Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **S-2** Year **2023** Pages **2576: 2584***

Investigate the Advancements in Federated Learning Techniques to Enable Privacy-Preserving Machine Learning

Nidhi Nitin Surve[1*], Tejas Prashant Bhanushali[2], Tanishq Sambhaji Patil[3], Ishaan Nimish Hadkar[4], Aaryan Mangesh Gujar[5]

[1, 2, 3, 4, 5] Department of Computer Engineering, D Y Patil Deemed to be University, Navi Mumbai, Re-Accredited by the NAAC with 'A++' Grade, Nerul, Navi Mumbai, India
[1] nidhisurve7425@gmail.com
*Corresponding Author E-mail: nidhisurve7425@gmail.com

Article History

Received: 26 March 2023 Revised: 12 July 2023 Accepted:29 July 2023

Abstract

A possible approach to address the increasing security and privacy concerns is federated learning (FL). Its primary benefit is dispersed client participation to learn the model without needing to submit any personal data. In this study, researchers have explored the key technologies underpinning FL from both practical and theoretical viewpoints, and they followed the creation experience of associated publications. In order to be more specific, researchers first categorize the research on FL architecture into different groups based on the network architecture of FL systems. Researchers then extend the theoretical framework of FL base designs, define the broad techniques, and reframe the application's difficulties. They also present the suggested methods for modelling training utilizing FL.
They have developed an additional generalized algorithm-building framework after analyzing and summarizing the current FedOpt algorithms and delving completely into the creation principles for multiple first-order algorithms. Such frameworks make it simple to develop FedOpt algorithms. Considering the significance of security and confidentiality in Florida, they outline possible dangers and countermeasures. The main aim of this research is to assess different types of advancements in the techniques of federated learning for enabling privacy-preserving in machine learning.

Keywords: *Federated Learning, Privacy-Preserving Machine Learning, Data Security, Non-IID Data, Secure Multi-Party Computation.*

1. INTRODUCTION

Due to the rapid expansion of computing resources, an increasing amount of information is found on the daily activities of people, which has become an innovative asset in modern society. Although big data has helped society tremendously by enabling both businesses and people to acquire new perspectives and foresights, its extensive reliance on data has raised concerns about security and confidentiality. Due to the extensive implementation of the "General Data Protection Regulation" by the European Union and similar laws in the United States and China, data privacy and security have undergone a significant new phase of growth in the past few years (Dash et al. 2022). This has resulted in greater emphasis and broad acceptance of safe computer technology such as unique confidentiality, protected multi-party computation, and FL. The primary objective of this study is to evaluate various forms of progress made in federated learning techniques to enable privacy-preserving in machine learning.

Data security and compliance can be successfully maintained through the use of federated learning. As an original approach to machine learning, it is fundamentally a distributed machine learning architecture in which many clients work together to finish one training assignment under the direction of an authoritative server. Client choice, communication, local processing with client data, and global aggregating on the server are common FL techniques.

The most prevalent FL scenario includes ***horizontal FL (HFL)***, in which both data owners utilize identical spaces of features but generate slightly distinct samples. HFL has been thoroughly researched, as it often

happens in real-world situations (Truong & Le, 2023). For instance, as people become more concerned with their health, a greater percentage of people are likely to use smartwatches to monitor their physical activity; these gadgets will deliver tremendous quantities of data that have comparable attributes, allowing for the model to be taught together via the assistance of a centralized server.

Vertical FL (VFL) focuses on a situation in which datasets among clients have different feature spaces but identical sample ID spaces. It was initially thought of as a form of working together between two individuals, but applying it to teams of people is an emerging trend. VFL is extremely relevant to the real world (Alazab et al. 2023). Without more data, these medical facilities will have a broader range of characteristics with which they can collaborate on the model. "Vertical federated learning" and "horizontally federated learning" are two broad classifications that can be utilized for categorizing FL. Various individuals possess various samples of an identical collection of features, whereas other individuals possess different feature data for the identical collection of samples.

