Informatics Bulletin, Faculty of Computers and Artificial Intelligence, Helwan University
Published Online ***Vol 7 Issue 1, January 2025***
(https://fcihib.journals.ekb.eg)

Federated Learning: A Literature Review on Decentralized Machine Learning Paradigm

Menna Mamdouh Orabi[1], Osama Emam[1], Hanan Fahmy[1]
[1]Information System Dept., Faculty of Computers and Artificial Intelligence, Helwan University, Egypt
menna.mamdouh@fci.helwan.edu.eg, osama_emam@@fci.helwan.edu.eg, hanan.fahmy@fci.helwan.edu.eg

***Abstract* — Federated Learning (FL) refers to a groundbreaking paradigm for distributed machine learning (ML), ensuring model training without compromising the privacy of local data. Despite its promise, FL suffers from some challenges, involving concerns over direct data leakage, the potential of compromising the model architecture privacy, and the overheads associated with connection and communication. This paper shows an in-depth study of FL, and its categorization according to the data partitioning formats such as horizontal FL, vertical FL, and federated transfer learning. A thorough examination of FL models is given, highlighting the need to incorporate strong privacy and security protections inside FL frameworks and illuminating the inherent difficulties these models present. The paper also examines previous research on FL, on how integrating security techniques to improve FL systems' general effectiveness. By consolidating current knowledge, the paper provides a roadmap for future directions, highlighting the possible solutions in mitigating challenges and advancing privacy-preserving federated learning.**

***Index Terms*— Machine Learning, Federated Learning, Privacy, Security**

I. Introduction

Recently, the increase of interconnected machines has generated massive data, commonly stated as big data. This rise in data generation, combined with growing concerns about privacy and devices' computational capabilities, has led to an imperative for localized data processing and storage [1], [2]. Artificial intelligence (AI) emerges as a pivotal element in unlocking the full potential of big data, steering the trajectory of machine intelligence and infrastructure efficiency toward an imminent future. ML constitutes a vital branch of AI, employing computational systems for making sense of data through pattern extraction, data fitting to functions, and data classification. ML systems possess the capability to learn and enhance their performance over time through the assimilation of historical data and accumulated experience. They depend on centralizing data in a singular location, typically within a central cloud data center [3], [4]. However, the conventional approach in machine learning involves consolidating data in a central cloud data center, a practice that raises significant concerns regarding the privacy of users and data confidentiality, as underscored by rules like The European Union's General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA)[5] [6]. The crucial importance of security and privacy in applications of technology has led to a paradigm change towards decentralization, to be applied in data collection and processing operations. FL provides a pivotal role for mitigating concerns regarding to security and privacy of data in the filed of ML. This innovative approach enables training the model locally on different devices independently, ensuring that sensitive data never quits its source. By decentralizing the learning process, federated learning minimizes the risks connected to centralized data storage and transmission. This not only safeguards user privacy but also addresses the potential vulnerabilities associated with data breaches. Federated learning fosters a collaborative model where machine learning models are trained collectively from decentralized data sources, promoting a more secure and privacy-preserving environment in the rapidly evolving landscape of artificial intelligence [7]. This paper introduces a study about the idiom, benefits, and categorization of FL and understands the issues related to FL.

Furthermore, The remainder of this paper is structured into four sections: Section II offers background about the main concepts, including machine learning, and federated learning. Section III shows a detailed overview of federated learning methodology. Section IV discusses the literature review with the main findings and presents the appropriate guidelines for further research directions in recent literature. Section V conclusion of this paper.

II. Background

This section highlights the essential points discussed in this research paper, including the hierarchy from centralized ML to FL signifies a change in the way ML models are trained and deployed.

Machine learning is an aspect of AI which enables machines to learn from historical data regardless of explicit programming. Its widespread application has significantly impacted various aspects of human life by utilizing large volumes of daily generated data to train models, enhancing the quality of services[8]. The process involves collecting reliable data, identifying patterns, preprocessing data, training models, evaluating them, tuning hyperparameters, and deploying

predictions. Techniques of ML like supervised, unsupervised, semi-supervised, and reinforcement learning, enable computers for autonomously learning and making predictions[9]. Figure 1 presents the workflow of ML by running on the cloud as a centralized location to train the model according to the collected data, so it achieves getting a generalization model with the need for a high level of stable communication channel and saving the data privacy. However, challenges arise, including the potential strain on communication resources during data transmission and concerns about privacy breaches when raw data is transferred to central servers to train the model[10]. The key factors for a successful machine learning model are security and data privacy, essential for optimal performance and usefulness in future predictions[11].

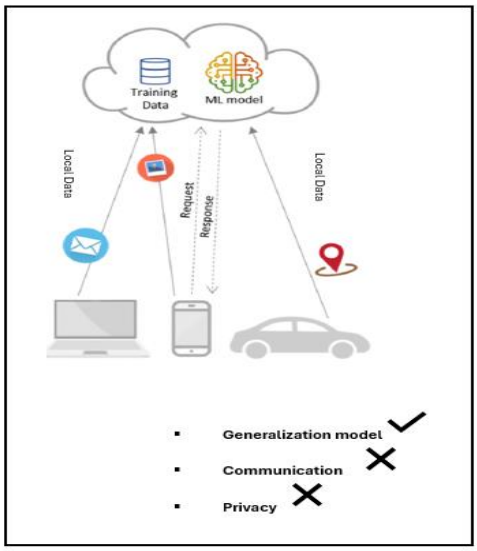


Figure 1:Machine Learning Workflow

A. Distributed on-site Learning

Distributed on-site Learning refers to a system where learning processes, particularly those comprising machine learning or data analysis, are spread over various on-site or local devices rather than being centralized. This methodology can involve training models on data available locally at various distributed locations, promoting privacy, reducing data transmission requirements, and addressing latency concerns. It might incorporate concepts from distributed systems and machine-learning techniques that operate on local data sources[12] [13].

