International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Federated Learning and Privacy-Preserving AI

Saransh

Department of Information Technology Student of Information Technology, Arya College of Engineering and IT, Kukas, Jaipur

ABSTRACT :

United Learning (FL) is an arising AI procedure that empowers cooperative preparation of models across decentralized gadgets while keeping information restricted on individual gadgets. This strategy is especially helpful in protection delicate conditions, as it disposes of the requirement for brought together information stockpiling, consequently alleviating security concerns. In combined learning, just model updates are imparted to a focal server, saving client information security and limiting the dangers related with information breaks. Protection safeguarding artificial intelligence procedures like differential protection and secure multiparty calculation can additionally upgrade the security of unified learning frameworks by adding commotion to the information or encoding correspondence channels. This paper investigates the standards and execution of united learning, its applications in protection delicate fields like medical care and money.

Index Terms –Federated Learning, Privacy-Preserving AI, Decentralized Machine Learning, Differential Privacy, Secure Multiparty Computation, Data Security and Compliance.

1. INTRODUCTION

In the period of man-made brainpower, information protection has turned into a basic concern, particularly in spaces like medical services, money, and network safety. Customary AI approaches depend on unified information assortment, which presents critical protection and security chances. Unified Learning (FL) offers a decentralized option by empowering cooperative model preparation across numerous gadgets while keeping information limited. This approach limits information openness and diminishes the gamble of breaks, making it especially significant for security touchy applications. By communicating just model updates rather than crude information, FL upgrades security and follows information insurance guidelines like GDPR. Besides, protection safeguarding computer based intelligence strategies, including differential security and secure multiparty calculation, further reinforce FL by adding commotion to information or encoding correspondence channels. Notwithstanding its benefits, FL faces difficulties, for example, correspondence above, model precision compromises, and adaptability issues. This paper investigates the standards of FL, its true applications, and the incorporation of protection safeguarding methods to guarantee secure and proficient AI. Also, we talk about provokes and future examination headings to upgrade FL's adequacy in different ventures.

1.1 Background and Importance of Data Privacy in AI

With the fast headway of man-made brainpower (computer based intelligence) and AI (ML), associations across different businesses depend intensely on information driven models to further develop direction and robotization. Conventional AI models require immense measures of information to be gathered and put away in a concentrated server for preparing. In any case, this concentrated methodology raises critical protection and security concerns, particularly in ventures like medical services, money, and network safety, where information responsiveness is central. Unapproved access, information breaks, and cyberattacks can uncover individual and classified data, prompting extreme lawful and monetary repercussions. Furthermore, administrative systems like the Overall Information Security Guideline (GDPR) and the California Buyer Protection Act (CCPA) force severe limitations on information assortment and use, making consistence a significant test. The requirement for computer based intelligence frameworks that can keep up with high model execution while guaranteeing information protection has driven the advancement of security saving AI procedures. One of the most encouraging ways to deal with tending to these worries is United Learning (FL), a decentralized preparation strategy that wipes out the requirement for crude information sharing. By empowering various gatherings to cooperatively prepare models without uncovering their information, FL presents a groundbreaking answer for security delicate applications.

1.2 Introduction to Federated Learning (FL)

Combined Learning (FL) is a decentralized man-made intelligence preparing procedure that empowers various gadgets or establishments to cooperatively prepare a common model without moving crude information to a focal server. All things considered, the information remains put away locally, and just model updates, like inclinations or weight changes, are sent to a worldwide server for conglomeration. This approach altogether improves information protection and security while additionally lessening the dangers related with concentrated information capacity. FL is especially valuable in situations where information won't be quickly shared due to administrative, moral, or specialized requirements. For example, in the medical services area, clinics and research establishments can utilize FL to foster computer based intelligence models for illness expectation and analysis without compromising patient privacy. Essentially, monetary establishments can prepare extortion location models without uncovering touchy exchange records. Moreover, FL is appropriate for edge registering and Web of Things (IoT) gadgets, where preparing models locally diminishes inactivity and data transfer capacity utilization. Regardless of these benefits, FL presents new specialized difficulties, like correspondence above, heterogeneity in gadget capacities, and security weaknesses. Tending to these difficulties is urgent for the far and wide reception of FL in protection delicate applications.

