relations from decentralized data. This idea can be borrowed for causal discovery in financial data.

   Benefits:

    (a) The federated approach of causal discovery in distributed setting can be applied in other domains like in distributed data ownership settings of financial ecosystem.

(b) Models that are learnt with respect to causal features can exhibit better generalization to non-iid data i.e. data from different distributions.

(c) Better privacy - inference attacks can be nullified to a greater extent with learning networks that exhibit better generalization.

Challenges:

(a) Unavailability of authentic financial data sets may restrict the researcher to infer meaningful causal discovery in finance domain.

(b) Due to private nature of the data, its not easy to get the financial data for research.

7. Deferentially Private Financial Data Generation - Can machine learning be used to generate secure, fake but realistic enough financial tabular data? The recent paper of Differentially Private Medical Data Generation using CTGANs [4], has proposed a differentially private framework for synthetic medical data generation using CTGANs. The model aimed to capture the complicated distribution of the columns and reproduce an approximate synthesized version. We can apply the proposed methods on large-scale medical financial data sets

   Benefits:

   (a) Incorporate differential privacy mechanisms into synthetic tabular data generation.

   (b) High model accuracies can be reached with proper hyperparameter tuning.

   (c) Flexible yet secure way to learn the distribution of locally stored data in federated learning framework

   Challenges:

   (a) Obtaining real financial data sets for research is expensive.

   (b) Privacy issues: identification of consumers from the corresponding financial records is feasible.

   (c) Access issues: lot of permissions needed for access the real finacial data.

8. Privacy-preserving Personalized Recommendation System - Providing a better user experience by understanding the needs of the customers on an individual level and recommending services accordingly . For example, Budget Management app (Cross-Device Federated Learning based Robo advisor) offering the benefit of highly specialized and targeted financial advice and guidance to create financial portfolios and solutions such as trading, investments, retirement plans, etc to customers especially investors with limited resources (individuals and small to medium-sized

businesses) who wish to manage their funds. In order to efficiently utilized the available clients, we can use a federated learning framework called HeteroFL[2], which supports the training of different sizes of local models in heterogeneous clients equipped with different computation and communication capabilities. As communication among the participating devices may not be stable, we can also use adaptive averaging algorithm [3] that adapts to the available hardware and communication network to maximize collaborative training throughput.

Benefits:

(a) Financial institutions will unlock stronger adoptions of machine learning frameworks in their services until the customer is safe using the technology without fear of their data being exchanged or examined by others.

Challenges:

(a) Non-availability of authentic financial data is one of the bottleneck restricting researchers to proceed with the research in this direction

9. Customer Retention and Churn Prediction - Using state-of-the-art machine learning algorithms to identify at-risk customers and design offers specifically to retain important ones is one of the important problem that every financial institution wants to solve. It includes a predictive, binary classification model to find out the customers at risk, followed by utilizing a recommendation model to determine best-suited offers that can help to retain these customers.

   Benefits:

   (a) It is a critical prediction because acquiring new clients often costs more than retaining existing ones.

   (b) Every time a client leaves, it represents a significant investment lost. Both time and effort need to be channelled into replacing them.

   Challenges:

   (a) To succeed at retaining customers who are ready to abandon the business, experts must be able to predict in advance which customers are going to churn and set up a plan of marketing actions that will have the greatest retention impact on each customer. The key here is to to be proactive and engage with these customers. While simple in theory, the realities involved with achieving this “proactive retention” goal are extremely challenging.

   (b) The churn prediction model should rely on real-time data to quantify the risk of churning and the current system is not sophisticated enough to attain the accuracy.

10. Audience Segment Targeting - Identifying targeted audiences for campaigns and advertisements based on their historical transactions can boost institutions campaign's performance by reaching targeted audiences.

    Benefits:

    (a) With selective audience target, we can expect increased Rates of Response from the customers.

    (b) This will also decrease the marketing expenditures and long-term costs.

11. Social Media Sentiment Analysis - Analyze the sentiment of the customers about any sensitive issues from their tweets, likes, shares etc. Customer Sentiment Analysis using NLP on customer social media usage, transactional behavior etc.

12. Predicting customers consumption of services from the banking system based on social-demographic data. (Santander Bank, USA is using one of these recommendation systems).