Figure 2 presents the workflow of this methodology where each device builds its model depending on its local dataset, just gets the model from the cloud source, and then no communication channel is needed between them. The main advantages of this methodology are the ability of models to adapt to changes over time, the lack of dependence on an internet connection, and no need to upload private information to the cloud.

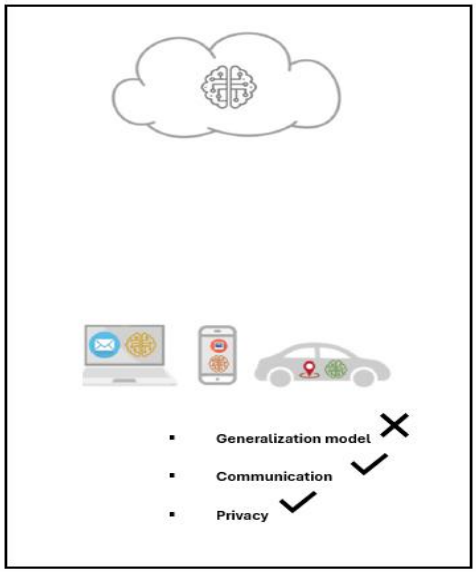


Figure 2: Distributed on-site Learning Workflow

B. Federated Learning

FL is a groundbreaking technique of ML which revolutionizes traditional centralized models. Unlike conventional methods where data is gathered and processed in a centralized server, federated learning distributes the learning process across decentralized devices. This innovative paradigm allows devices such as smartphones, IoT-connected devices, or servers to train a shared machine-learning model without sharing data[12][13].

In federated learning, the model is initially generated on a central server and then sent to individual devices. These devices process the model locally using their respective data and only share the model updates, instead of the actual data, back to central server. This privacy-preserving technique addresses concerns about the security and privacy of data, because of the sensitive information remains on users' machines[12]. Figure 3 presents the workflow of FL and how it offers several advantages, including reduced communication costs, enhanced privacy, and the ability to learn from diverse datasets without centralized data aggregation. This approach is especially valuable in scenarios in which data is decentralized, like in healthcare, finance, or edge computing environments, fostering collaborative machine learning while keeping privacy and data security[14].

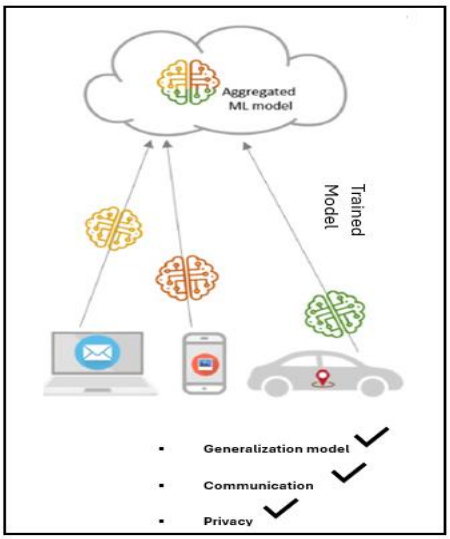


Figure 3:Federated Learning(FL) Workflow

Table 1 shows the main differences between ML and FL based on centralization, data handling, communication, data privacy, and collaboration.

TABLE 1
MACHINE LEARNING VS. FEDERATED LEARNING

	Machine Learning	Federated Learning
Centralization	Centralized processing	Decentralized learning
Data Handling	Large, centralized dataset	Diverse datasets on individual devices
Communication	Constant communication with a central server	Reduced communication with only model updates
Privacy	Potential privacy concerns	Privacy-preserving with only model updates shared
Collaboration	Limited collaboration due to centralization	Enables collaborative learning without central data aggregation

The shift from centralized to FL is prompted via the necessity for privacy-preserving ML, especially in applications like mobile devices, healthcare, and edge computing. FL allows model training avoiding disclosing raw data, making it suitable for situations where data cannot or should not be centralized. The choice between centralized, distributed, decentralized, or federated learning depends on factors such as privacy requirements, data distribution, and communication constraints.

III. FEDERATED LEARNING METHODOLOGY

In the next section, the focus will be on the details of FL methodology, its classifications, and applications adopted by recent studies to get the benefit of FL .

A. Federated Learning workflow

Federated Learning is defined as a machine learning technique which allows a model to be trained across various decentralized devices or servers keeping local data samples without sharing them [15]. This enables the training of models without centralizing sensitive data. Figure 4 presents a detailed workflow of FL:

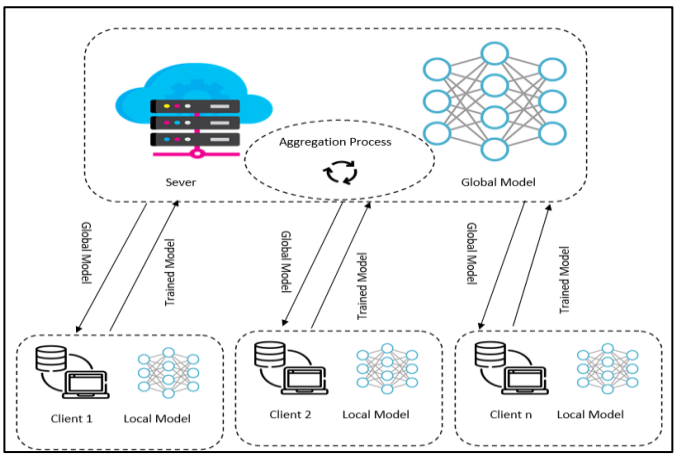


Figure 4: A detailed workflow of Federated Learning

This detailed workflow highlights the key steps as following [13][16][17]:

Initialization: Select the model architecture and hyperparameters that will be used for training. Initialize a global model on a central server or in a cloud environment.

