The Emergence of Commercial Federated Learning

by Franco Charette

Commerce 490a Directed Studies

August 14, 2020

For Christopher Rowell

UBC Sauder School of Business

Table of Content

1. Introduction

1.1 Concept

Federated learning is the technique of training a machine learning algorithm across multiple decentralized systems holding their own data and providing their own computation power. Federated learning aims at decentralizing data sourcing and computation work while the similarly sounding concepts of distributed learning only aims at parallelizing computation work. Federated learning reduces the security risk associated with the transportation and pooling of large datasets, allows stakeholders to collaborate without exposing sensitive data, provides a personalisation of global trends, and distributes computation and communication costs. Its most promising applications are in pharmaceutical discovery, healthcare, recommendation engines, self-driving cars, financial crime detection and insurance fraud detection.

1.2 Background

The concept of federated learning emerged in 2015 in the research article *Federated Optimization: Distributed Optimization Beyond the Datacenter*[1]. The solution proposed in this paper was a distributed version of the Stochastic Variance Reduced Gradient(SVRG) algorithm, which reduced the number of times the machine learning model from each data sources required to be compared, hence reducing the intensity of data transfer from the datasets to the central node. This approach introduced a novel trade-off between communication cost and computation cost at the location of the data. The term federated learning was coined in a follow-up 2016 research article Federated *Optimization: Distributed Machine Learning for On-Device Intelligence*[2]. The authors proposed and tested a setting “in which users do not send the data they generate to companies at all, but rather provide part of their computational power to be used to solve optimization problems.”[2]

1.3 Legal operating environment

Artificial intelligence regulations affect the field of federated learning indirectly through machine learning, but data privacy regulations have the largest influence.

Regulation of artificial intelligence is still in its infancy, with the exception of autonomous vehicles and facial recognition[3]. In Europe, “Many countries have recently issued their national plans, guidelines, or codes—which often highlight essential principles for developing ethical AI—without having passed much substantive law(i.e. European Parliament’s resolution on Civil Law Rules on Robotics, European Union’s Ethics Guidelines for Trustworthy AI and OECD’s Council Recommendation on Artificial Intelligence). The United-States’ approach also indicates that federal governance of AI will be standards-driven without substantive laws. Most AI bills and executive orders are attempting to correct algorithmic discrimination. Canada also does not have specific laws governing artificial intelligence.

Data privacy in the E.U. is governed by the General Data Protection Regulation(GDPR) as of 25 May 2018. The GDPR primarily aims at giving control to individuals over their personal data and at unifying the regulation within the EU. The GDPR also addresses the transfer of personal data outside the European Economic Area[4].

Data privacy in the United-States is governed by a collection of hundreds of laws enacted at the federal, state and municipal levels to protect the personal data of U.S. residents. Although there is no single governing data protection legislation, the Federal Trade Commission and the Office for Civil Rights are important agencies in enforcing federal U.S. privacy policy. They process large size complaints related to identity theft, online privacy and financial matters among many others.

Data privacy in Canada is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA) in the case of personal information held by private sector organizations that are not federally-regulated. Unless the personal information crosses provincial or national borders, PIPEDA does not apply to organizations operating entirely within Alberta, British Columbia and Quebec, which have their own private-sector laws deemed substantially similar. Not-for-profits such as political parties, associations, municipalities, universities, schools, and hospitals are generally covered by their own provincial privacy laws. Exception to this rule is when a not-for-profit engage organization is engaged in a commercial activity which is outside of its core activity such as a university selling an alumni list[5].

2. Use cases

For the purpose of this report, use cases are categorised by the extent of their implementation. Use cases deployed in industry received the investment necessary to be programmed and assessed, while use cases discussed in research are purely theoretical. The former are more informative on the current state of the technology since they have gone through a business cycle while the theoretical use cases are legitimate research projects pointing to future implementations. Speculative use cases without associated deployment or research were omitted.

2.1 Use cases deployed in industry

Melloddy is a consortium between 10 pharmaceutical companies aiming at using federated machine learning to accelerate drug discovery[6]. It was founded in June 2019 with $18 million in funding jointly from the European Union and The European Federation of Pharmaceutical Industries and Associations (EFPIA).

Owkin is a new venture founded in 2016 to help cancer research centers and pharmaceutical companies in developing better drugs for patients via their Owkin Studio platform. It has raised over $30M, hires over 100 computer/data scientists and serves clients in Europe and North-America[7].

WeBank anti-money laundering project is a partnership between several Chinese banks. Positive cases of money laundering account for much less than 1% of all transactions, which is an insufficient amount of data for machine learning algorithms to be trained. The multi-bank cooperation was leveraged to provide a more extensive set of positive cases[8].

Google Gboard is the first known use of federated learning. It “enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device”[9].

