Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/4/20230487

Federated transfer learning: Concept and application

Tengjun Ni

Liangjiang International College, Chongqing University of Technology, Chongqing, 401135, China

nitengjun2002@163.com

Abstract. As the development of Machine Learning, more and more data are used to train models in order to guide people's daily life. Faced with privacy and efficiency challenges these days, Federated Transfer Learning (FTL) has grown in popularity, as it has a great ability to protect data privacy while also dealing with the problem of data scarcity. In this passage, the author studies the FTL and its different applications, including sales industry, Industrial Internet of Things Devices, Finance application, Medical Application and Autonomous Driving, analyses the usage in the different industries. Further, the author discusses the privacy and robustness of FTL, which are the core features of FTL. In the end, the author concluded the features of FTL and also gave a prospection of FTL.

Keywords: Federated Learning, Transfer Learning, Privacy, Robustness.

1. Introduction

Since the first time Artificial Intelligence (AI) was put forward at the Dartmouth Conference in 1956, it has been regarded as one of the most popular topics. Federated Learning (FL), a new kind of machine learning, which is one of the main parts of AI, has been put forward. In order to solve the problem of data privacy and security protection, FL provides a federation to get a centralized model for every user.

Meanwhile, the annotation data mastered by all parties of the consortium can be effectively applied to enrich annotation data. While FTL uses Homomorphic Encryption and Polynomial Approximation to replace the method of Differential Privacy. The author briefly analyses the adaptability of FTL apply in several different domains, and the privacy and robustness of FTL.

2. Related Work

2.1. Federated Learning

Faced the lack of the data for AI training, especially for small institution and company, to deal with the "data island", Federated Learning came out.Federated learning is a distributed machine learning framework with privacy protection and secure encryption technology[1] [2]. There are three kinds of Federated Learning, including horizontal federated learning, vertical federated learning and federated transfer learning[3].

2.1.1. Horizontal federated learning. Horizontal federated learning is also called Feature-Aligned Federated Learning. The method is widely used when the participants have similar features but different

DOI: 10.54254/2755-2721/4/20230487

users. That is, the data characteristics of participants in horizontal federated learning are aligned, as figure 1 illustrates. Different from the tradition of machine learning, all the participants use their own training data without providing it to others and collaboratively learn a shared prediction model. What they need to do is to upload the parameters to the server and the server will give back a new prediction model. Persist in so doing, the training model's loss will be lower enough, so that the accuracy of the model will become better.

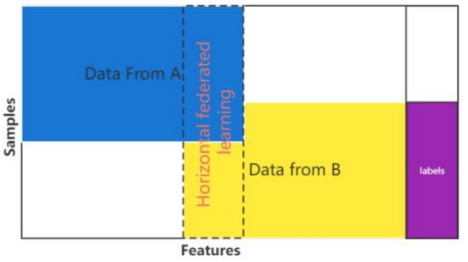

Figure 1 Horizontal federated learning.

2.1.2. Vertical federated learning. Vertical federated learning is the union of features, participants have similar samples but different features. Participants will align the samples without provide them to others, so that the private data will not be revealed, as figure 2 illustrates. In vertical federated learning, all the participants do not expose the data with different samples among them[4]. Similar to the horizontal federated learning, vertical federated learning use encryption-based data. All of the participants are unaware of each other's actual data, but they work together to train the model. With the trained model, they can predict more data with high accuracy.

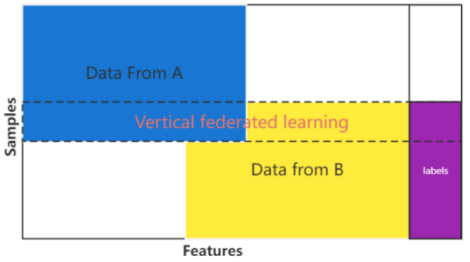

Figure 2 Vertical federated learning.