13. Predicting total and individual customers spending. (Fayrix has developed an ensemble method for Sberbank -largest transnational and universal bank of Russian federation, Central and Eastern Europe).

    There are several other use cases that can be solved using differnt federated learning settings and state-of-the-art Artificial Intelligence technologies that are not yet solved just because we don't have the data due to privacy and regulations. Federated Learning can play a vital role in pushing this data barrier.

5 Conclusion

With the implementation of the General Data Protection Rule (GDPR), financial institutions follow the regulation restricting the data flow outside their premises, resulting in a data shortage to develop networks. We need to know how we can build such framework in this new environment as researchers, and we understand the importance of data availability. When only a portion of data owners exchange personal data with web servers and the majority of the owners choose not to share these data, the output of these models suffers.

Federated learning protects user data by exchanging model changes (for example, gradient information) rather than raw data. Nonetheless, sharing model changes during the training period can expose confidential information to a third party or the central server. Some of the recent research [13] shows that federated learning is subject to privacy attack. Although recent techniques such as stable multiparty computation where data has multiple shareholders and they all would have to collude to violate the data privacy and differential privacy seek to improve the privacy of federated learning, these approaches also come at the expense of model output or machine efficiency. Understanding and balancing these trade-offs is a significant aspect in implementing private federated learning structures, both technically and empirically.

6 Acknowledgement

This work was supported by Verbundprojekt: SafeFBDC - Untersuchung der Eignung eines Financial Big Data Clusters zur Absicherung der Datensouveränität im Finanzsektor / and name Teilvorhaben: TruFinance - Trustable Secure Data Sharing ML (FKZ/Förderkennzeichen): 01MK21002K

References

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 308–318, 2016.

[2] Enmao Diao, Jie Ding, and Vahid Tarokh. Heterofl: Computation and communication efficient federated learning for heterogeneous clients. *arXiv preprint arXiv:2010.01264*, 2020.

[3] Michael Diskin, Alexey Bukhtiyarov, Max Ryabinin, Lucile Saulnier, Anton Sinitsin, Dmitry Popov, Dmitry Pyrkin, Maxim Kashirin, Alexander Borzunov, Albert Villanova del Moral, et al. Distributed deep learning in open collaborations. *Advances in Neural Information Processing Systems*, 34, 2021.

[4] Mei Ling Fang, Devendra Singh Dhami, and Kristian Kesrting. Dp-ctgan: Differentially private medical data generation using ctgans. In *International Conference on Artificial Intelligence in Medicine*, 2022.

[5] Erdun Gao, Junjia Chen, Li Shen, Tongliang Liu, Mingming Gong, and Howard Bondell. Federated causal discovery. *arXiv preprint arXiv:2112.03555*, 2021.

[6] Mikhail Khodak, Renbo Tu, Tian Li, Liam Li, Maria-Florina F Balcan, Virginia Smith, and Ameet Talwalkar. Federated hyperparameter tuning: Challenges, baselines, and connections to weight-sharing. *Advances in Neural Information Processing Systems*, 34, 2021.

[7] Antti Koskela, Joonas Jälkö, and Antti Honkela. Computing tight differential privacy guarantees using fft. In *International Conference on Artificial Intelligence and Statistics*, pages 2560–2569. PMLR, 2020.

[8] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 eighth ieee international conference on data mining*, pages 413–422. IEEE, 2008.

[9] Hanxiao Liu, Karen Simonyan, and Yiming Yang. Darts: Differentiable architecture search. *arXiv preprint arXiv:1806.09055*, 2018.

[10] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.

[11] Junki Mori, Isamu Teranishi, and Ryo Furukawa. Continual horizontal federated learning for heterogeneous data, 03 2022.

[12] Anton Vakhrushev, Alexander Ryzhkov, Maxim Savchenko, Dmitry Simakov, Rinchin Damdinov, and Alexander Tuzhilin. Lightautoml: Automl solution for a large financial services ecosystem. *arXiv preprint arXiv:2109.01528*, 2021.

[13] Aidmar Wainakh, Fabrizio Ventola, Till Müßig, Jens Keim, Carlos Garcia Cordero, Ephraim Zimmer, Tim Grube, Kristian Kersting, and Max Mühlhäuser. User label leakage from gradients in federated learning. *arXiv preprint arXiv:2105.09369*, 2021.

[14] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):1–19, 2019.