Snips was a voice assistants platform(similar to Google Assistant or Amazon Echo) founded in 2013 in Paris and consisted of over 50 machine/federated learning experts. I was acquired by Sonos (Nasdaq: SONO) for $37.5 million in November 2019[10].

2.2 Use cases discussed in research, but not implemented

Financial lending: increasing white listing behaviors between financial institutions improves completeness of information, leading to better risk accuracy, premiums and profits[11].

Insurance fraud detection: implementing multi-party computation between insurance providers would reduce double claiming frauds[12].

Smart Retail: increasing vertical connection of customer data silos of different levels of privacy would improve completeness of information leading to better targeting. For example, gathering purchasing power information(held by credit card companies), personal preference(held by social media companies) and other metrics(held by other apps) would improve recommendation engines[13].

Community cooperation: utilising mass user data kept private due to privacy concerns could allow new mass collaborations. For example, the utilisation of data from the taxi driver community in New-York to provide everyone better insights on supply and demand[14].

Self-driving cars: Machine learning can be separated in three basic paradigms: supervised learning(labels), unsupervised learning(no labels) and reinforcement learning(reward system). Reinforcement learning is a promising field where multiple isolated agents can share their local learning to improve the global learning[15].

3. Use cases analysis

To better understand the use cases from section 2, we analyse some driving forces motivating the implementation of federated learning, some common structural models and some factors influencing attractiveness. We will end with a brief summary of the benefit provided by federated learning.

3.1 Driving forces

Federated learning use cases are driven by the need for data privacy and by the new opportunities enabled by improving hardware capabilities. Those drivers are aligning with changes in laws, customer awareness, the internet of things(IOT) and the pursuit of cost reduction. The effect triggered by the factor alignments create an attractive environment for the federated learning concept.

Driver	Factors	Effects	Role of Federated Learning
Privacy	Legal changes	- Stronger regulation leads to privacy becoming essential - Changing regulation leads to companies seeking to lower risk	Allow cross-silo data collaborations
	Customer awareness	- Favorable reputation of federated learning leads to its use for strategic product differentiation	Federated learning as a product feature
Hardware	Enabling technologies progression	- Lower hardware cost leads to more data collected - Higher computing power leads to more local analysis - Algorithm efficiency leads to less power consumption - Faster communication leads to real time applications	Compute data where collected to shift the focus from extracting data to extracting insights
	Cost reduction	- Drive to cost saving leads to pushing computation cost to the data owner.	Computing at the edge to reduce servers expenses

Privacy driven federated learning projects arise from using valuable and sensitive data that had previously been siloed due to privacy concerns. The privacy concerns may relate to competitive data privacy, where competition pressures organisations to collaborate on data. The privacy concerns may relate to stronger privacy laws and higher perceived value of data. The maturation of machine learning and network security technologies are enabling concepts such as federated learning, multi-party computation, differential privacy and intersection sets. For the first time, these technologies allow access to data without the violation of privacy laws such as the GDPR, Health Insurance Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA). Uncertainty surrounding privacy laws around the globe, latest policies and proposed laws point to the maintaining or strengthening of current privacy laws, making the privacy driver likely to persist.

At the industry specific level, the field of healthcare is a main adopter of the technology. The pharmaceutical industry is wrapping up a decade of decline on return on investment from research and development, led by an 67% increase average cost of bringing an asset to market and 53% decline in forecast peak sales. This trend is driven by increased constraints, increased competition and increased downward pressure on healthcare budgets. By 2018, projected internal rate of return declined to its lowest level of 1.9%, pushing companies to transform digitally and adopt new research processes[16].

Hardware driven federated learning projects arise from leveraging cheaper and more powerful microchips to process lean machine learning algorithms on-device, then sending light weight

insights. This is a contrast with the current widespread approach of collecting data on-device, sending data to a server, conducting computation and returning the result to the device. It is worth noting that value is not contained in data, but in the insights enabled by data. Hence, companies stand to obtain the same value from insights while shifting the collection, communication and computation cost away from their operations.

This trend can already be seen in IOT. The Seattle start-up Xnor built a cracker size microchip-camera combination that processes its own machine vision algorithms using its own solar power without server communication at a cost of $10 per unit. This example is significant because it foreshadows use cases that were impossible in the past due to expensive setup of hardware, communication and server rental. Apple acquired Xnor for $200 million in January 2020[17]. As the number and computation power of devices increases, the decentralisation of artificial intelligence computing allowed by federated learning is the next logical step.

3.2 Leading models

The use cases of federated learning can be categorized in three leading models, each featuring sub-variations.