1.3 Role of Privacy-Preserving AI Techniques

While FL enhances privacy by preventing raw data transmission, additional privacy-preserving AI techniques are often integrated to further strengthen security. Differential Privacy (DP) is one such technique that ensures individual data points remain indistinguishable within a dataset by adding controlled noise to model updates before they are shared. This prevents adversaries from inferring sensitive information while still allowing useful model training. Secure Multiparty Computation (SMPC) is another critical approach that enables multiple parties to jointly compute functions over their inputs without revealing the actual data. Additionally, homomorphic encryption allows computations to be performed directly on encrypted data, ensuring that sensitive information remains protected throughout the training process. Federated Averaging (FedAvg), an optimization algorithm used in FL, helps reduce communication costs by averaging model updates before sending them to the global server. These privacy-enhancing techniques ensure compliance with data protection regulations such as GDPR and HIPAA while maintaining the utility of AI models. However, incorporating these methods introduces computational complexity and potential trade-offs in model accuracy, making it essential to balance security and performance in FL systems.

1.4 Challenges in Federated Learning

In spite of its true capacity, United Learning (FL) faces a few difficulties that should be tended to for successful execution. One of the essential difficulties is correspondence above, as FL requires successive trades of model updates between various gadgets and a focal server. This can prompt expanded network blockage and dormancy, especially in enormous scope arrangements. Another issue is information heterogeneity, where various gadgets might have non-IID (autonomous and indistinguishably appropriated) information, prompting imbalanced preparation and diminished model precision. Furthermore, gadget heterogeneity presents difficulties, as members in a FL framework might have shifting computational power, battery duration, and organization availability, influencing by and large preparation productivity. Security concerns, for example, model harming assaults, where foes infuse malignant updates to control the worldwide model, likewise compromise FL frameworks. Additionally, protection gambles actually exist, as enemies might endeavor induction assaults to remove delicate data from model updates. Tending to these difficulties requires streamlining FL designs, executing strong safety efforts, and creating methodologies to work on model collection while guaranteeing reasonableness and effectiveness.

2. TECHNIQUES

The essential procedures in Combined Learning (FL) and Protection Safeguarding computer based intelligence center around getting information during model preparation and guaranteeing client security. In FL, model collection is critical, where neighborhood models prepared on decentralized gadgets are accumulated at a focal server to make a worldwide model. Differential security adds controlled commotion to display refreshes, forestalling the recognizable proof of individual data of interest while keeping up with model execution. Secure Multiparty Calculation (SMPC) empowers information sharing and calculation across parties without uncovering individual information, guaranteeing protection during cooperative learning. Also, Homomorphic Encryption permits calculations on scrambled information, guaranteeing that touchy data stays secret in the interim. Information anonymization methods further guarantee that the information utilized for model preparation can't be followed back to people. These procedures aggregately improve the protection and security of FL frameworks, empowering their application in touchy regions like medical services, money, and that's only the tip of the iceberg, while guaranteeing consistence with guidelines like GDPR.

2.1 Model Aggregation in Federated Learning:

Model collection is at the center of United Learning (FL), empowering decentralized gadgets to team up in preparing a common AI model while keeping their information limited. In this cycle, each taking part gadget prepares its neighborhood model utilizing its own private dataset. When preparing is finished, the gadgets send just the model updates, like loads and slopes, to a focal server as opposed to communicating the crude information itself. The server then totals the got refreshes, ordinarily by averaging them to frame a worldwide model. This collection procedure permits the model to work on through the joined information on numerous gadgets while keeping up with severe protection, as individual information is rarely shared. Different collection calculations, like Combined Averaging (FedAvg), are utilized to adjust the commitment of every gadget's model update in view of elements like gadget size, computational power, and information dispersion. Model conglomeration in FL permits associations to use decentralized information without compromising security or protection, which is especially significant in delicate regions like medical services and money.

2.2 Differential Privacy:

Differential security is a strong method intended to protect individual information inside enormous datasets. With regards to Combined Learning (FL), differential protection is applied to the model updates sent from the neighborhood gadgets to the focal server. Rather than communicating the specific model updates, every gadget adds clamor to the updates before they are shared. This clamor is painstakingly adjusted to save the security of individual data of interest while guaranteeing the general presentation of the worldwide model. The vital idea driving differential security is that the consideration or rejection of any singular's information shouldn't fundamentally influence the model's result. By applying differential protection, FL frameworks can moderate the gamble of uncovering delicate data from preparing information, like clinical or monetary records, regardless of whether an enemy approaches the totaled model updates. How much clamor presented can be controlled utilizing boundaries like epsilon, which adjusts the compromise among protection and model exactness. This method is particularly vital when FL is applied to delicate spaces where client protection is fundamental, like in medical care, money, and individual information examination.