Data Partitioning: Distribute the data across multiple machines or servers. Each machine keeps an aspect of the dataset, and the data remains localized, preventing the necessity for it to be sent to a central server.

Local Model Training: Each device performs local model training depending on its data. This involves computing the gradient of the model parameters concerning the local data and updating the local model.

Model Update Aggregation: After the process of local training, the local models' parameters are not centrally transmitted to the server. Instead, only the model updates (gradients) are transmitted. Aggregation functions such as federated averaging or secure aggregation are used for combining these updates into a global update without exposing the individual updates.

Global Model Update: The aggregated global update is employed as the global model, updating its parameters. This step ensures that the global model improves based on the knowledge learned from all corporating machines.

Communication Rounds: Steps 3-5 are recurred for a predetermined set of communication rounds. During each round, the machines perform local training, send modifies to the central server, and the server updates the global model.

Model Evaluation: Periodically, the global model's performance is assessed on a validation set to monitor its generalization to new data and to ensure that it is learning meaningful patterns.

Termination Criteria: The training process progresses until a predefined convergence criterion is matched, like achieving a certain degree of accuracy or after a fixed number of communication rounds.

Model Deployment: Once training is complete, the final global model can be performed for making predictions on new data. The model can be used on the central server or published to the local machines, depending on the application.

Privacy and Security Measures: Throughout the process, privacy and security measures must be in place to protect sensitive information. Techniques like differential privacy, secure aggregation, and encryption can be performed for enhancing privacy.

Federated Learning presents a powerful paradigm to train ML models in a decentralized manner, leveraging the incorporative knowledge across various machines while preserving data privacy[18]. The workflow involves initializing a global model, partitioning data across local devices, and iteratively exchanging model updates without exposing raw data. This collaborative approach enables the creation of robust models without centralizing sensitive information.
The iterative nature of communication rounds and model updates allows the global model to learn from diverse data sources, leading to enhanced generalization and performance. Privacy and security measures, like differential privacy and secure aggregation, play a vital role in assuring the protection of sensitive information throughout the training process[19].

Federated Learning finds applications in scenarios where data is distributed across devices or entities, such as mobile devices, edge devices, or in healthcare settings. The deployment of the final model can occur centrally or be distributed, depending on the use case[20].

Despite its promising advantages, Federated Learning also poses challenges, including communication overhead, potential model performance disparities across devices, and the need for robust privacy-preserving techniques. Ongoing studies and development are required to overcome these issues and improve the FL framework[21].

In summary, Federated Learning stands as a roadmap of ML, privacy, as well as distributed systems, offering a promising avenue for collaborative model training while respecting the privacy concerns inherent in decentralized data environments. As technology continues to evolve, federated learning is poised to become an integral part of the machine learning landscape, facilitating the development of robust and privacy-aware models across various domains.
Figure 5 summarizes and presents the main advantages and disadvantages of machine learning and federated Learning.

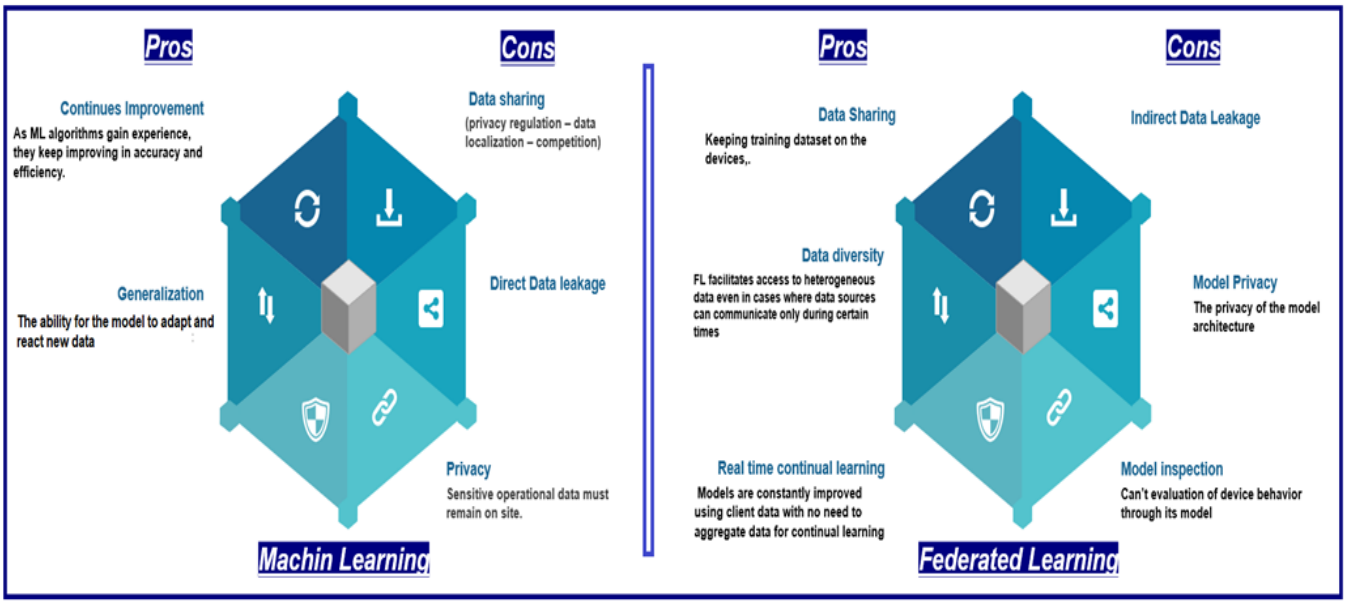
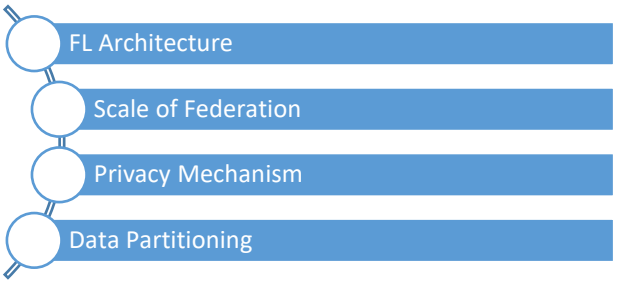