3.2.1 Model type 1

The model illustrated in figure one was the original federated learning concept proposed by google in the 2016 research article titled *Federated Optimization: Distributed Machine Learning for On-Device Intelligence.* The central server coordinates a large number of public nodes which collaborate without knowing each other. This central node has access to a large amount of data distributed across a large amount of edge nodes. This commanding power over such a large network may be enabled by providing a popular service in exchange of data access. In the consumer space, it lends itself well to providing useful mobile/desktop application download in exchange of data access. The element differentiating the federated learning approach is that the data remains with the client and is not transferred to a central dataset. The best known use of this approach is the google Gboard, where the user agrees to participate in data federation with others to better the global and local text prediction. As cheaper, efficient and powerful IOT devices begin computing their own AI insights, this federated learning model is also a natural fit for the consumer, commercial and industrial IOT space. Emerging cases using this model in combination with IOT devices are Sonos voice assistants, home assistants and security surveillance systems.

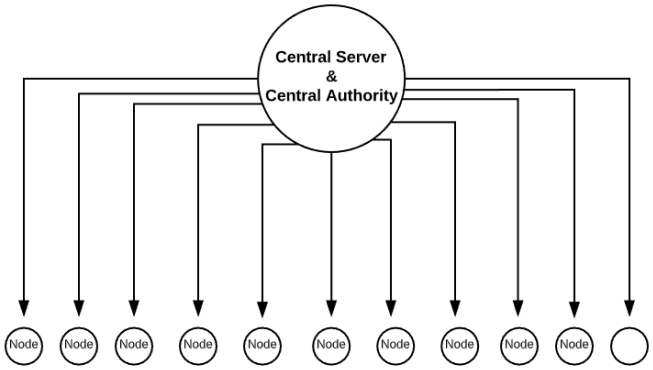

Figure 1

One sub-variation of this model can be seen in figure two, where groups of edge nodes form clusters of shared attributes. For example, clustering can be done using geographical location for saving server communication cost or obtaining a regional model.

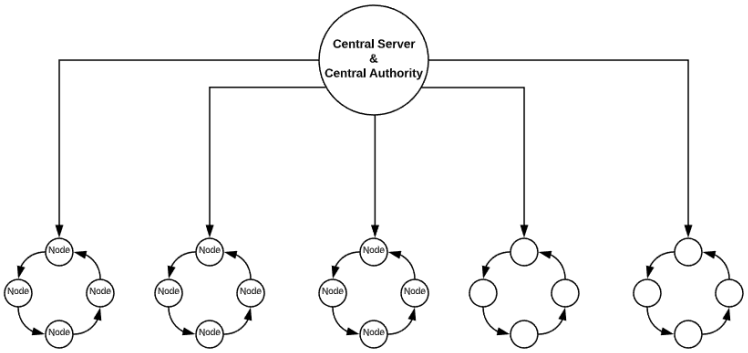

Figure 2

3.2.2 Model type 2

The model illustrated in figure three can be described as a private network collaborating over a common goal using a central server. The central server coordinates a relatively small number of private nodes that actively collaborate by trusting each other moderately. This requires several organizations, each owning a large amount of data, to collaborate in the pursuit of a common interest. Although the granular data remains private, the insights are shared among the participants, requiring business trust between parties, sometimes despite being competitors. This model lends itself well in situations where the “tide lifts all ships”. Well known applications of this model are WeBank’s money laundering project and the Melloddy pharmaceutical consortium. As quickly evolving tools such as differential privacy, private set intersection and cryptography increase data privacy safety in collaboration settings, innovative collaborations of this type are more likely in the short and medium term.

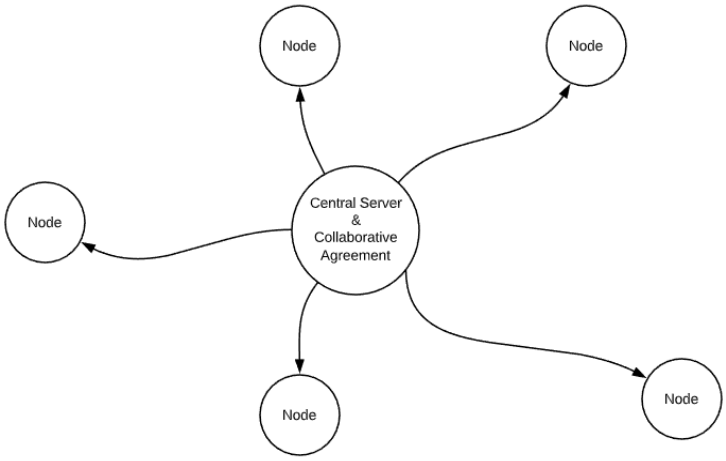

Figure 3

One sub-variation of this model can be seen in figure four, where any organization could create their own personalized private network by paying fees in exchange of running their federated learning algorithms on a curated selection of third party nodes. Current technologies such as application programming interface(API) would be extended to accommodate federated learning access. For example, accessing data silos could be as simple as making federated learning API calls to a first node specialized purchasing power data, then combined to a second node specialized in social media data, then combined to a third node containing location data. The resulting model from this vertical federated learning task(compiling information about one item from different sources) could be used to further enhance customer offer personalizations and product recommendations.

