Private and Secure Machine Learning in Wireless Mobile Communication

Sogo Pierre Sanon[†], Josephine N. A. Tetteh [‡], Rekha Reddy[†], and Hans D. Schotten[*†]
[†]Intelligent Networks Research Group, German Research Center for Artificial Intelligence
D-67663 Kaiserslautern, Email: {firstname.lastname}@dfki.de
[*]Institute for Wireless Communication and Navigation, RPTU Kaiserslautern-Landau
D-67663 Kaiserslautern, mail: {lastname}@rptu.de
[‡]Frankfurt Institute for Advanced Studies, Frankfurt am Main, Germany Frankfurt,
Email: tetteh@fias.uni-frankfurt.de

Abstract

As wireless mobile communication continues to evolve, the demand for efficient and accurate Machine Learning (ML) models to manage different use cases has grown substantially. Distributed Collaborative Machine Learning (DCML) techniques offer a promising solution by enabling multiple devices/entities to collaboratively train an ML model without having to share their data with each other. Although these methods can enhance user data privacy, many researches have shown their limitations. One way to ensure privacy in DCML techniques is to use Differential Privacy (DP). DP is a framework that offers mathematically guaranteed privacy. This research paper presents an investigation into the integration of DP mechanisms within DCML frameworks for wireless mobile communication environments. It evaluates the performance of DP and DCML techniques in various aspects of wireless mobile communication, including network traffic analysis, and network slicing. Through experimental simulations, the impact of DP on model performance, convergence rate, and computation overhead is analyzed. The results provide insights into the trade-offs between privacy preservation and ML model effectiveness. This research contributes to the understanding of how the combination of DP and DCML methods can be effectively integrated into wireless mobile communication.

This is a preprint of the publication which has been presented at the IEEE Future Networks World Forum 2023.

Index Terms

Wireless Mobile communication, Differential Privacy, Split Learning, Federated Learning, SplitFed Learning

I. Introduction

Wireless communication has become an essential part of our lives. It is used in a wide variety of applications, from smartphones and laptops to smart home devices and self-driving cars. As the number of wireless devices and applications continues to grow, the complexity of wireless networks is also increasing. The diversity in these use cases necessitates a flexible and adaptive network infrastructure. Machine Learning (ML), especially Distributed Collaborative Machine Learning (DCML), has emerged as an indispensable tool in achieving this.

DCML techniques such as Federated Learning (FL), Split Learning (SL), and Splitfed Learning (SFL) [1]–[3], facilitate collaboration on ML model training without sharing raw data, thus, preserving individual privacy while improving model efficiency. These approaches efficiently allocate computational resources, minimize communication overhead, and can be scaled to handle large datasets and numerous participants. They are particularly relevant in wireless mobile communication environments, where data is generated and processed across many devices. However, the distributive nature of these techniques increases the attack surface on the collaboratively trained ML models [4]. For instance, in [5] a backdoor attack algorithm to exploit the FL based mmWave beam selection method is proposed. In addition, stringent data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are being enforced, leading to the development and adoption of more private and secure ML techniques.

Traditional privacy-preserving methods, like data anonymization and data masking, have been valuable tools in protecting individual privacy, particularly in situations where data sharing is necessary. However, these methods have revealed vulnerabilities over time, especially when faced with adversaries with advanced data re-identification and de-anonymization capabilities [6]. Thus, while these approaches offer practical solutions, their effectiveness diminishes as data complexity and the potential for information leakage increases, prompting the development of more advanced approaches like Differential Privacy (DP) to address evolving privacy challenges.

DP offers a mathematically rigorous approach to privacy protection [7]. It provides a strong foundation for quantifying and controlling the privacy risk associated with data releases and queries. It ensures that the presence or absence of any individual's data has a negligible impact on the outcome of data analyses. DP accomplishes this by introducing carefully calibrated noise or randomness into data queries, effectively

obscuring the contributions of individual data points. This approach not only offers robust privacy guarantees but also allows for meaningful data analysis and statistical inference. DP has gained prominence as a leading-edge privacy-preserving methodology in real-world applications [8]–[11].