As the dataset includes characteristics and IDs from various areas, ***federated transfer learning (FTL)*** could be utilized for transferring knowledge between them. Data labeling has become a laborious and expensive procedure that is often required in social computing networks. The data set and the feature space can be solved collectively using FTL approaches to decrease the computational burden of the federation. Information can be carried from the domain of origin to the target field in a data federation utilizing FTL while maintaining the privacy of the customers' data. There have been numerous recent major study achievements in the area of FL, such as improvements in security and performance (Zhang *et al.* 2021). Communication limitations due to variables including network variety, geographical distance, and data latency during transfer are a prevalent cause of performance issues in Florida.

In federated learning, the slow or rapid divergence of the global model is brought about by the non-IID distribution of data. Regulating optimization has become common in the training of machine learning models to prevent overfitting and improve convergence. In order to solve these issues, researchers have looked into cutting-edge FL algorithms to boost the effectiveness of model training. Techniques such as compression, asynchronous cooperation, sparsification, and worldwide acceleration are all included in this group of methods. In terms of security issues, FL can pose extra risks due to the importance of multiple parties' participation (Girgis et al. 2021). The FL procedure can be susceptible to information leakage and gateway attacks, however, novel remedies and innovations have appeared over the past few years that improve safety defence abilities.

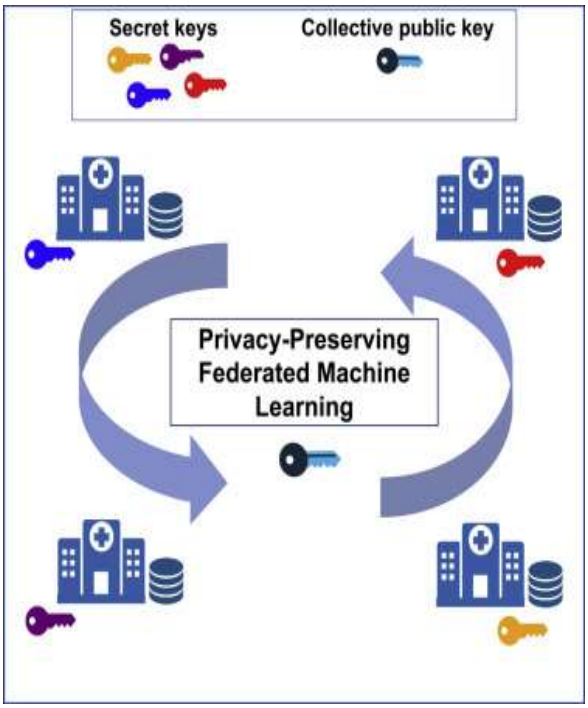

Figure 1: Privacy preserving federal machine learning
(Source: Girgis et al. 2021)

Privacy-preserving analysis of information has served as an area of research for more than fifty years, but it has only been in the past ten years that practical methods have been widely adopted. Consumer digital products have begun to utilize "cross-device federated learning" and "federated data analysis". "Google's Gboard mobile keyboard", in addition to capabilities on "Pixel phones" and "in Android Messages", all incorporate a great deal of federated learning. Although Google was the initial user of "cross-device FL", there has been increasing interest in this setting beyond just that corporation (Xia et al. 2021). For instance, "Apple's QuickType keyboard" and "the vocal classifier" for "Hey Siri" utilize "cross-device FL" in iOS 13 and doc. AI is developing a cross-device FL solution to support medical research, and Snips has experimented with cross-device FL for hotword recognition. Several sectors, including intelligent manufacturing, risk assessment and predictions for reinsurance, medicine discovery, health record mining, health information segmentation, and others, have suggested or detailed cross-silo applications.