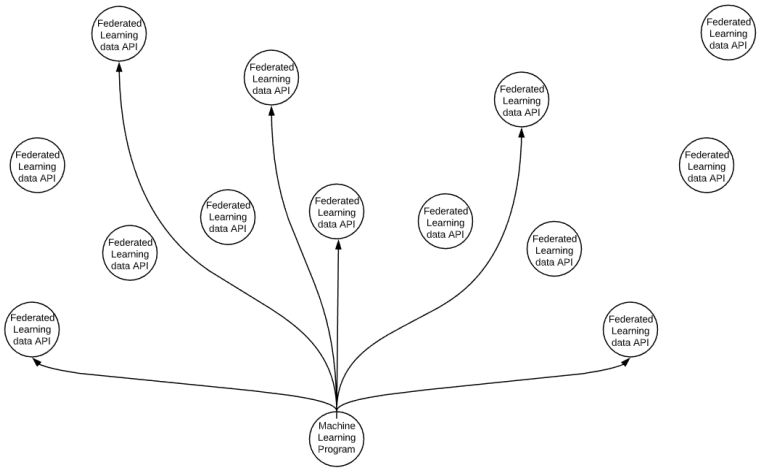

Figure 4

3.2.3 Model type 3

The model illustrated in figure five can be described as a peer-to-peer network collaborating over a common goal. A minimalist central player facilitates a large network of public nodes that actively collaborate by trusting each other moderately. This requires the grouping of a large number of “unionized” players striving towards a common goal. It lends itself to fragmented workers or small organizations in a common industry that are unable to extract AI insights from their individually small, but collectively powerful datasets. These “communities” may have historically collaborated on issues affecting their industries/livelihood/vision, but they may not understand the value of their current data and computing power. A researched example use case is the federation of New-York cab drivers location data, income data, and client data to build a route recommendation engine to better match supply and demand, hence optimizing individual drivers’ profits.

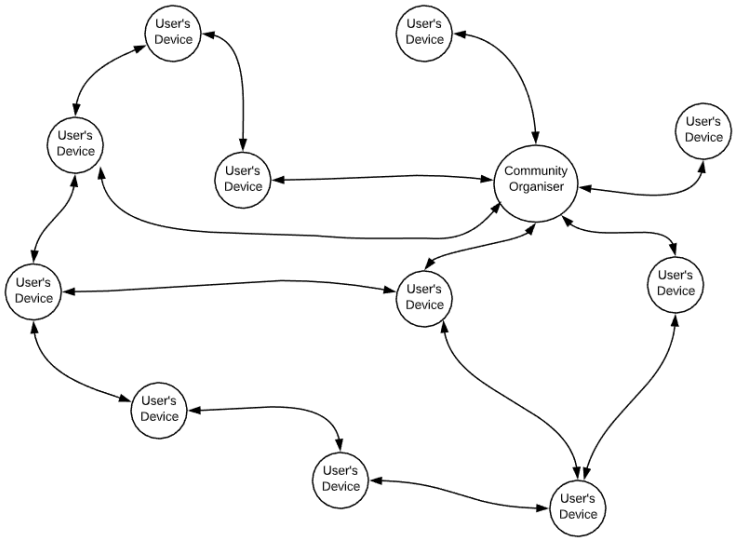

Figure 5

One sub-variation of this model can be seen in figure six where the peer-to-peer network is extended to a non-trusting environment where different players have different incentives. A non-trusting environment requires the creation of incentives to encourage useful behavior and deterrents to discourage detrimental behaviors. In the case where incentives are tokens, this model approaches the concepts of decentralized applications such ethereum Dapps.