2.2. Transfer Learning

Transfer Learning is a kind of machine learning that transfers from one domain to another to solve problems across domains[5]. It's aim is to transfer annotated data or knowledge structures from related domains to accomplish or improve the learning performance of the target domain or task.

Different from the traditional machine learning, Transfer Learning allows the domains, tasks, distributions used in either the training or test set to be totally different. As the figure 3 below, traditional machine learning can only do the task from their own samples, so that circle sample can only deal with circle problem, and same as triangle and diamond ones. While by using Transfer Learning, it combines the two different kinds of samples (circle and triangle) together, in order to give the prediction of the target task (diamond ones). It's quite easy to find that, by using Transfer Learning, we can use less data to predict more complicated results.

DOI: 10.54254/2755-2721/4/20230487

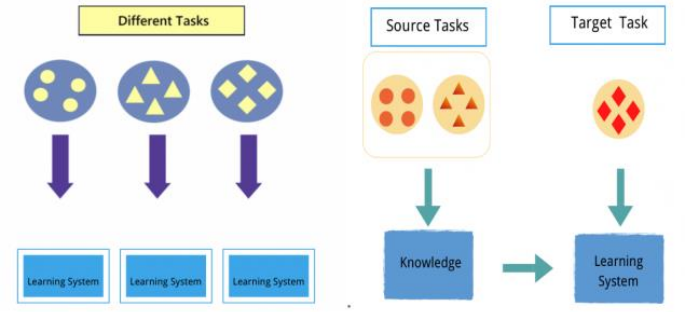

Figure 3. Differences between traditonal machine learning and transfer learning.

3. Federated Transfer Learning

Federated Transfer Learning (FTL) is aimed at under the premise of protecting the data policy, dealing with the problem of the lack of the data by using transfer learning. As we all know, data is the most valuable and scarce thing in machine learning, but most data is private. That's why Federated Transfer Learning came out. Federated Transfer Learning is the expand of Federated Learning, which can be used on not only two sample spaces, but also two different datasets [6].

Federated Transfer Learning migrates features from different feature spaces into the same latent representation and then trains them using labels from the labeled data collected by different participants. In the FL practical framework proposed by Google, the emphasis is on the fact that the participants, that is, the users in the federated learning architecture, are independent, but the characteristics must be the same between the different participants. While FTL emphasize that the characteristics of different participants are different. That's the advantage of FTL to face to those problems of insufficient data and small data volume.

As the figure follows, two data form A and B holds really small overlap, whether the feature space or the sample space. Both Horizontal Federated Learning and Vertical Federated Learning cannot get a result with a high accuracy. However, that's when Federated Transfer Learning come in handy. Using the technology of Transfer Learning, more data from the non-overlapping place spring up, and by these relatively reliable data, a better learning result will be provided. To sum up, using transfer learning is to broaden the scarce feature and sample spaces.

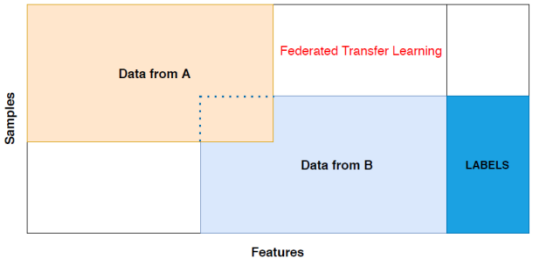

Figure 4. Federated Transfer Learning.

As the figure below, during FTL, A and B calculate and encrypt their intermediate results, including gradients and losses. And the third party collected these results and decrypted these gradients and losses. After that, A and B received the parameters and update their own models. In order to avoid exposing participants' data in the process of back propagation, FTL adopts homomorphic encryption to ensure security and polynomial difference approximation to ensure privacy. Unlike classical FL, where raw data and models are stored locally, FTL makes participants encrypt gradients before data transfer and uses techniques such as adding random masks to prevent participants from guessing each other's information at any stage of the task [7].