As the demand for federated learning technology rises, a growing number of assets, such as applications and structures, are being created to accommodate it. For example, there is the "TensorFlow Federated System", "the Federated AI Technology Enabler", "PySyft", "Leaf", "PaddleFL", and "the Clara Training Framework". Commercial information systems that incorporate federated learning are being created by big as well as small technology companies. Both of these types of FL are employed as instances, as they are especially common and important, but these characteristics could show up in various combinations in different FL situations. FL implementation requires consistent standards, and standard formulation initiatives are also ongoing in conjunction with the growing application (Thilakarathne et al. 2022). The year 2018 witnessed the official start of the creation of FL standards by an assortment of international organizations. Previously published architecture and functional standards have been created by IEEE and ITU-T. Standardization initiatives are also under way for both the safety requirements and technological uses of FL with multi-party safe computation.

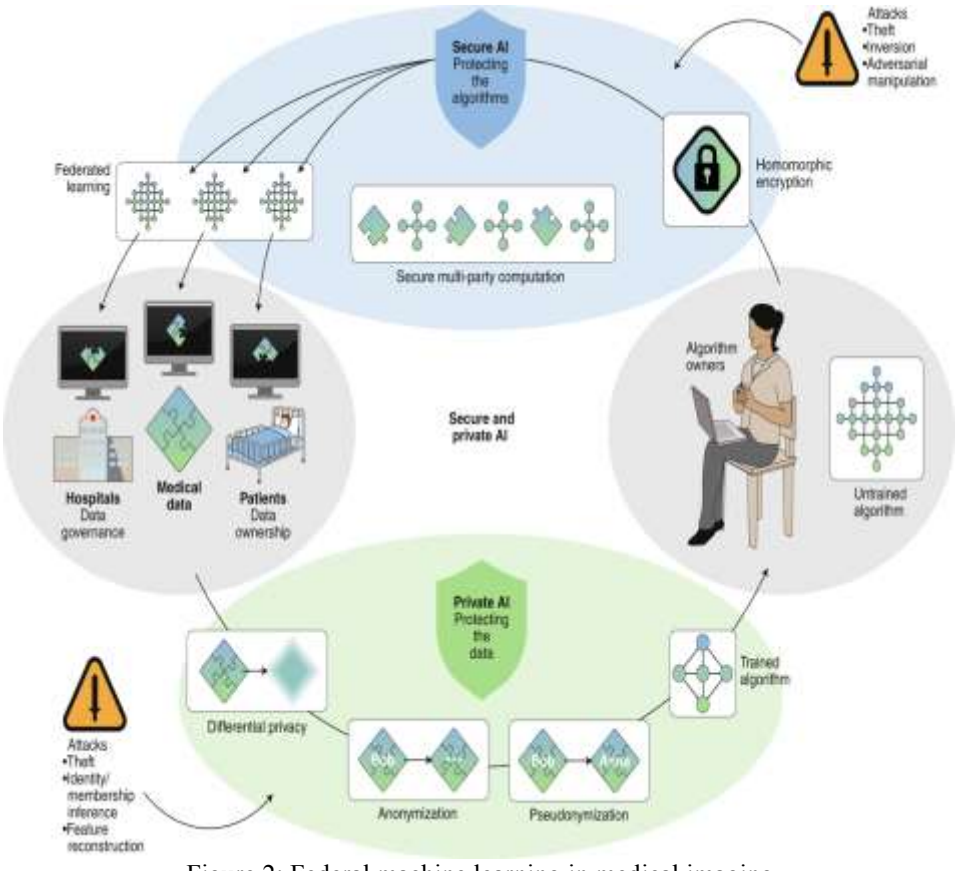

Figure 2: Federal machine learning in medical imaging
(Source: Thilakarathne et al. 2022)