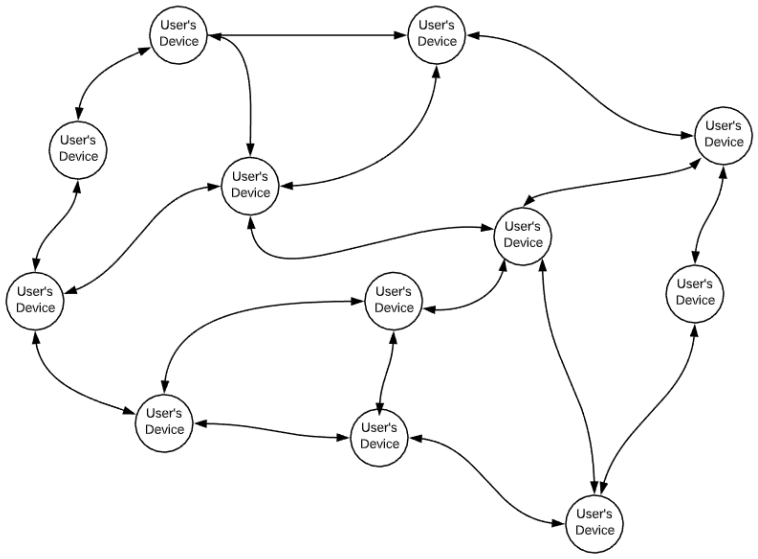

Figure 6

3.3 Centralized versus peer-to-peer federated learning

In a centralized federated learning setting, a central server is responsible to select nodes, coordinate the different steps of the algorithms and aggregate the received model updates. In decentralized federated learning, the nodes in a graph network coordinate themselves to obtain the global model as the model updates are exchanged between interconnected nodes without the orchestration of the central server. The “centralized” federated learning setting has been researched extensively, hence a large amount of resources is available. The “decentralized” federated learning setting has been researched much less, but it can be adapted to utilize the advancement of the “centralized “ federated learning.

Some advantages of the centralized federated learning setting are the large amount of open resources, project ownership and simplicity. Using the large amount of open resource code made available by technology leaders developing the centralized system reduces the cost of development of federated learning systems. Secondly, since implementing a federated learning system can be costly, the centralization of the codebase provides intellectual property protection and a leverage to collect return on investment. Lastly, until federated learning technology gains robustness, handling errors and failures in one central location eases the complexity of implementing systems.

Some disadvantages of the centralized federated learning setting are that the server can potentially represent a single point of failure, a powerful central server may not always be available in more collaborative learning scenarios and the server may even become a bottleneck when the number of clients is very large[21].

Some advantages of the decentralized federated learning setting are increased trust, complete distribution of communication and computation cost and lower cost barrier of entry. Removing the central server means that the federated learning instructions are passed to every node in the system, guaranteeing transparency for every participant. In a central server setting, only the group managing the central server knows how the data is being manipulated[18]. Secondly, the decentralization of the communication cost and the removal of central server cost reduces the need to raise money from the participant. This can be an important aspect in implementations such as a decentralized social media platform where participants expect a free service and dislike the consequences of other revenue sources such as advertisement[19]. Finally, removing the need to rent or buy a server removes one barrier of entry for small organizations lacking the financial resources and the enterprise level expertise[20].

Some disadvantages of the decentralized federated learning setting are the lack of leadership, increased technology complexity and increased complexity of incentives. On most projects, some central leadership may be preferable to set up the learning tasks, choosing the model to be trained, choosing the algorithm to use, debugging when something does not work as expected, etc. Even in a complete decentralised system, a certain degree of trust in an authority is beneficial to lead the project. Second, the added network complexity of various graph topology, asynchrony and heterogenous communication quality must be taken into account to assess robustness, magnitude of bias, speed of consensus, etc. Lastly, motivating decentralized actors to provide quality data, labels and computing power, while demotivating malicious actors is a difficult challenge in a fully decentralized approach.

3.4 Important factors in the adoption of federated learning systems

In an environment where both the market and technology is evolving quickly, federated learning is navigating a “rough water” situation. More factors than we can enumerate can influence the adoption of specific use cases, but some factors apply to all use cases.

Location: European privacy laws makes federated learning more attractive than North-America privacy laws

Number of different stakeholders: The more distinct types of actors needed, the more complex the adoption may be since every actor may have different incentives

Size of stakeholders: Large stakeholders may be slower at adopting innovation due to bias inherent to their own current success, internal structures and incentives systems[22]. On the other hand, they may have more R&D funding to dedicate to a project.

Relative power of the proponent: The adoption of a federated learning project can be fast when the proponent has a central authority in the system. For example Google Gboard only took one year to implement because it was included by default in an update of the android system. Reaching a critical mass of adopters is important to provide proper training data to machine learning algorithms.

Technology maturity: The central server setting has received much more research investment compared to the peer-to-peer setting. Furthermore, no peer-to-peer federated learning

implementation with business success has been found to date. Implementing a brand new technology and likely new business model may translate to higher risk of failure.

Economic environment: Economic cycles affect the market appetite for risk, which affects the number of projects and the type of technologies supported by private and corporate investments.

Enabler versus supporter: If federated learning technology enables gain impossible in the past, adoption case is more likely than if it is only one piece of a larger puzzle. For example, federated learning enables healthcare cases, while federated learning supports the internet of things.

Perception: Federated learning implementation requires risky investment of reputation, time and money from both decision makers and end users. Diffusion of innovation depends largely on human perceptions such as the relative perceived advantage, compatibility with current behaviours, complexity of the concept, trialability of the technology and observability to other organizations.

3.5 Summary of benefits

Distilling the use cases, drivers, models and considerations provide some insights on the benefits gained by using federated learning. These benefits can be used to find new use cases. The table below combines and rewrites the information covered in this section in terms of benefits.