2.3 Secure Multiparty Computation (SMPC):

Secure Multiparty Calculation (SMPC) is a cryptographic strategy that empowers different gatherings to register capabilities on their confidential information without uncovering any of the singular data sources. With regards to United Learning (FL), SMPC assumes a urgent part in safely conglomerating model updates without uncovering any delicate data. Rather than straightforwardly sharing model updates, every gadget scrambles its information or updates and sends it to a focal server. The server then plays out the vital collection ventures without having the option to get to the encoded information. This technique guarantees that the security of individual gadgets is safeguarded, as the server can't surmise the crude information or explicit updates from the total. SMPC conventions can include methods like mystery sharing, where each piece of information is parted into numerous parts and conveyed across various gadgets, guaranteeing that no single gadget has total information on the information. By utilizing SMPC, unified learning can be made safer, empowering cooperative model preparation in conditions where security is basic, like monetary exchanges or clinical information examination.

2.4 Homomorphic Encryption:

Homomorphic encryption is a high level cryptographic procedure that permits calculations to be performed on encoded information without unscrambling it first. This property makes it an optimal technique for guaranteeing information protection in Combined Learning (FL) applications. While involving homomorphic encryption in FL, every gadget scrambles its model updates prior to sending them to the focal server. The server then, at that point, totals the encoded refreshes and produces a worldwide model while never approaching the crude information or the singular updates in plaintext. The scrambled model is then sent back to the gadgets for additional preparation. This encryption guarantees that regardless of whether the server is compromised or a foe accesses the model, they will just experience the encoded information, which is for all intents and purposes difficult to decode without the proper cryptographic keys. Homomorphic encryption adds an additional layer of safety to United Learning frameworks, empowering private cooperative learning while at the same time guaranteeing that the information stays classified all through the whole interaction. Albeit this strategy can be computationally costly, continuous progressions in encryption techniques and advancements are making it progressively attainable for use in genuine situations, especially in touchy applications like clinical exploration and money.

3. Federated Learning (FL)

Combined Learning (FL) is a decentralized AI approach that empowers numerous gadgets or establishments to cooperatively prepare a model without sharing crude information. Dissimilar to conventional unified learning, FL keeps information limited, lessening security gambles and guaranteeing consistence with information insurance guidelines like GDPR. Rather than sending touchy data, just model updates are imparted to a focal server, limiting the gamble of information breaks. FL is especially valuable in security touchy fields like medical care, money, and edge registering, where information privacy is urgent. To additional upgrade security, strategies like differential protection and secure multiparty calculation are incorporated, adding commotion to information or encoding correspondence. In spite of its benefits, FL faces difficulties connected with versatility, correspondence proficiency, and model exactness, which require creative arrangements. Future exploration centers around upgrading preparing effectiveness, security structures, and personalization to make FL more vigorous for genuine applications.

3.1 Architecture and Working Mechanism of FL

The engineering of FL comprises of three principal parts: client gadgets, (for example, cell phones, IoT gadgets, or emergency clinic servers), a focal server, and a correspondence component. The FL cycle commonly follows an iterative work process: (1) The focal server instates the worldwide model and sends it to taking an interest clients. (2) Every client prepares the model locally on its confidential information. (3) The privately prepared models are sent back to the focal server as updates. (4) The server totals these updates utilizing strategies like Unified Averaging (FedAvg) to work on the worldwide model. (5) The refreshed worldwide model is sent back to the clients, and the cycle rehashes until combination. This cycle guarantees that crude information never leaves the client's gadget, decreasing the gamble of information breaks. Furthermore, techniques like nonconcurrent refreshes and various leveled FL further develop productivity and adaptability, empowering FL to be conveyed across assorted genuine applications.

3.2 Privacy-Preserving Techniques in FL

Since FL is utilized in delicate conditions, different protection saving procedures are coordinated to improve security. Differential security (DP) guarantees that singular information focuses can't be recognized by adding commotion to demonstrate refreshes before transmission. Secure Multiparty Calculation (SMPC) empowers various gatherings to process a capability without uncovering their confidential information sources, guaranteeing protection during model conglomeration mutually. Homomorphic encryption (HE) permits calculations to be performed straightforwardly on encoded information, forestalling openness of crude information during preparing. Moreover, confided in execution conditions (TEEs), like Intel SGX, give a solid equipment based execution climate that shields model updates from outside dangers. These procedures all in all upgrade FL's security by limiting information spillage gambles and keeping up with consistence with information assurance regulations.