DOI: 10.54254/2755-2721/4/20230487

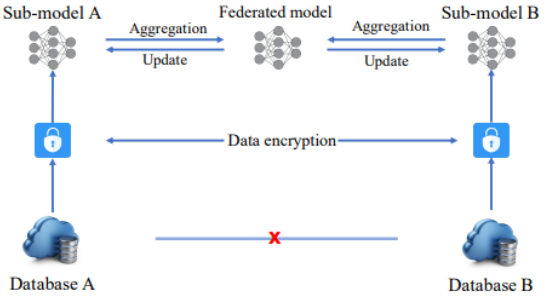

Figure 5. The way of FTL model to ensure the data privacy 4. The application of Federated Transfer Learning.

3.1. Sales industry

The recommendation algorithm plays an important role in today's sales industry, especially in e-commerce. But when it comes to some new products and new customers, it's a good idea to use Federated Transfer Learning to deal with how to recommend certain products to certain people, which is totally one of the most difficult things in the commercial area.

Some companies have already tried to use Federated Transfer Learning by using their customers' basic data and comment data to train a FTL model, in order to help those websites provide accurate projections to specific people.

In [8], it illustrates that how the company use the movie comments to recommend some related products. On the surface, there's no relation between movie and electronics.

Figure 6. Product recommendations reference in users' movie reviews4.2 Industrial Internet of Things Devices.

Nowadays, Federated Learning has been widely used in IIoT technology during factories' daily production. But it is harder for devices to fit the rapid development of the need of processing [9]. In addition, some attacks happen unavoidably because of the large amount of data generation and processing [10]. And the most important thing is that usually people cannot acquire adequate data for Federated Learning[11]. So Federated Transfer Learning works.

As the algorithm of FTL for IIoT devices, data from devices are provided to edge servers, after deduplication and training models, these models will be upload to the cloud servers. Cloud servers then gather and optimize the new model, and transfer the model to edge servers and devices. After keep looping the processes, a model which is trained suitable enough has been generated. In [12], the author through some experiments analyze the feasibility of the usage of Federated Learning and Transfer Learning.

DOI: 10.54254/2755-2721/4/20230487

3.2. Finance application

With the rapid development of the financial services, lots of small and micro businesses come forth, but for those company, they don't have enough users' finance data to build some related model, which restrict the development of these companies. By using Federated Transfer Learning, these small and micro companies can absorb the data from the large companies without get the details. By this way, small and micro companies can provide a good model and customers' privacy in the huge companies are protected.

The application can be divided into two kinds, one is based on features and the other is based on models.

3.2.1. The application of FTL based on features. As the figure, for small company C, it's really hard for the company to train a perfect model with only few data, while company C can find the similar dataset based on the feature and transfer learning the model. Only in this way, can the company C get the most reasonable model.

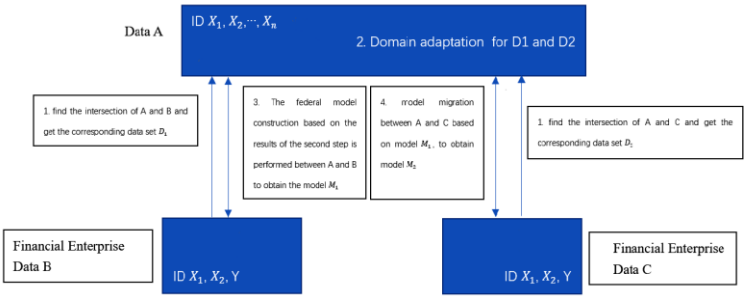

Figure 7. Applications of feature-based federal transfer learning 4.3.2 The application of FTL based on models.

In practical financial scenarios, such as pre-loan risk assessment of new products, because the risk control mode of credit products is similar, FTL can be used to transfer and re-apply the model.

As shown in the figure below, when the sample data of product B is small, the GBDT model can be constructed by using the sample data of product A, and then the LR algorithm can be used for model transfer learning.

Model-based federated migration learning can not only protect data security, but also reuse the original results and improve the accuracy and efficiency of the model.