	Benefits	Privacy driven	Hardware Driven	Model 1	Model 2	Model 3
1	Enables data collaboration where previously impossible due to privacy laws	X		X	X	
2	Enables organizational collaborations previously impossible due to fear of disclosing valuable competitive information	X			X	
3	Enables individual collaborations previously impossible due to fear of disclosing sensitive information	X		X		X
4	Enables smaller organizations to pool sufficiently large amounts of data to utilize artificial intelligence	X			X	X
5	Enables Individuals to maintain ownership of the raw data while receiving the benefits of collaborating with their peers	X		X	X	X
6	Increases accuracy of recommendation engines, personalized ads and personalized offers	X		X	X	
7	Provides a strategic feature of differentiation for products aimed at customers valuing data privacy	X		X	X	X
8	Reduces cost of server rental/ownership required to obtain the same insights(computing cost is distributed to each nodes)		X	X	X	X
9	Reduces cost of IOT installations due lesser communication hardware setup(insights data is much smaller than raw data)		X	X	X	X
10	Provides participants with local, regional and global insights		X	X	X	X

4. Technology stack

The closest indication of the current technologies used at leading companies are the open resources they continually release and the publicly available academic-industry research they co-author. Once a use case has been confirmed to be worth implementing, these open source libraries contain most pieces needed to build a working federated learning project.

4.1 Open source technologies

The four most popular open source federated learning tools and libraries collections are TensorFlow Federated, PySyft, PaddleFL and FATE. The most popular open source peer-to-peer federated network is PyGrid. LEAF is a set of tools and libraries standards.

TensorFlow Federated[23] is an open-source framework for machine learning and computations on decentralized data. It is maintained by Google and is built on the TensorFlow framework.

PySyft[24] is an open-source framework enabling federated learning, differential privacy, encrypted computation(CrypTen), multi-party computation and homomorphic encryption. It is maintained by OpenMined and is built on the Tensor Flow and PyTorch frameworks.

PyGrid[25] is an open-source network enabling peer-to-peer model training by using the PySyft tools and libraries collection mentioned above. It is also maintained by OpenMined and is built on the Tensor Flow and PyTorch frameworks.

PaddleFL[26] is an open source federated learning framework enabling vertical federated learning strategies such as privacy-preserving logistic regression, neural network with multi-party computation. It also provides horizontal federated learning strategies such as federated averaging, differential privacy and secure aggregation. It is maintained by Baidu and is built on the PaddlePaddle framework.

Federated Ai or FedAi or FATE[27] is an open-source project based on homomorphic encryption and multi-party computation. It supports a number of federated learning algorithms strategies including vertical federated learning, horizontal federated learning, and federated transfer learning. It was released by the Chinese digital bank WeBank and is maintained by the online community via the Linux Foundation.

LEAF[28] is an open-source benchmark for federated settings. It consists of a suite of open-source datasets, an array of statistical and systems metrics, and a set of reference implementations. It brings together a set of standard methods across federated learning platforms. It is maintained by Carnegie Mellon University

4.2 Technology challenges

Federated learning research and innovation has been experiencing a strong growth since its beginning in 2015. This section will discuss some challenges and corresponding active areas of research. These are categorised into algorithm, privacy, failure and bias research[29].

4.2.1 Improving algorithmic effectiveness

Independent and identically distributed(IID) data has an ideal and clear approach, but non-IID data come in several varieties, each bringing their own set of difficulties. Common ways in which data tend to deviate from being IID are non-identical client distributions(feature distribution skew, label distribution skew, same label, but different features, same features, but different label, quantity skew, etc.), violations of independence and dataset shift. Solutions being researched are to modify existing algorithms, augment client data and use a combination of models.

Machine learning algorithms must be modified to suit the federated learning approach. Algorithms have to be flexible to statelessness when the total number of devices is large, cryptography techniques(cryptographic secure aggregation protocols, differential privacy, model compression, etc.). The development of new algorithms that specifically target the characteristics of the federated learning setting remains an important open problem.

Tailored techniques to suit naturally occurring deviance such as personalization(using a global model to produce highly personalized predictions), multitask learning(separate the learning by tasks rather than by client) and meta learning(adapt the global model to local instance) can make federated learning more useful and more accurate.

Engineering a federated learning training requires novel development tools, development steps and debugging to engineering a machine learning training on one dataset. This makes construction more difficult and convoluted.

Communication in federated learning can be a primary bottleneck that must be mitigated by using techniques such as accuracy reduction and compression(gradient compression, model broadcast compression, local computation reduction, etc.) or accentuated with privacy techniques such as secure aggregation and noise addition

Federated learning has primarily considered supervised learning tasks where data is labeled on the client side. Much work must be done to extend the technology to other machine learning paradigms such as unsupervised learning and reinforcement learning.