Figure 5: Pros and Cons of Machine Learning Vs Federated Learning

B. Federated Learning Classification

Different factors affect FL classification which impacts the performance and effectiveness of federated learning classification including architecture alternatives, data partitioning, machine learning model, scale of federation, and privacy mechanisms.



1) Architecture Alternatives

The federated learning can be implemented using different architectural approaches representing different organizational structures for implementing FL systems as following centralized, hierarchical, regional, and decentralized[22][23]:

i. Centralized Architecture[22]:

- Characteristics**:** In a centralized architecture, a single central server or coordinator manages the entire federated learning process.
- Workflow**:** The central server is in charge of aggregating and coordinating the learning models from all collaborating machines in the network.
- Advantages**:** Simplicity in coordination and model aggregation. The central server has complete control and visibility over the learning process.
- Challenges**:** Privacy concerns may arise as all raw data may need to be transmitted to the central server, raising potential security issues.

ii. Decentralized Architecture[12]:

- Characteristics: During a decentralized architecture, there is no central server or coordinator. Each participating device or node communicates directly with others.
- Workflow: Nodes collaborate directly for model updates without a central coordinator. This can be achieved through techniques like peer-to-peer communication.
- Advantages: Maximized privacy as there is no need for a central entity to have access to raw data. It can be more resilient and scalable in certain scenarios.
- Challenges: Communication and coordination can be challenging in a fully decentralized setup. Ensuring convergence and model consistency without a central entity requires sophisticated algorithms.

iii. Hierarchical Architecture[24]:

- Characteristics: The hierarchical architecture introduces a multi-level structure, with different levels of coordination. It may include multiple levels of servers or coordinators.
- Workflow: Higher-level coordinators may aggregate information from lower-level ones, and the process continues until reaching the top-level coordinator.
- Advantages: Provides a balance between centralized control and distributed processing. It can be useful for managing large-scale federated learning systems.
- Challenges: Increased complexity in coordination compared to the centralized approach. The design of the hierarchy may impact communication efficiency.

iv. Regional Architecture[25]:

- Characteristics: In a regional architecture, the federated learning system is divided into regions, each with its own coordinator.
- Workflow: Coordinators at the regional level manage the federated learning within their respective regions. They may interact with each other to exchange global model updates.
- Advantages: Can enhance scalability and reduce communication overhead compared to a purely centralized approach. It allows for more localized control.
- Challenges: Coordination between regional coordinators and maintaining a globally consistent model can be challenging.

Each architecture has its own trade-offs in terms of communication efficiency, scalability, privacy, and complexity. The selection of architecture often based on the specific needs and limitations of the FL application.

2) Scale of Federation

The scale of federation refers to the extent of collaboration and the complexity of the federated learning system. As the scale increases, challenges related to communication, heterogeneity, and privacy become more prominent and need careful dedication in the design and execution of FL systems[21]. The federation scale is divided mainly into two categories which are cross-silo and cross-device. In the context of cross-silo and cross-device federated learning, it involves understanding the scope and complexity of collaboration across different organizational silos and diverse types of devices[26].

3) Privacy Mechanism

Privacy mechanisms in FL aim to preserve the privacy of individual data whilst facilitating collaboration model training over decentralized devices. Key mechanisms include local model updates (sharing only model updates, not raw

data), differential privacy (adding noise to prevent individual identification), secure aggregation (ensuring private aggregation of updates), homomorphic encryption (allowing computations on encrypted data), and adaptive strategies for participant selection and learning rates. These mechanisms collectively help maintain privacy in federated learning by preventing unauthorized access to sensitive information and ensuring that the collaborative model training process is secure[21][17].

4) Data Partitioning

Data partitioning is the distribution or division of data among several devices or nodes in a decentralized network. Data partitioning is a crucial aspect of federated learning as it determines how the data is divided among these devices. The main types of data partitioning are horizontal, vertical, and transfer-federated learning. Horizontal federated learning focuses on distributing samples across devices, vertical federated learning partitions features and transfer learning involves leveraging pre-existing knowledge to enhance model performance in federated learning[28][29]. These strategies collectively contribute to the cooperation and privacy-preserving nature of FL, and they are considered the main categories of FL.

C. Federated Learning Categories

FL is categorized according to the way that data is partitioned in sample spaces, which are client devices that send data to the central server, and feature spaces, which are the key characteristics used to categorize the available data set in the system to main three categories: horizontal data partitioning, vertical data partitioning, and hybrid data partitioning, also known as federated transfer learning. Figure 6 illustrates the three types of FL which are horizontal FL, vertical FL, and federated transfer learning[30][31].