The financial sector and the Internet of Things merely represent a few instances of data-intensive industries that must go through a digital transformation quickly. In most cases, their data flow applications are on an enormous scale, and they offer more stringent requirements to ensure security. In order to achieve effective information integration and consumption, it is essential for these traditional industries to establish a safe and confidential information flow (Xu et al. 2021). Therefore, Florida may be an excellent choice to encourage the digital growth

of established companies and guarantee a safe and compliant transfer of data. As advances in FL uses and techniques keep growing, it simultaneously grows the intricacies of the issues that such advancements are intended to solve.
Federated learning has emerged as a ground-breaking approach in the field of machine learning, offering the promise of privacy-preserving model training while maintaining the utility of centralized models. Over the past few years, significant advancements have been made in federated learning techniques, addressing various challenges and making it a viable solution for industries and applications where data privacy is paramount.

One key advancement in federated learning is the development of more efficient algorithms. Early federated learning models suffered from high communication overhead, making them impractical for large-scale deployments. Researchers have since introduced novel techniques like federated averaging, which enables model updates to be aggregated efficiently, reducing the communication burden on participating devices. This advancement has made federated learning feasible for resource-constrained devices, such as smartphones and IoT devices, where data privacy is crucial (Thilakarathne et al. 2022). Privacy preservation in federated learning has also seen substantial progress. Differential privacy, a mathematical framework for ensuring privacy in data analysis, has been integrated into federated learning algorithms. This approach allows organizations to protect individual data points while still benefiting from aggregated insights. Adding noise to model updates or applying privacy-preserving aggregation techniques, federated learning systems can achieve strong privacy guarantees without compromising the accuracy of the trained models.

2. MATERIALS AND METHODS

Research philosophy
The pragmatic theory of research was chosen for the present investigation among other potential methods. Researchers who employ a practical strategy in their work employ study designs that include practical decisions that reflect 'what will work best' in addressing the inquiries at hand (Mendling et al. 2021). This enables them to carry out research in novel and exciting manners to discover and carry out solutions to research difficulties. Pragmatism argues for a focus on practical uses in the study of science. The objective here is to employ federated methods of learning to enhance privacy-preserving machine learning. Through placing an emphasis on practical issues, one can be more realistic. The primary objective of pragmatism is to identify practical issues and efficient remedies for real-world issues (Bloomfield & Fisher, 2019). In order to address concerns about confidentiality in the field of machine learning, researchers have looked into federated methods of learning, which use a problem-based strategy. Pragmatism encourages the use of various solutions to an issue. It encourages the combination of both quantitative and qualitative methods with the goal of addressing the research problem.

Research design
For the purpose of this study, researchers decided to take a method that is called experimental research design. The objective of an experimental study design is to assess the effect of altering any number of independent variables on one or more of the dependent ones. These kinds of investigations serve a purpose for testing hypotheses, exploring unknown waters, and developing conceptual structures as they demonstrate cause-and-effect connections between factors (Planas & Alfonso, 2023). Researchers may acquire greater awareness of complicated phenomena, including buying decisions and social relationships, through the use of experimental research techniques. Researchers have to take into consideration moral issues, including informed consent and fraud, while designing studies. In the beginning, it is essential to create clear, verifiable theories on the effectiveness of recent advances in federated learning techniques for preserving user confidentiality in machine learning. In order to minimize the likelihood of prejudice and guarantee accurate outcomes, it is preferable to randomly distribute datasets or people to each group of experiments.

Figure 3: Research design
(Source: Planas & Alfonso, 2023)

Research approach

The researcher chose the approach known as inductive over the deductive approach. The objective of inductive research is to create and evaluate hypotheses regarding an issue or circumstance based on what has been observed. In inductive research, the acquired data is used to develop a hypothesis about the root cause of the data, as compared to deductive research, which begins with an idea and then builds up data and observations to verify the hypothesis (Ghio et al. 2021). As researchers use inductive tactics, they go beyond existing concepts and structures to find and comprehend previously overlooked trends, patterns, and discoveries. This is a great help when working with modern tools and methods. There might not be an extensive body of research or widely recognized theories that can be built to expand in the field of privacy-preserving algorithmic learning along with federated learning. An inductive approach is employed when researchers must begin with no preconceived ideas or preconceptions in order to gather real data and develop novel hypotheses or models according to observed trends or behaviors.