4.2.2 Improving data security

Various attacks can be attempted on a federated learning central server. For example, a malicious actor could create bias in the model being learned or prevent a model from being learned. Given the complexity of the technology, research continues to improve security by combining interdisciplinary concepts such as secure multi-Party computation(MPC), trusted execution environment (TEE), differential privacy(DP), homomorphic encryption, etc.

Attacks such as adversarial clients watching model iterations or stealing the final model can also be made on the edge nodes. Research continues on MPC, TEE, DP and model encryption.

While data privacy continues to improve, work remains to be done on making the benefits more intuitive to the users, prevent a false sense of security and simplify the implementation of privacy techniques(MPC, TEE, DP, etc.)

Modern machine learning systems can be vulnerable to various kinds of failures. The distributed nature, architectural design, and data constraints of federated learning increase the potential for failure and attacks. Furthermore, security tools can make the detection and correction of the problems more challenging.

4.2.3 Reducing attacks and system failures

Malicious attacks such as data poisoning, label poisoning and model update poisoning are more prevalent in federated learning. Improving the robustness using techniques such as differential privacy is being explored in recent work.

Non-malicious failures are less damaging, but potentially more common. Errors occurring at the client, pipeline or server side can be particular to federated learning programs needing improved robustness.

4.2.4 Reducing sources of bias

Complex processes can cause an output model to be unfair for some groups. This is especially difficult to detect when demographic information cannot be observed. Vertical federated learning approaches have the potential to resolve these issues by combining datasets that can correlate the demographic information to detect biases.

Federated learning can produce a new type of bias through the client sampling methods. For example, using connection type/quality, device type, location, activity patterns, and local dataset size can over-represent a particular demographic at the expense of others. Evolving frameworks like agnostic federated learning is one approach to control for this type of bias.

5. Looking forward

5.1 Technology perspective

Federated learning relies on the development of other technologies such as network, encryption, data collection, machine learning, etc. Since federated learning is mainly an add-on feature to machine learning, its adoption is bound to follow a similar pace. Given that we are still early in the world’s adoption of machine learning, broad federated learning adoption is likely to take several years. Large organizations that have the ability to invest in research or consortium supported by government grants are already starting to utilize federated learning for enhancing current machine learning abilities. Given that machine learning in its early stage of mass adoption and that federated learning further enhances its abilities, the coming years will be a fertile ground for innovation.

5.2 Business perspective

Given that federated learning requires collaboration between parties, there may be lessons to be learned from the adoption of cooperative technologies such as blockchain and enterprise resource planning(ERP) systems. Blockchain in business cases are still in the adoption stage 10 years after the introduction of Bitcoin that popularized the concept. ERP systems took 3 decades to permeate all businesses. We may infer that federated learning could gain mass adoption in the coming 10-30 years. Given the expertise, investment and data required to implement federated learning use cases, it is likely that the spread of the technology will favor large organizations early on, then trickle down to medium size organizations, then eventually small businesses.

5.3 Community perspective

There is a real potential to empower communities by using federated data and federated learning. Federated learning model 2 has the highest chance of being within reach for tech savvy organizations within years. The technology could provide industry and community groups with access to data a chance at participating in the machine learning trend. While large organizations are ramping their use of data and seeing the benefits of their efforts, groups with fragmented data should consider this technology to remain competitive. For example, small courrier/trucking companies, specialized insurance companies and community banks have access to data that can be enhanced when combined. In the case of model 3, the amount of technical skills required to build and use this technology may slow down its mass individual use.

6. Concluding Remarks

Federated learning decentralizes data access and computation work, resulting in increased data privacy, distribution of computation cost and reduction of communication cost. The technology has undergone an explosive growth in industry and academia since 2016. Its privacy enabling qualities has already led to production deployments on legal and business issues while its potential to decentralize computation and communication cost point to continued widespread adoption. Within the 3 models described, the private network model 2, which enables the connection of data silos and the collaboration of organisations, appears the most promising for its mass adoption. Those interested in using the federated learning can get started using open source code released by large organisations such as TensorFlow Federated and by joining communities of programmers such as the PySyft OpenMined community.

References

[1] Jakub Konečný, H. Brendan McMahan, and Daniel Ramage. Federated Optimization: Distributed Optimization Beyond the Datacenter, 2015. URL https://arxiv.org/pdf/1511.03575.pdf

[2] Jakub Konečný, H. Brendan McMahan, and Daniel Ramage . Federated Optimization: Distributed Machine Learning for On-Device Intelligence, 2016. URL https://arxiv.org/pdf/1610.02527.pdf

[3] Chae, Y. (2020, January 1). U.S. AI Regulation Guide: Legislative Overview and Practical Considerations. Retrieved August 11, 2020, from https://www.bakermckenzie.com/-/media/files/people/chae-yoon/rail-us-ai-regulation-guide.pdf

[4] GDPR Archives. (n.d.). Retrieved August 11, 2020, from https://gdpr.eu/tag/gdpr/

[5] Office of the Privacy Commissioner of Canada. (2019, June 07). PIPEDA in brief. Retrieved August 11, 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[6] MELLODDY. (n.d.). Retrieved August 11, 2020, from https://www.melloddy.eu/

[7] “Home.” *OWKIN*, 3 Aug. 2020, owkin.com/.