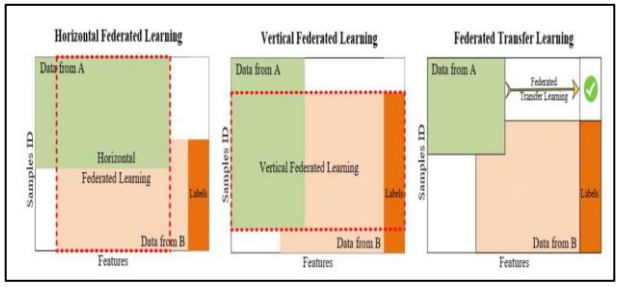


Figure 6: Categories of FL[30]

1) Horizontal Federated Learning:

In horizontal federated learning(HFL), each device has different samples of the same features (columns), and the main aim is to learn a global model overt all machines, where the participant's devices share the same features but with the little intersection of sample space, for example, the dataset for medical conditions from hospitals and clinics[16][32]. The training technique here includes a set of steps, as presented in Figure 7:

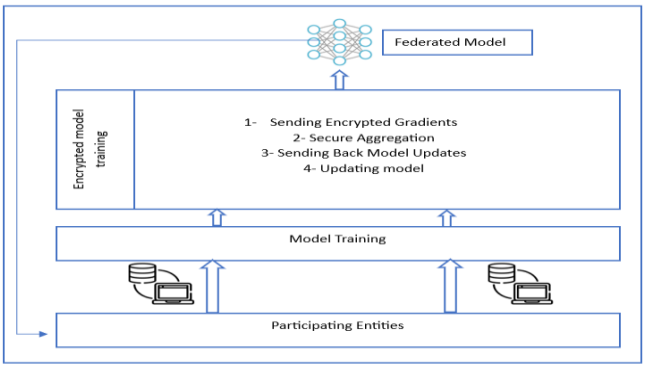


Figure 7: HFL Workflow

i. Participants compute training gradients locally, mask them via encryption process, differential privacy, or secret sharing, and then transmit the masked results to the server.

ii. The aggregator machine ensures the security level of aggregation while keeping participant information private.

iii. The aggregator distributes the aggregated model to participants.

iv. Participants update their trained model with decrypted gradients.

2) Vertical Federated Learning:

In vertical federated learning(VFL), dataset samples across different devices or servers have complementary feature sets. Each device possesses unique features, and collectively, they form a complete feature space[12][32]. The training technique here includes a set of steps, as presented in Figure 8:

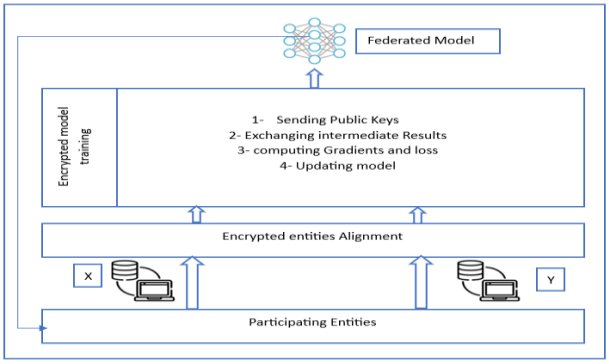


Figure 8:VFL Workflow

i. The authorized aggregator generates encryption pairs and sends public keys to entities x and y.

ii. X and Y encrypt and exchange intermediate values to calculate gradients and losses.

iii. X and Y generate an additional mask and encrypted gradients, respectively. Y also computes encrypted loss. X and Y transmit encrypted values to the aggregator.

iv. The aggregator sends decrypted gradients and the value

of loss to X and Y. The gradients are then unmasked by X and Y, which updates the model.

3) Federated Transfer Learning:

Federated Transfer Learning (FTL) merges the advantages of transfer learning and FL, catering to scenarios with decentralized data. Initially, a model is pre-trained on a central server using a rich dataset (source domain)[27]. This pre-trained model is then distributed to local devices or servers, each with its distinct dataset (target domain). The local models fine-tune themselves to their respective data, adapting to specific characteristics while preserving privacy. The aggregated knowledge from these localized models enhances the global model's performance without the need to share raw data centrally[33].

FTL proves invaluable in applications where data is distributed across various locations, striking a balance between leveraging prior knowledge and respecting data privacy.

These three categories represent different approaches to federated learning, addressing various scenarios where collaboration among decentralized entities is crucial. HFL works well in cases when entities have data with the same features but different samples, VFL suits scenarios where entities have complementary feature sets, and federated transfer learning enables knowledge transfer across domains for improved model performance. Each category addresses specific privacy and collaboration considerations, providing flexibility for diverse applications[20][32].

Table 2 summarizes the main comparison factors between these three categories.