3.3 Applications of FL in Privacy-Sensitive Domains

FL has various applications across security delicate areas. In medical care, FL empowers emergency clinics to cooperatively prepare computer based intelligence models on understanding information without sharing crude clinical records, further developing illness finding and therapy suggestions. In finance, banks use FL to identify misrepresentation and survey credit takes a chance while guaranteeing client information privacy. Cell phones and IoT gadgets benefit from FL via preparing customized artificial intelligence models, like console ideas and voice colleagues, without compromising client information security. Independent vehicles influence FL to improve traffic expectation models and wellbeing components while keeping vehicle sensor information hidden. Furthermore, FL is utilized in network safety to identify malware designs cooperatively while keeping up with information classification. These applications feature FL's adaptability in empowering computer based intelligence progressions while saving client protection.

3.4 Challenges and Limitations of FL

In spite of its benefits, FL faces a few difficulties that obstruct its far reaching reception. One significant issue is correspondence above, as regular model updates between client gadgets and the server require critical transfer speed and computational assets. Information heterogeneity is another test, where client gadgets might have non-indistinguishable information dispersions, prompting one-sided models and decreased exactness. Framework heterogeneity, where gadgets have shifting computational capacities, can cause failures in preparing. Guaranteeing model strength against antagonistic assaults and information harming is likewise significant, as pernicious clients can control model updates. Furthermore, consistence with administrative prerequisites like GDPR and HIPAA adds intricacy to FL organizations. Tending to these difficulties requires upgrading correspondence methodologies, further developing accumulation strategies, and coordinating more grounded security instruments.

3.5Future Directions and Advancements in FL

The eventual fate of FL lies in beating its restrictions and extending its applications. Customized FL, where models adjust to individual client information while profiting from worldwide learning, is building up momentum. Decentralized FL (distributed learning) eliminates the focal server, making FL more adaptable and tough. Blockchain-based FL improves security and trust by empowering straightforward model conglomeration. Energy-effective FL arrangements are being created to improve preparing on asset compelled gadgets. Research is additionally zeroing in on unified support realizing, which empowers computer based intelligence models to powerfully gain from decentralized conditions. As protection guidelines keep on advancing, FL will incorporate more powerful security methods to guarantee consistence. These progressions will make FL more effective, versatile, and secure, empowering its broad reception in genuine computer based intelligence applications.

4. Privacy-Preserving AI

Security safeguarding artificial intelligence guarantees information privacy while empowering AI applications. In United Learning (FL), this is accomplished by keeping information on nearby gadgets and just sharing model updates, decreasing the gamble of information breaks. Procedures like differential security acquaint controlled clamor with forestall the ID of individual pieces of information. Secure multiparty calculation (SMPC) permits various gatherings to cooperatively prepare models without uncovering their confidential information. Homomorphic encryption further improves security by empowering calculations on encoded information. These strategies assist FL with conforming to guidelines like GDPR and CCPA, guaranteeing moral computer based intelligence organization. In any case, coordinating protection methods frequently accompanies compromises in effectiveness and model exactness. Research keeps on advancing protection safeguarding computer based intelligence for versatility and genuine applications in delicate areas like medical care and money.

4.1 Differential Privacy

Differential Protection (DP) is a strategy that guarantees individual information focuses stay undefined inside a dataset by bringing controlled commotion into calculations. This approach keeps assailants from deriving private data regardless of whether they approach measurable results. DP works by adding irregularity to the information during preparing or surmising, guaranteeing that the presence or nonappearance of any single record doesn't altogether modify the model's way of behaving. It is generally utilized in applications like medical services and money, where it is basic to keep up with classification. Organizations like Apple and Google use DP to dissect client information while protecting security. The harmony among security and exactness stays a test, as unreasonable clamor can corrupt model execution. High level strategies, for example, versatile DP, expect to upgrade commotion levels progressively to improve both security and utility.