[8] *Utilization of FATE in Anti Money Laundering Through Multiple Banks*. FedAI.org. (2019, October 25). https://www.fedai.org/cases/utilization-of-fate-in-anti-money-laundering-through-multiple-banks

[9] *Federated Learning: Collaborative Machine Learning without Centralized Training Data*. Google AI Blog. (2017, April 6). https://ai.googleblog.com/2017/04/federated-learning-collaborative.html.

[10] *Snips Acquired by Sonos*. snips.ai. https://snips.ai/.

[11] *Utilization of FATE in Risk Management of Credit in Small and Micro Enterprises*. FedAI.org. (2020, January 8). https://www.fedai.org/cases/utilization-of-fate-in-risk-management-of-credit-in-small-and-micro-enterprises/.

[12] *Fraud Detection: QEDIT's privacy-compliant solution*. QEDIT. https://www.qed-it.com/fraud-detection/.

[13] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. Federated Machine Learning: Concept and Applications, 2019. URL https://arxiv.org/pdf/1902.04885.pdf

[14] Paritosh Ramanan, and Kiyoshi Nakayama. BAFFLE : Blockchain Based Aggregator Free Federated Learning, 2020. URL https://arxiv.org/pdf/1909.07452.pdf

[15] Xinle Liang, Yang Liu, Tianjian Chen, Ming Liu and Qiang Yang. Federated Transfer Reinforcement Learning for Autonomous Driving, 2019. URL https://arxiv.org/pdf/1910.06001.pdf

[16] Steedman, M. (2019). Ten years on. Measuring the return from pharmaceutical innovation. Retrieved August 11, 2020, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-measuring-return-r&d-ten-years-on.pdf

[17] Coldewey, D. (2019, February 13). Xnor's saltine-sized, solar-powered AI hardware redefines the edge. Retrieved August 11, 2020, from https://techcrunch.com/2019/02/13/xnors-saltine-sized-solar-powered-ai-hardware-redefines-the-edge/

[18] Abhijit Guha Roy, Shayan Siddiqui, Sebastian P¨olsterl, Nassir Navab, and Christian Wachinger. BrainTorrent: A Peer-to-Peer Environment for Decentralized Federated Learning, 2019. URL https://arxiv.org/pdf/1905.06731.pdf

[19] Chaoyang He, Conghui Tan, Hanlin Tang, Shuang Qiu, and Ji Liu. Central Server Free Federated Learning over Single-sided Trust Social Networks, 2020. URL https://arxiv.org/pdf/1910.04956.pdf

[20] M. Carcary, E. Doherty, and G. Conway, “The adoption of cloud computing by irish smes-an exploratory study,” Electronic Journal of Information Systems Evaluation, vol. 17, no. 1, p. 3, 2014.

[21] Xiangru Lian, Ce Zhang, Huan Zhang, Cho-Jui Hsieh, Wei Zhang, and Ji Liu. Can Decentralized Algorithms Outperform Centralized Algorithms? A Case Study for Decentralized Parallel Stochastic Gradient Descent, 2017. URL https://papers.nips.cc/paper/7117-can-decentralized-algorithms-outperform-centralized-algorithms-a-case-study-for-decentralized-parallel-stochastic-gradient-descent.pdf

[22] Christensen, C. M., Kaufman, S. P., & Shih, W. C. (2020, March 2). *Innovation Killers: How Financial Tools Destroy Your Capacity to Do New Things*. Harvard Business Review. https://hbr.org/2008/01/innovation-killers-how-financial-tools-destroy-your-capacity-to-do-new-things.

[23] Tensorflow. *tensorflow/federated*. GitHub. https://github.com/tensorflow/federated.

[24] OpenMined. *OpenMined/PySyft*. GitHub. https://github.com/OpenMined/PySyft.

[25] OpenMined. *OpenMined/PyGrid*. GitHub. https://github.com/OpenMined/PyGrid.

[26] PaddlePaddle. *PaddlePaddle/PaddleFL*. GitHub. https://github.com/PaddlePaddle/PaddleFL.

[27] FederatedAI. *FederatedAI/FATE*. GitHub. https://github.com/FederatedAI/FATE.

[28] TalwalkarLab. *TalwalkarLab/leaf*. GitHub. https://github.com/TalwalkarLab/leaf.

[29] Peter Kairouz, H. Brendan McMahan, and al. Advances and Open Problems in Federated Learning, 2019. URL https://arxiv.org/pdf/1912.04977.pdf