In this study, the integration of DP mechanisms into DCML frameworks for wireless mobile communication environments is explored. Various DP-based distributed ML techniques are comprehensively evaluated, with a specific focus on applications like network traffic analysis, and network slicing. Experimental simulations are employed to quantitatively assess the impact of DP on key performance metrics such as model accuracy, convergence rate, and computation overhead. These will be particularly important in upcoming wireless mobile communication systems such as Beyond 5G (B5G) and Sixth Generation (6G). In summary, the main contributions of this study are as follows:

- **Addressing privacy concerns in DCML**: The privacy concerns associated with the utilization of DCML techniques in wireless mobile communication are discussed.
- **Integration of DP into DCML**: The application of DP within various DCML techniques in the domain of wireless mobile communication are explored.
- **Identifying the most effective DP-enhanced DCML approaches**: The most effective DCML techniques for implementing DP in wireless mobile communication are identified, with a focus on their ability to preserve privacy and improve accuracy.

The rest of the work is organised as follows: Section II presents the related works. Section III gives an overview and description of DP as well as the use of DP in machine learning in general. It also gives a background of the various DCML techniques considered in this work. In Section IV, the application of DP and DCML in wireless mobile communication is discussed and a threat model is presented. Section V presents the performance evaluation for major tasks in wireless mobile communication. Section VI concludes the paper and presents discussions for future work.

II. Related Work

DP, developed by *Dwork et al.* has gained significant attention since its introduction in 2006 [7]. Events like the Netflix Prize competition [6] and other privacy breaches have demonstrated the inefficiency of data anonymization and highlighted the need for a more robust technique for privacy like DP. It has been adopted by many companies including Google [8], Apple [11], Uber [9], and also by US Census Bureau for the 2020 Census [10].

DP has been combined with DCML techniques, such as FL [2], SL [12] and the combination of both [3], [13], in many studies. The addition of DP to these techniques provides a more robust privacy-preserving framework by protecting against some known vulnerabilities in FL and SL [4].

In wireless mobile communication applications, FL has gained significant traction. *Sanon et al.* proposed an FL framework that ensures accurate and efficient prediction while preserving data privacy [14]. Also a combination of FL and Homomorphic Encryption (HE) in wireless mobile communication has been studied in [15]. SL has been used in [16] in a wireless Multiple Input Multiple Output (MIMO) communication network, utilizing MIMO-based over-the-air computation (OAC) to reduce communication costs. Also, [17] developed HiveMind, an SL system tailored for Fifth Generation (5G) Mobile Edge Computing (MEC). Other researches in this direction include [18]–[20]. The application of DP in wireless communication has been proposed in [21], [22].

With upcoming wireless mobile communication systems, B5G and 6G, expected to be more complex with security and privacy paramount, more focus needs to be placed on DCML as well as privacy-preserving techniques. Previous studies have investigated DCML approaches in various aspects of wireless mobile communication. However, there is still a lack of comprehensive comparative studies on the integration of DCML with DP. This work aims to contribute to the advancement of this research area by investigating the potential of DP in various DCML techniques for different aspects of wireless mobile communication. It presents a practical study on network traffic analysis and network slicing, thus providing valuable support to communications service providers (CSPs) in implementing robust and privacy-preserving methodologies within their operational frameworks.

III. Preliminaries

ML models can sometimes memorize details about the data they are trained on. This information could be leaked later on, which could have negative consequences for individuals. DP is a framework for measuring this leakage and reducing the risk of it happening.

A. Differential Privacy and its Variants

ε-DP [23], (ε, δ)-DP [24], Rényi Differential Privacy (RDP) [25] and Gaussian DP [26] are different formulations of the DP concept, each providing varying levels of privacy protection and flexibility.