TABLE 2
FL CATEGORIES

	HFL	**VFL**	**FTL**
Data Distribution	Each node has different samples with the same features.	Each node has different features, but the same samples.	Nodes have both different features and samples.
Sharing Data	Only model updates are shared, not raw data.	Shares only the necessary information for model training, maintaining privacy.	Shares model updates and may transfer learned features or representations.
Model aggregation updates	Aggregation typically involves averaging updates from different parties.	Aggregation can involve more complex operations depending on the shared samples and features.	Aggregation can involve various methods, including feature transfer or knowledge distillation.
Privacy	Well-suited for privacy preservation since raw data is not shared.	Privacy is maintained by sharing only necessary information, but still depends on the protocol.	Privacy-preserving, but the extent depends on the transfer learning approach.
Communication overhead	High	Low	depends on the type of transfer learning being used.
Complexity	Law	High	depends on the type of transfer learning being used and the domains involved.
Application	Healthcare	User- behavior analysis	Speech Recognition for Multilingual Applications

IV. LITERATURE REVIEW

Federated learning is gaining increasing attention, and it stands as a promising avenue for research with the potential to reshape various technologies and domains. Its ability to facilitate the training of machine learning models across decentralized devices, such as smartphones, edge machines, and Internet of Things (IoT) devices, without the necessity of centrally sharing raw data, has fueled its appeal. This distinctive approach not only addresses privacy concerns but also unlocks previously untapped big data sets [34]. Beyond privacy considerations, federated learning intersects with diverse technologies and fields, spanning healthcare, finance, and autonomous systems. In the healthcare sector, it facilitates collaborative model training on patient data from different hospitals, leading to enhanced diagnostic accuracy and personalized treatment recommendations. In the realm of autonomous systems[35][36], it plays a crucial role by enabling distributed learning among connected vehicles and edge devices, thereby improving overall safety and performance[37].

It is expected that there will be ongoing exploration of the combined use of FL with other technologies and fields, resulting in groundbreaking developments. This section presents a review of the current studies in the field of FL.

The selection between HFL and VFL in various fields depends on different factors such as the type of data distribution, specific use cases, and the scope of model application. Currently, the focus is on the HFL approach, where a substantial dataset is divided among multiple parties sharing a common feature space. Healthcare is the most popular field that accommodates both types of federated learning, depending on the case study. For example, if hospitals and healthcare providers work together to provide new models, horizontal federated learning can be most suitable for creating predictive models and persevering the localization of patient information [5].

Other applications of horizontal federated learning include Mobile keyboard prediction, and utilizing horizontal federated learning to enhance predictive text and autocorrect suggestions. Each user's typing data remains on their device and the aggregated model benefits from a diverse range of user behaviors [38]. Recommendation systems, employing horizontal federated learning for training recommendation models [39]. User interaction data contributes to improving recommendations without centralizing sensitive user preferences.

In other directions, VFL is applied to the applications in banks and financial institutions collaborating on financial fraud detection. Vertical federated learning allows organizations that have different data sets, such as transaction history and customer profiles, to collaborate to build a more accurate fraud detection model [40].

Vertical federated learning is used to optimize inventory management and demand forecasting in the field of supply chain where companies in various parts of a supply chain collaborate. Each company shares relevant data without sharing details [41].

The field of data analytics in the Internet of Things (IoT), where IoT devices generate data with different specs and characteristics. Vertical federated learning enables various device owners to cooperate on training the model without exchanging sensor data, thereby enhancing collective insights [42].

Li et al. [43] provided a detailed overview of FL, highlighting challenges and future directions. Major challenges include communication efficiency because of frequent interactions between the central server and other machines, especially in cases of large-scale or limited bandwidth. Privacy and security issues are increasing because of sharing models, posing risks such as adversarial attacks and data leakage. The presence of non-IID data across devices adds complexity to the training process. Addressing these challenges is crucial for the advancement of federated learning strategies.

Hard et al. [38] introduced a Coupled Input-Forget Gates (CIFG) model that trained using FL by demonstrating its advantage over the normal way of training based on a server-trained CIFG model and a baseline n-gram model in keyboard prediction for next-word. The study also explored federated learning's application in mobile keyboard prediction, addressing challenges related to device heterogeneity, such as varying computational power, battery life, and network connectivity. The authors highlighted the difficulties stemming from resource limitations, communication constraints, and uneven participation in federated learning, where not all devices contribute equally or consistently. Additionally, the paper discussed the complexities of model aggregation, emphasizing that inefficient or inaccurate methods can result in network overhead and synchronization issues, leading to suboptimal global models and slower convergence.

Mothukuri et al. [44] conducted an extensive examination of the security factors and privacy dimensions of FL. The study identified the limitations of communication, poisoning, and backdoor attacks as the primary security threats, with a particular emphasis on inference-based attacks being the high risk of FL privacy.

Y. Lu et al. [45] introduced a privacy-preserving federated learning mechanism, showcasing its application in training a machine learning model to identify cyber-attacks while maintaining data privacy. However, a notable limitation of this approach is its dependence on a central server to manage the FL process, posing a potential vulnerability if the central server becomes compromised.

Ji et al. [46] provided how different learning algorithms integrate with the FL framework, addressing main concerns such as the efficiency of learning and statistical heterogeneity. Termed as federated X learning, it delves into the fusion of FL with other paradigms like multitask learning, meta-learning, transfer learning, unsupervised learning, and reinforcement learning.

Current studies on federated learning lack sufficient consideration of security aspects in data exchange, exposing concerns about potential data leakage and the compromise of model privacy. The participation of multiple clients in FL models introduces vulnerabilities to various attacks on clients, servers, and communication channels.

To address these challenges, model development should follow the main information security principles—confidentiality, integrity, and availability (CIA).

In response to these concerns, some studies, such as Kurniawan et al. [47], have explored vulnerabilities in federated learning models. They identified issues like communication vulnerabilities, gradient leakage, client and server compromise and the vulnerabilities of aggregation algorithms. Additionally, the authors proposed a privacy-preservation scheme for active learning through encryption-based FL. While this scheme effectively addresses some vulnerabilities, it remains susceptible to issues like insecure communication channels, compromised clients, and compromised servers.

Liu et al. [48] presented an exploration of the risks, attacks, and defense mechanisms associated with Federated Learning (FL) throughout its entire process, categorized into three phases including auditing for the data and behavior, training, and prediction.