Data collection

For this particular study, the researchers decided to use secondary data collection. Secondary data is able to be obtained from an extensive range of locations, such as books, interviews, internet-based databases, and archives. The accessible nature of secondary data is frequently mentioned as an important benefit over primary data. Utilizing these assets involves nothing in the way of investigation or effort (Rodriguez et al. 2021). The growing number of electronic media and the widespread accessibility of the internet allowed for the spread of secondary data. It is fairly straightforward to get access to secondary sources of data. Secondary study techniques have developed due to the Internet. A great deal of secondary resources is either entirely free for users or quite affordable. It is effective both in terms of time and money.

Figure 4: Data collection
(Source: Rodriguez et al. 2021)

Data analysis

The present study involves the most secondary qualitative data. The objectives of qualitative investigation vary from those of quantitative studies. Researchers who employ a qualitative method in their research have an interest in the particulars of their informants' experiences. After gathering, contrasting, and assessing the responses of the sources, judgments can be reached. The reason behind an event, correlation, or behavior frequently constitutes the primary focus of a qualitative study. Researchers may employ qualitative data to learn more about the components that influence the adoption and achievement of federated methods of learning in different settings. This background is essential for understanding the real-world consequences of these approaches. Methods for qualitative study can be adjusted to accommodate a variety of circumstances. As the research progresses and additional data emerges, researchers may modify their methodology and queries appropriately. Qualitative analysis of data is often hard and requires an understanding of specific methods.

3. RESULT AND DISCUSSION

Using non-IID data, it is harder to train a single worldwide model upon a collection of customer datasets, which was the original purpose of federated learning. In order to achieve this objective more effectively, it only seems logical to develop or modify current algorithms. Data augmentation for standardizing information among users is an option in certain situations. In this case, one option is to create a small dataset appropriate for global dissemination (Han et al. 2022). This dataset might have originated from a freely accessible proxy data source, a dataset that is not responsive to user privacy, or an extraction of the original information. The most basic division is between the two distinct categories of presuming IID and non-IID information for the per-client routines getting optimized.

In order to be more specific, having IID data for the clients' means that every mini-batch of information utilized in the client's localized updates is statistically comparable to a randomly selected sample from the entire training dataset. As each client gathers its own unique training data, which differs in amount and shipping, and fails to share it with other clients or the main node, it is clear that the IID assumption hardly applies in reality. But using this assumption makes theoretical convergent analysis of federated optimization algorithms a lot easier (Peyvandi et al. 2022). It also gives us a way to look at how non-IID feedback affects the efficiency of optimization. Therefore, it is important to begin by learning about the wide range of optimization techniques available for the IID data situation.

$$\min_{x \in \mathbb{R}^m} F(x) := \mathop{\mathbb{E}}_{z \sim \mathcal{P}} [f(x; z)].$$

Researchers have thought about a model of intermittent communication that is similar to the one that was proposed. In this model, M stateless customers take part in each of the T phases, and in each round, each client can figure out shifts for K samples that are "z1,..., zK sampled IID from P". Moreover, without compromising generalization, researchers may presume M = N in the IID-data setting, where clients are regarded as replaceable. The assurances that are issued will differ according to the assumptions established regarding.

Researchers have examined several kinds of "multi-model" methods or techniques that eventually lead to the effective utilization of numerous models for various customers during the inferential phase.

In dealing with non-IID data, these techniques can be particularly helpful as they have a chance to surpass even the best possible worldwide shared model (Darzidehkalani et al. 2022). Techniques allowing for independent inference sessions with user-specified parameters for the model are also discussed by the researchers. However, in other cases, essentially incorporating user and environmental variables into the model can yield identical benefits. As numerous customers have varied language behaviors, on-device modification of the model's settings has been effective in addressing this problem.