DOI: 10.54254/2755-2721/4/20230487

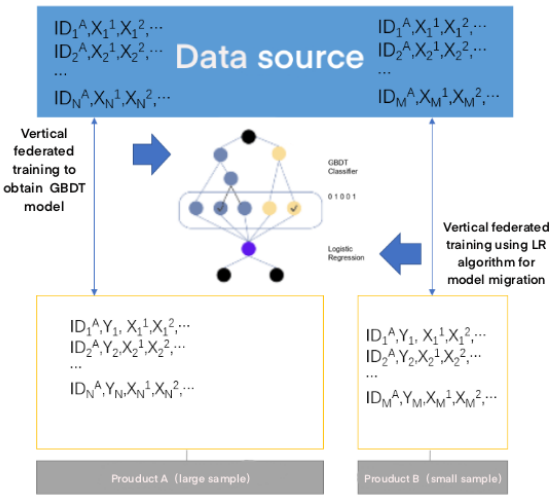

Figure 8. Model-based application of federal transfer learning4.4 Medical Application.

As many AI applications begin to be used in the medical field, data protection in the medical industry is becoming more and more important. Data for healthcare facilities is particularly sensitive to privacy and security issues, and simply collecting it together is not feasible; In addition, because of the large number of institutions involved in medical care, it is difficult to collect sufficient data with rich characteristics that can be used to comprehensively describe patients' symptoms.

In smart healthcare systems, medical data, genetic data, medical imaging data, expert knowledge, electronic health records, etc., are all important data that cannot be directly used due to data privacy or data security. Secondly, medical-related data may be multi-source heterogeneous data, including medical images, gene sequencing, health records, etc. Only by using federated transfer learning technology can these data be fused for better application in scenarios [13].

Federated Transfer Learning technology can help expand the sample and feature space of training data and reduce the difference of sample distribution among medical institutions, thus improving the performance of the shared model and playing an important role. If a significant number of healthcare organizations can participate in the construction of data federation through federated migration learning, healthcare AI will bring more benefits to more patients [14].

3.3. Autonomous Driving

As the development of autonomous driving, FTL is also helpful for it, Xinle Liang[15] et al. proposed a federated transfer learning for real-time knowledge extraction combining reinforcement learning. In this framework, all participants would take corresponding actions according to the knowledge learned by others, so that they could learn from scratch and avoid collisions with obstacles in the indoor environment. The results show that the simulated vehicle agent can transfer the knowledge to the physical vehicle in real time, the average obstacle distance is increased by 27%, and the number of collisions is reduced by 42%.

4. Privacy and Robustness in FTL

Privacy and robustness are two most important attributes that people concerned. The level of privacy and robustness of FTL is the index of how safe FTL is. Aiming at protect the data for machine learning, attacks of all kinds should be prevented.

4.1. Privacy protection

Privacy threatens can be divided into two kinds, semi-honest and malicious. For semi-honest, the participants are considered honest-but-curious, they try to know others' data but obey FL protocols.

DOI: 10.54254/2755-2721/4/20230487

While as for malicious, adversaries try to attack the eco-system by modifying, re-playing, or removing messages without obeying protocols. Lyu[16] concluded three main means to defense threatens, including homomorphic encryption, Secure Multiparty Computation and Differential privacy.

4.2. Robustness

Robustness threatens can also divided into two kinds of attack, untargeted and targeted. Untargeted attack is aimed to arbitrarily destroy the integrity of the target model. Targeted attacks induce the model to output the target tag specified by the opponent for a particular test example, while testing the error of the other test examples is unaffected. As for untargeted attack, using Byzantine fault algorithm to get rid of those adversarial parties. When it comes to targeted backdoor attacks, the model can protect against them using detection and erasing methods [17].