V. Conclusion

Federated Learning is a significant technology in achieving a high level of data privacy in machine learning by training models across decentralized devices. This paper focuses on introducing all aspects of federated learning and its potential. Also, it presents challenges of FL such as communication overhead, heterogeneity among devices, security concerns, and strategic behavior that must be addressed. Future work focuses on optimizing communication, enhancing security measures, exploring decentralized architectures, and addressing issues of compromising the model architecture's privacy. Overcoming these challenges and advancing research in these areas is important to get fully realize the benefits of FL across diverse domains. The incorporation of a federated learning framework with suitable security technology, with a focus on mechanisms for selecting users and data, becomes essential, acting as a safeguard against potential security breaches.

References

[1] S. Sicari, A. Rizzardi, and A. Coen-Porisini, “Insights into security and privacy towards fog computing evolution,” *Comput. Secur.*, vol. 120, p. 102822, 2022, doi: 10.1016/j.cose.2022.102822.

[2] A. Bárcena and J. M. Salazar-Xirinachs, “Economic Commission for Latin America and the Caribbean (ECLAC), Digital technologies for a new future (LC/TS.2021/43), Santiago, 2021.,” *Econ. Comm. Lat. Am.*, pp. 1–95, 2021, [Online]. Available: https://www.cepal.org/sites/default/files/publication/files/46817/S2000960_en.pdf

[3] Y. Xu *et al.*, “Artificial intelligence: A powerful paradigm for scientific research,” *Innovation*, vol. 2, no. 4, 2021, doi: 10.1016/j.xinn.2021.100179.

[4] A. Ghosh, D. Chakraborty, and A. Law, “Artificial intelligence in Internet of things,” *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, 2018, doi: 10.1049/trit.2018.1008.

[5] M. Joshi, A. Pal, and M. Sankarasubbu, “Federated Learning for Healthcare Domain - Pipeline, Applications and Challenges,” *ACM Trans. Comput. Healthc.*, vol. 3, no. 4, 2022, doi: 10.1145/3533708.

[6] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, “A survey on federated learning: challenges and applications,” *Int. J. Mach. Learn. Cybern.*, 2022, doi: 10.1007/s13042-022-01647-y.

[7] R. O. Ogundokun, S. Misra, R. Maskeliunas, and R. Damasevicius, “A Review on Federated Learning and Machine Learning Approaches: Categorization, Application Areas, and Blockchain Technology,” *Inf.*, vol. 13, no. 5, 2022, doi: 10.3390/info13050263.

[8] O. Spjuth, J. Frid, and A. Hellander, “The machine learning life cycle and the cloud: implications for drug discovery,” *Expert Opin. Drug Discov.*, vol. 16, no. 9, pp. 1071–1079, 2021, doi: 10.1080/17460441.2021.1932812.

[9] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–21, 2021, doi: 10.1007/s42979-021-00592-x.

[10] A. L’Heureux, K. Grolinger, H. F. Elyamany, and M. A. M. Capretz, “Machine Learning with Big Data: Challenges and Approaches,” *IEEE Access*, vol. 5, pp. 7776–7797, 2017, doi: 10.1109/ACCESS.2017.2696365.

[11] İ. Yazici, I. Shayea, and J. Din, “A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems,” *Eng. Sci. Technol. an Int. J.*, vol. 44, 2023, doi: 10.1016/j.jestch.2023.101455.

[12] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, “A survey on federated learning,” *Knowledge-Based Syst.*, vol. 216, 2021, doi: 10.1016/j.knosys.2021.106775.

[13] S. Abdulrahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, and M. Guizani, “A survey on federated learning: The journey from centralized to distributed on-site learning and beyond,” *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5476–5497, 2021, doi: 10.1109/JIOT.2020.3030072.

[14] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019, doi: 10.1145/3298981.

[15] E. Hallaji, R. Razavi-Far, M. Saif, B. Wang, and Q. Yang, “Decentralized Federated Learning: A Survey on Security and Privacy,” *IEEE Trans. Big Data*, no. January, pp. 1–20, 2024, doi: 10.1109/TBDATA.2024.3362191.

[16] J. C. Jiang, B. Kantarci, S. Oktug, and T. Soyata, “Federated learning in smart city sensing: Challenges and opportunities,” *Sensors (Switzerland)*, vol. 20, no. 21, pp. 1–29, 2020, doi: 10.3390/s20216230.

[17] Y. Jin, H. Zhu, J. Xu, and Y. Chen, *Federated learning : fundamentals and advances*. 2023.

[18] H. Cho, A. Mathur, and F. Kawsar, “FLAME: Federated Learning across Multi-device Environments,” *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 6, no. 3, 2022, doi: 10.1145/3550289.

[19] M. Moshawrab, M. Adda, A. Bouzouane, H. Ibrahim, and A. Raad, “Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives,” *Electron.*, vol. 12, no. 10, pp. 1–35, 2023, doi: 10.3390/electronics12102287.

[20] H. Ludwig, *Federated Learning*. 2022. doi: 10.1007/978-3-030-96896-0.

[21] J. Li, X. Li, and C. Zhang, “Analysis on Security and Privacy-preserving in Federated Learning,” *Highlights Sci. Eng. Technol.*, vol. 4, pp. 349–358, 2022, doi: 10.54097/hset.v4i.923.

[22] H. Zhang, J. Bosch, and H. H. Olsson, “Federated learning systems: Architecture alternatives,” *Proc. - Asia-Pacific Softw. Eng. Conf. APSEC*, vol. 2020-Decem, pp. 385–394, 2020, doi: 10.1109/APSEC51365.2020.00047.