4.2Secure Multiparty Computation (SMPC)

Secure Multiparty Calculation (SMPC) is a cryptographic procedure that empowers numerous gatherings to mutually figure a capability over their contributions without uncovering those contributions to one another. This guarantees that delicate information stays private in any event, during cooperative calculations. SMPC is especially helpful in situations where different associations need to share bits of knowledge without uncovering crude information, like extortion identification in monetary foundations or cooperative clinical examination. It utilizes conventions like mystery sharing, jumbled circuits, and unmindful exchange to safeguard information uprightness. In spite of areas of strength for its ensures, SMPC can be computationally costly, making productivity a critical area of examination. Improvements, like crossover cryptographic methodologies, are being created to make SMPC more useful for enormous scope simulated intelligence applications.

4.3Homomorphic Encryption

Homomorphic Encryption (HE) permits calculations to be performed straightforwardly on scrambled information without requiring decoding. This guarantees that touchy data stays safeguarded all through the preparation and derivation process. HE is especially significant in distributed computing situations, where clients can rethink simulated intelligence calculations without uncovering their confidential information. Completely Homomorphic Encryption (FHE) empowers erratic calculations on encoded information yet is computationally costly. To some extent Homomorphic Encryption (PHE) and Fairly Homomorphic Encryption (SHE) offer more effective options by supporting restricted activities. Continuous exploration centers around working on HE's proficiency to make it possible for constant simulated intelligence applications. Its mix into Combined Learning improves security by guaranteeing that even model updates remain scrambled, relieving gambles related with malevolent servers.

4.4 Data Anonymization and De-Identification

Data Anonymization techniques transform personally identifiable information (PII) into anonymous data, ensuring that individuals cannot be re-identified. Common methods include generalization (reducing data specificity), suppression (removing sensitive attributes), and tokenization (replacing PII with pseudonyms). K-anonymity, L-diversity, and T-closeness are widely used frameworks for ensuring anonymization effectiveness. However, advances in machine learning have shown that de-anonymization attacks can re-identify individuals, highlighting the need for robust privacy-preserving methods. Anonymization is particularly important in industries like healthcare, where patient records must remain confidential while being used for research and analytics. Combining anonymization with cryptographic techniques enhances security, ensuring compliance with privacy regulations such as GDPR and HIPAA.

4.5 Blockchain for Privacy-Preserving AI

Blockchain innovation is progressively being coordinated into Protection Saving computer based intelligence to guarantee straightforwardness, security, and decentralization. In Unified Learning, blockchain can give a permanent record of model updates, forestalling altering and guaranteeing responsibility. Savvy agreements can robotize protection safeguarding conventions, for example, confirming differential security ensures before model updates are acknowledged. Blockchain additionally works with secure information dividing among numerous gatherings while keeping up with access control and auditability. Notwithstanding, incorporating blockchain with artificial intelligence presents difficulties, including versatility and high energy utilization. Half breed models consolidating blockchain with off-chain calculation are being created to improve proficiency while keeping up major areas of strength for with ensures.

5.Decentralized Machine Learning

Decentralized AI is a critical part of unified learning (FL), empowering various gadgets or hubs to cooperatively prepare a model without sharing crude information. Not at all like customary incorporated approaches, FL guarantees information stays on nearby gadgets, upgrading protection and security. This is especially valuable in delicate areas like medical care and money, where information privacy is vital. By communicating just model updates rather than whole datasets, FL diminishes the gamble of information breaks and unapproved access. Procedures like differential protection and secure multiparty calculation further upgrade security by adding commotion to information or encoding interchanges. Decentralized advancing additionally further develops adaptability, permitting models to be prepared effectively across appropriated networks. In any case, difficulties like correspondence above, non-IID (free and indistinguishably dispersed) information, and keeping up with model precision should be tended to. Progressions in protection safeguarding simulated intelligence are fundamental to defeating these difficulties and guaranteeing secure, proficient decentralized learning structures.

5.1 Edge AI and On-Device Learning

Edge artificial intelligence alludes to AI models being sent and prepared straightforwardly tense gadgets, for example, cell phones, IoT sensors, and independent frameworks, rather than depending on cloud-based calculation. This approach altogether diminishes dormancy, upgrades constant independent direction, and limits information transmission to outer servers, subsequently further developing protection and security. On-gadget learning further refines this idea by empowering nonstop learning on nearby gadgets, guaranteeing that models are refreshed in view of customized information. Methods like information refining, model pruning, and quantization assist with streamlining models for proficient execution on asset compelled gadgets. Edge simulated intelligence is essential in applications like shrewd homes, modern mechanization, and independent vehicles, where prompt reactions and protection are fundamental.