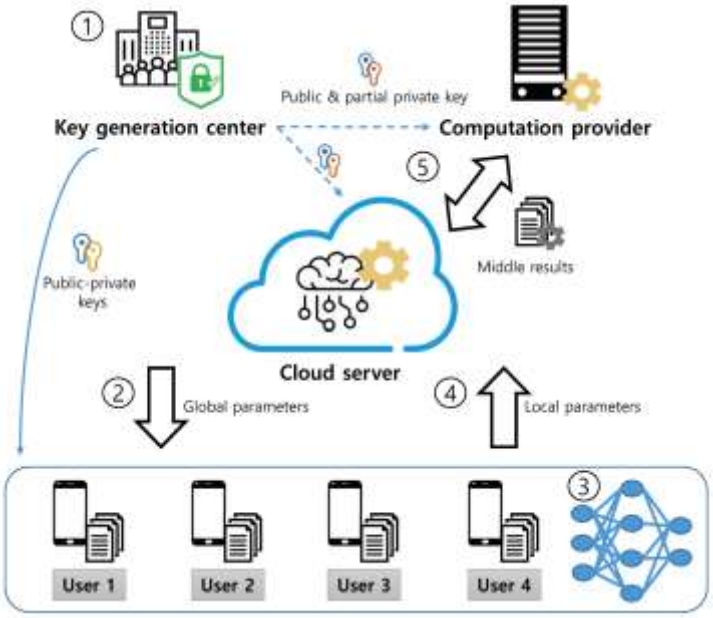

Figure 5: Federal machine learning for homomorphic encryption
(Source: Darzidehkalani et al. 2022)

Through the right modifications, a single global model can produce individually specific expectations for every single client. However, as few datasets that are freely accessible include such additional features, it continues to be an important unresolved topic of identifying ways to incorporate contextual data for different duties in FL-trained models. Methods from multi-task training become immediately useful if one considers each client's localized problem as an individual assignment. The MOCHA algorithm, created by Smith et al., is a prominent example of a work in multi-task federated learning that addresses issues related to communication efficiency, losers, and tolerance for faults (Fang & Qian, 2021).
One model has been developed for every procedure in multi-task learning. Due to the fact that each client is developing its own independent approach, most multi-task training techniques require autonomous clients. This is the reason these methods work well in cross-FL silo scenarios but are harder to carry out in real-life scenarios with multiple devices. A different approach is to reconsider the relationship between consumers and training tasks, based on the understanding that there is a continuum between employing a single global model and customizing responses for every individual user (Yang et al. 2023). Choosing the task to be performed on a selected group of the clients, possibly chosen explicitly or maybe centered on grouping or the interconnected parts of a learned graph with respect to the clients, could be a prime instance.

In addition, when researchers talk about "local fine tuning," they are talking about methods in which a single model is created through federated training and then sent to all clients, where it is changed even more by initial training on the current dataset before it is used in inference. This approach fits smoothly into the federated learning model lifecycle. The global model is able to be trained with a relatively small number of clients each round; the global model is only distributed to all clients briefly after distribution. The only difference is that a final training process takes place, customizing the model to the current dataset before it is used to make immediate forecasts for the consumer. Fine-tuning, transfer learning, domain modification, and interpolation using a local model are frequently employed in nonfederated learning (Thompson, 2019). In the setting of federated learning, it is essential to determine the precise approach used to perform this interpolation and to get its accompanying training guarantees. Some of the more refined structure of federated learning can also get lost, as those techniques generally assume only two domains: target and source.