5. Conclusion

Federated Transfer Learning, as a new studying mode, which can not only protect the privacy, but also can enlarge the datasets and make more accurate models, is becoming more and more popular these days. It has been used in many industries. Because of the high data demands of FTL, it's absolutely hard for me to provide a data result, which is why I cannot verify the robustness of the FTL model specifically. As the accumulation of the data, gradually, the problem would be dealt. From the perspective of social needs, FTL caters to people's requirements for privacy protection and makes private data more secure, which is also what we like to see. So that based on the idea of FTL, it's wise for us to make a FTL ecosystem. In the future, companies from the same industry can form a union, in order to realize the positive growth of each other's models without disclosing privacy, so as to better serve customers.

References

[1] Jakub Konecný, H. Brendan McMahan, Daniel Ramage, and Peter Richtárik. 2016. Federated optimization: Distributed machine learning for on-device intelligence. CoRR abs/1610.02527 (2016). arxiv:1610.02527

[2] Jakub Konecný, H. Brendan McMahan, Felix X. Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. 2016. Federated learning: Strategies for improving communication efficiency. CoRR abs/1610.05492 (2016). arxiv:1610.05492

[3] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, "Federated Machine Learning: Concept and Applications," Feb. 2019. Available: https://arxiv.org/abs/1902.04885

[4] S. Hardy, W. Henecka, H. Ivey-Law, R. Nock, G. Patrini, G. Smith, and B. Thorne, "Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption," arXiv preprint arXiv:1711.10677, 2017.

[5] Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., … He, Q. (2020). A Comprehensive Survey on Transfer Learning. Proceedings of the IEEE, 1–34. doi:10.1109/jproc.2020.3004555

[6] Yongqiang Peng, Zongyao Chen, Zexuan Chen, Wei Ou, Wenbao Han, Jianqiang Ma. "BFLP: An Adaptive Federated Learning Framework for Internet of Vehicles", Mobile Information Systems, 2021

[7] Jing Q , Wang W , Zhang J , et al. Quantifying the Performance of Federated Transfer Learning. 2019. http://arxiv.org/abs/1912.12795

[8] Zhang P , Sun H , Situ J , et al. Federated Transfer Learning for IIoT Devices with Low Computing Power Based on Blockchain and Edge Computing[J]. IEEE Access, 2021, PP(99):1-1.

[9] L. D. Xu, W. He, and S. Li, ``Internet of Things in industries: A survey," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 22332243, Nov. 2014.

[10] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, ``Security and privacy challenges in industrial Internet of Things," in Proc. 52nd ACM/EDAC/IEEE Annu. Design Autom. Conf. (DAC), Jun. 2015, pp. 1-6.

[11] K. Kaur, S. Guo, M. Chen, and D. Rawat, ``Transfer learning for 5G-aided industrial Internet of

DOI: 10.54254/2755-2721/4/20230487

Things," IEEE Trans. Ind. Informat., early access, Apr. 6, 2021, doi: 10.1109/TII.2021.3071310

[12] P. Zhang, H. Sun, J. Situ, C. Jiang and D. Xie, "Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing," in IEEE Access, vol. 9, pp. 98630-98638, 2021, doi: 10.1109/ACCESS.2021.3095078.

[13] Xu, J., Glicksberg, B.S., Su, C. et al. Federated Learning for Healthcare Informatics. J Healthc Inform Res 5, 1–19 (2021). https://doi.org/10.1007/s41666-020-00082-4

[14] John Blitzer, Ryan T McDonald, Fernando C. N. Pereira. Domain adaptation with structural correspondence learning. EMNLP '06: Proceedings of the 2006 Conference on Empirical Methods in Natural Language ProcessingJuly 2006 Pages 120–128

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

[16] Lyu L, Yu H, Ma X, et al. Privacy and robustness in federated learning: Attacks and defenses[J]. arXiv preprint arXiv:2012.06337, 2020.

[17] Y. Li, B. Wu, Y. Jiang, Z. Li, and S.-T. Xia, “Backdoor learning: A survey,” arXiv preprint arXiv:2007.08745, 2020.