[23] S. K. Lo, Q. Lu, L. Zhu, H. Y. Paik, X. Xu, and C. Wang, “Architectural patterns for the design of federated learning systems,” *J. Syst. Softw.*, vol. 191, pp. 1–19, 2022, doi: 10.1016/j.jss.2022.111357.

[24] A. A. Abdellatif *et al.*, “Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced

data," *Futur. Gener. Comput. Syst.*, vol. 128, no. ii, pp. 406–419, 2022, doi: 10.1016/j.future.2021.10.016.

[25] B. Hu, Y. Gao, L. Liu, and H. Ma, "Federated Region-Learning: An Edge Computing Based Framework for Urban Environment Sensing," *2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc.*, pp. 1–7, 2018, doi: 10.1109/GLOCOM.2018.8647649.

[26] Q. Xia, W. Ye, Z. Tao, J. Wu, and Q. Li, "A survey of federated learning for edge computing: Research problems and solutions," *High-Confidence Comput.*, vol. 1, no. 1, p. 100008, 2021, doi: 10.1016/j.hcc.2021.100008.

[27] K. Hu *et al.*, "Federated Learning: A Distributed Shared Machine Learning Method," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/8261663.

[28] W. Xia, Y. Li, L. Zhang, Z. Wu, and X. Yuan, "Cascade Vertical Federated Learning," *Proc. - IEEE Int. Conf. Multimed. Expo*, vol. 2022-July, pp. 1–40, 2022, doi: 10.1109/ICME52920.2022.9859921.

[29] M. Ahmadzai and G. Nguyen, "Data Partitioning Effects in Federated Learning," *CEUR Workshop Proc.*, vol. 3588, pp. 138–149, 2023.

[30] Y. Huang *et al.*, "A High-Precision Method for 100-Day-Old Classification of Chickens in Edge Computing Scenarios Based on Federated Computing," *Animals*, vol. 12, no. 24, pp. 1–17, 2022, doi: 10.3390/ani12243450.

[31] M. Aledhari, R. Razzak, R. M. Parizi, and F. Saeed, "Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Access*, vol. 8, no. August, pp. 140699–140725, 2020, doi: 10.1109/ACCESS.2020.3013541.

[32] A. M. Abdelmoniem, C. Y. Ho, P. Papageorgiou, and M. Canini, "A Comprehensive Empirical Study of Heterogeneity in Federated Learning," *IEEE Internet Things J.*, 2023, doi: 10.1109/JIOT.2023.3250275.

[33] S. Saha and T. Ahmad, "Federated transfer learning: Concept and applications," *Intelligenza Artif.*, vol. 15, no. 1, pp. 35–44, 2021, doi: 10.3233/IA-200075.

[34] M. Khan, F. G. Glavin, and M. Nickles, "Federated Learning as a Privacy Solution - An Overview," *Procedia Comput. Sci.*, vol. 217, pp. 316–325, 2023, doi: 10.1016/j.procs.2022.12.227.

[35] A. Rahman *et al., Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues*, vol. 26, no. 4. Springer US, 2022. doi: 10.1007/s10586-022-03658-4.

[36] H. Li *et al.*, "Review on security of federated learning and its application in healthcare," *Futur. Gener. Comput. Syst.*, vol. 144, pp. 271–290, Jul. 2023, doi: 10.1016/J.FUTURE.2023.02.021.

[37] Y. Xianjia, J. P. Queralta, J. Heikkonen, and T. Westerlund, "Federated Learning in Robotic and Autonomous Systems," *Procedia Comput. Sci.*, vol. 191, pp. 135–142, Jan. 2021, doi: 10.1016/J.PROCS.2021.07.041.

[38] A. Hard *et al.*, "Federated Learning for Mobile Keyboard Prediction," 2018, [Online]. Available: http://arxiv.org/abs/1811.03604

[39] S. Hui, E. Song, and A. Hu, "Horizontal Federated Learning and Secure Distributed Training for Recommendation System with Intel SGX".

[40] M. Naseri, Y. Han, and E. De Cristofaro, "BadVFL: Backdoor Attacks in Vertical Federated Learning," 2023, [Online]. Available: http://arxiv.org/abs/2304.08847

[41] H. Wang, F. Xie, Q. Duan, and J. Li, "Federated Learning for Supply Chain Demand Forecasting," *Math. Probl. Eng.*, vol. 2022, 2022, doi: 10.1155/2022/4109070.

[42] D. N. Gupta, R. Kumar, and S. H. Ansari, *Federated Learning for an IoT Application*. 2022. doi: 10.1007/978-3-030-85559-8_4.

[43] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50–60, 2020, doi: 10.1109/MSP.2020.2975749.

[44] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, "A survey on security and privacy of federated learning," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 619–640, 2021, doi: 10.1016/j.future.2020.10.007.

[45] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," no. June, pp. 50–56, 2020.

[46] S. Ji *et al.*, "Emerging trends in federated learning: from model fusion to federated X learning," *Int. J. Mach. Learn. Cybern.*, no. 0123456789, 2024, doi: 10.1007/s13042-024-02119-1.

[47] H. Kurniawan and M. Mambo, "Homomorphic Encryption-Based Federated Privacy Preservation for Deep Active Learning," *Entropy*, vol. 24, no. 11, pp. 1–14, 2022, doi: 10.3390/e24111545.

[48] P. Liu, X. Xu, and W. Wang, "Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives," *Cybersecurity*, vol. 5, no. 1, 2022, doi: 10.1186/s42400-021-00105-6.