The subject of cryptography, referred to as "Secure Multi-Party Computation (MPC)", focuses on the difficulty of enabling multiple parties to collaboratively compute an expression of their secret input in a manner that only exposes the result they want to the interested parties. A problem with communicating real numbers is that most encryption techniques rely on actions in limited areas. In order to avoid uncontrollable underflows, it is typical to modify ML models along with training techniques to function with values that are normalized and rely on precise quantization. Any function can be computed safely, even in the presence of opponents who plan harm, and this has been recognized for decades. Although problems have general clarification, these solutions tend to be impractical due to their ineffectiveness. The latest focus in the field of science has been to create specialized protocols with particular uses, such as in logistic and linear regression and neural networks for inference and

training. These initiatives frequently take place in a cross-silo situation, or an arrangement in which analysis is assigned to a network of computers that do not collaborate in their efforts.

These protocols require significant communication, making it challenging to migrate them to the cross-device scenario. A small part of the federated learning procedure could be moved to an authorized setting in the cloud, whose code can be approved and verified through the use of trusted execution environments known as TEEs, or secure enclaves. TEEs may provide many essential characteristics for establishing trust in the correct and private execution of a piece of code. Confidentiality is the status of the code's operation that remains private until the code itself chooses to make the data public. The integrity of the code implies that there is no other way to alter its operation besides the user's involvement. In the case of measuring or attestation, the TEE can demonstrate to a third party how the binary code is currently running and the state it was placed in before execution began, thus providing the basis for security and confidentiality.

The features that are accessible in many TEE executions are "Intel's SGX-enabled CPUs", "Arm's TrustZone", and "RISC-V's Sanctum". Though "Tramer and Boneh" explore ways to connect TEEs with GPUs for machine learning inference, existing secure enclaves impose limitations on memory and enable accessibility only to the resources of the CPU, indicating that they prohibit computation on GPUs or machine learning computers. It is also challenging for TEEs to entirely prevent any and every kind of side channel threat.

Although safe enclaves do indeed protect all code executed inside them, there are additional considerations that must be taken into consideration in their actual application. For example, the code run within the enclave must frequently be designed as a data-oblivious handle so that its execution environment and memory access patterns hide information about the information upon which it performs computations. In order to add insult to damage, measurement or attestation typically only proves that a specific binary is running and it is the responsibility of the system's architect to offer a method for proving that a binary has the needed confidentiality properties, which might require the binary to be constructed using an accurate process from open-source code.

4. CONCLUSION

Federated learning removes the possibility of performing machine learning from the need to store information in the cloud by enabling distant client devices to collaborate and create an integrated prediction model while keeping every bit of training information on the device. This expands the capacity of mobile devices beyond prediction by integrating model training onsite. Both the corporate world and educational institutions have witnessed an unprecedented increase in interest in this field in recent years. A number of companies have been established with the objective of using federated learning to tackle privacy and data collection concerns in various sectors, and numerous big technology companies are currently using federated learning in operation. Additionally, the diversity of articles assessed in this work indicates that federated learning has begun to gain traction in an array of interdisciplinary areas, which include but are not limited to machine learning, optimizing, statistics, information theory, cryptography, fairness and privacy.

References

Alazab, A., Khraisat, A., Singh, S., & Jan, T. (2023). Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. *Electronics*, *12*(16), 3382. https://doi.org/10.3390/electronics12163382

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses Association*, *22*(2), 27-30. https://search.informit.org/doi/abs/10.3316/INFORMIT.738299924514584

Darzidehkalani, E., Ghasemi-Rad, M., & van Ooijen, P. M. A. (2022). Federated learning in medical imaging: part I: toward multicentral health care ecosystems. *Journal of the American College of Radiology*, *19*(8), 969-974. https://doi.org/10.1016/j.jacr.2022.03.015

Dash, B., Sharma, P., & Ali, A. (2022). Federated learning for privacy-preserving: A review of PII data analysis in Fintech. *International Journal of Software Engineering & Applications (IJSEA)*, *13*(4). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323967

Fang, H., & Qian, Q. (2021). Privacy preserving machine learning with homomorphic encryption and federated learning. *Future Internet*, *13*(4), 94. https://doi.org/10.3390/fi13040094

Ghio, D., Greenwell, K., Muller, I., Roberts, A., McNiven, A., & Santer, M. (2021). Psychosocial needs of adolescents and young adults with eczema: a secondary analysis of qualitative data to inform a behaviour change intervention. *British journal of health psychology*, *26*(1), 214-231. https://doi.org/10.1111/bjhp.1246.