5.2 Blockchain for Secure Decentralized Learning

Blockchain innovation improves decentralized AI by giving a straightforward, sealed, and secure climate for model updates and collection. In blockchain-based FL, model updates are recorded on a circulated record, guaranteeing responsibility and forestalling vindictive changes. Savvy contracts work with mechanized and trustless execution of learning errands, taking out the requirement for a focal power. Also, cryptographic procedures, for example, zero-information verifications and secure multiparty calculation can be coordinated with blockchain to additional improve security. While blockchain further develops trust and security, difficulties, for example, high computational expenses, versatility issues, and organization idleness should be addressed to guarantee down to earth execution in certifiable situations.

5.3 Privacy-Preserving Techniques in Decentralized Learning

Security is a main pressing issue in decentralized picking up, requiring progressed procedures to safeguard delicate information while keeping up with model execution. Differential protection guarantees that singular information focuses can't be recognized by adding controlled clamor to display refreshes. Homomorphic encryption permits calculations on encoded information without decoding it, safeguarding privacy all through the preparation interaction. Secure multiparty calculation (SMPC) empowers cooperative model preparation without uncovering individual information to different members. Combined refining is one more arising method where information is partaken in a compacted structure rather than crude model boundaries, decreasing protection gambles. These procedures assume a vital part in guaranteeing that decentralized AI follows guidelines like GDPR while keeping up with effectiveness and precision.

5.4Communication Efficiency and Model Aggregation

One of the vital difficulties in decentralized learning is lessening correspondence above between circulated hubs and focal servers. FL and other decentralized approaches depend on successive model updates, which can strain network assets. Strategies like slope pressure, quantization, and pruning assist with limiting the size of updates while protecting model exactness. Various leveled FL presents different layers of collection, where edge gadgets first total nearby models prior to sending them to a focal server, diminishing transmission capacity utilization. Versatile correspondence methodologies, for example, occasional updates and particular boundary sharing, further advance asset usage. Tending to these correspondence challenges is basic for conveying decentralized AI in huge scope, certifiable applications.

5.5 Security Challenges and Threat Mitigation in Decentralized ML

Decentralized AI frameworks are defenseless against different security dangers, including information harming, model reversal assaults, and ill-disposed controls. Byzantine adaptation to non-critical failure components assist with alleviating assaults where noxious members endeavor to ruin the educational experience. Procedures like inconsistency location and hearty total calculations (e.g., Krum and Middle accumulation) can sift through compromised model updates. Secure areas give equipment based security to decentralized ML by secluding delicate calculations. Consistent checking, access control, and antagonistic preparation further fortify security, guaranteeing that decentralized learning frameworks stay strong against arising dangers.

REFERENCES:

1. Auditable Homomorphic-Based Decentralized Collaborative AI with Attribute-Based Differential Privacy
   Authors: Lo-Yao Yeh, Sheng-Po Tseng, Chia-Hsun Lu, Chih-Ya Shen
   Published: February 28, 2024
   Link:https://arxiv.org/abs/2403.00023

2. Federated Learning and Differential Privacy: Software Tools Analysis, the Sherpa.ai FL Framework and Methodological Guidelines for Preserving Data Privacy
   Authors: Nuria Rodríguez-Barroso, Goran Stipcich, Daniel Jiménez-López, José Antonio Ruiz-Millán, Eugenio Martínez-Cámara, Gerardo González-Seco, M. Victoria Luzón, Miguel Ángel Veganzones, Francisco Herrera
   Published: July 2, 2020
   Link:https://arxiv.org/abs/2007.00914

3. FedER: Federated Learning through Experience Replay and Privacy-Preserving Data Synthesis
   Authors: Matteo Pennisi, Federica Proietto Salanitri, Giovanni Bellitto, Bruno Casella, Marco Aldinucci, Simone Palazzo, Concetto Spampinato
   Published: June 20, 2022
   Link:https://arxiv.org/abs/2206.10048

4. Federated Learning and Privacy
Authors: Kallista Bonawitz, Peter Kairouz, Brendan McMahan, Daniel R. Ramage
Published: 2021
Link:https://research.google/pubs/federated-learning-and-privacy/

5. FedAdOb: Privacy-Preserving Federated Deep Learning with Adaptive Obfuscation
Authors: Hanlin Gu, Jiahuan Luo, Yan Kang, Yuan Yao, Gongxi Zhu, Bowen Li, Lixin Fan, Qiang Yang
Published: June 3, 2024
Link:https://arxiv.org/abs/2406.01085