Girgis, A., Data, D., Diggavi, S., Kairouz, P., & Suresh, A. T. (2021, March). Shuffled model of differential privacy in federated learning. In *International Conference on Artificial Intelligence and Statistics* (pp. 2521-2529). PMLR. https://proceedings.mlr.press/v130/girgis21a.html

Han, G., Zhang, T., Zhang, Y., Xu, G., Sun, J., & Cao, J. (2022). Verifiable and privacy preserving federated learning without fully trusted centers. *Journal of Ambient Intelligence and Humanized Computing*, 1-11. https://link.springer.com/article/10.1007/s12652-020-02664-x

Mendling, J., Berente, N., Seidel, S., & Grisold, T. (2021). The philosopher's corner: Pluralism and pragmatism in the information systems field: The case of research on business processes and organizational routine. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *52*(2), 127-140. https://doi.org/10.1145/3462766.3462773

Peyvandi, A., Majidi, B., Peyvandi, S., & Patra, J. C. (2022). Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0. *Multimedia tools and applications*, *81*(18), 25029-25050. https://link.springer.com/article/10.1007/s11042-022-12900-5

Planas, N., & Alfonso, J. M. (2023). Secondary-school teachers' noticing of aspects of mathematics teaching talk in the context of one-day workshops. *The Journal of Mathematical Behavior*, *71*, 101084. https://doi.org/10.1016/j.jmathb.2023.101084

Rodriguez, L., Crossman, J., & Bordia, S. (2021). An interdisciplinary approach to secondary qualitative data analysis: what why and how. In *Handbook of qualitative research methodologies in workplace contexts* (pp. 133-156). https://doi.org/10.4337/9781789904345

Thilakarathne, N. N., Muneeswari, G., Parthasarathy, V., Alassery, F., Hamam, H., Mahendran, R. K., & Shafiq, M. (2022). Federated Learning for Privacy-Preserved Medical Internet of Things. *Intell. Autom. Soft Comput*, *33*(1), 157-172. DOI:10.32604/iasc.2022.023763

Thompson, S. (2019). The power of pragmatism: how project managers benefit from coaching practice through developing soft skills and self-confidence. *International Journal of Evidence Based Coaching and Mentoring*, (S13), 4-15.DOI: 10.24384/86ee-ps25

Truong, V. T., & Le, L. B. (2023). MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse based on Blockchain and Online Federated Learning. *IEEE Open Journal of the Computer Society*. https://ieeexplore.ieee.org/abstract/document/10239541/

Xia, Q., Ye, W., Tao, Z., Wu, J., & Li, Q. (2021). A survey of federated learning for edge computing: Research problems and solutions. *High-Confidence Computing*, *1*(1), 100008. https://doi.org/10.1016/j.hcc.2021.100008

Xu, R., Baracaldo, N., & Joshi, J. (2021). Privacy-preserving machine learning: Methods, challenges and directions. *arXiv preprint arXiv:2108.04417*. https://arxiv.org/abs/2108.04417

Yang, L., He, J., Fu, Y., & Luo, Z. (2023). Federated Learning for Medical Imaging Segmentation via Dynamic Aggregation on Non-IID Data Silos. *Electronics*, *12*(7), 1687. https://doi.org/10.3390/electronics12071687

Zhang, L., Zhang, Z., & Guan, C. (2021). Accelerating privacy-preserving momentum federated learning for industrial cyber-physical systems. *Complex & Intelligent Systems*, *7*, 3289-3301. https://link.springer.com/article/10.1007/s40747-021-00519-2.