*1) ε-**Differential Privacy**:* ε-DP is the most common variant of DP. A mechanism/algorithm (any computation that can be performed on the data) $\mathcal{A}$ is ε-DP if, for any two neighboring datasets (datasets that differ in only one individual's data), the probability of the algorithm outputting any particular result is at most e^{ε} times greater for one dataset than for the other. Formally, for two neighboring datasets D and D' and a set S

$$P[\mathcal{A}(D) \in S] \leq e^{\varepsilon} \times P[\mathcal{A}(D') \in S]. \tag{1}$$

Here, ε is a privacy parameter that controls the level of privacy protection, with smaller values of ε providing stronger privacy guarantees. A smaller ε implies that the presence or absence of any individual's data has a limited impact on the

final query result. An algorithm $\mathcal{A}$ that is not ε-DP can achieve it by applying the Laplace mechanism [23] or exponential mechanism [27].

2) $(\varepsilon, \delta)-$***Differential Privacy****:* (ε, δ)-DP is a more general and flexible variant of ε-DP. An algorithm is (ε, δ)-DP if, for any two neighboring datasets D, D':

$$P[\mathcal{A}(D) \in S] \leq e^{\varepsilon} \times P[\mathcal{A}(D') \in S] + \delta. \tag{2}$$

The main advantage of (ε, δ)-DP is that it can be used in applications where there is a small probability of failure, quantified by δ. Gaussian mechanism is used to achieve (ε, δ)-DP [24]. For this work, (ε, δ)-DP variant is considered. More information on other variants can be found in [25], [26].

B. Global, Local Differential Privacy and Applications

DP can be classified into two types, Local Differential Privacy (LDP) [28] and Global Differential Privacy (GDP) [29]. LDP is a model of DP with the added requirement that even if an adversary has access to the personal responses of an individual in the database, that adversary will still be unable to learn too much about the user's personal data. This is contrasted with GDP, a model of DP that incorporates a central aggregator with access to the raw data.

1) ***Local Differential Privacy****:* In LDP the data curator or central aggregator does not know the actual value, and thus privacy is protected. The user does not have to trust the data curator or the database owner to use his/her data responsibly. However, since each user must add noise to their own data, the total noise is much larger and typically would need many more users to get useful results. LDP finds practical use in various applications. Google's RAPPOR gathers data on users' activities and website visits, enhancing products without privacy issues [8]. Apple's Private Count Mean Sketch improves predictive models using emoji and word data from iPhone users [11]. LDP safeguards personal health data in aggregating streams for research, maintaining user privacy.

2) ***Global Differential Privacy****:* GDP involves adding noise to the query outputs of a database, specifically at the end of the process before sharing the results with a third party. The noise addition is carried out by a trustworthy data curator who has access to the original raw data in the database. This protective measure safeguards user privacy from individuals querying the database. An interesting use case of GDP is the Census Bureau Adopts Cutting Edge Privacy Protections for 2020 Census, that is, the US Census use DP to anonymize the data before publication [10].

As observed above, DP can be used in many tasks including data anonymization, and secure queries. One important application of DP is in ML, especially Deep Learning (DL).

C. Differential Privacy in Machine Learning

In DL, there are techniques for achieving DP. The main ones include Differential Privacy Stochastic Gradient Descent (DP-SGD) and Private Aggregation of Teacher Ensembles (PATE). In this work, DP-SGD is used.

DP-SGD is a powerful technique that combines the principles of DP with the popular optimization algorithm, Stochastic Gradient Descent (SGD) [30]. It aims to enable privacy-preserving DL by injecting carefully calibrated noise into the gradient updates during the training process. This addition of noise ensures that the updates to the model's parameters are sufficiently random, protecting the privacy of individual data points while still allowing effective model training.

The privacy guarantee in DP-SGD ensures that an individual data point's presence in the training dataset will not significantly impact the model's output or final decision. DP-SGD is (ε, δ)-DP.

D. Federated Learning

Initially introduced by Google [2], FL is a collaborative distributed learning framework developed to facilitate the training of machine learning models on distributed devices that generate privacy-sensitive training data locally. In the initial round of FL, the central server initializes a global model and sends it to a selected group of participating clients. After receiving this initial model, each client commences its training process using its locally available training data. Following training, each client sends back its updated model to the server. The server then aggregates all the received models to generate an updated version of the global model. This process of computation and communication continues iteratively until the global model converges. There are many aggregation techniques, with the most commonly used being Federated Averaging (FedAvg) [31]. In this work, FedAvg is used.

E. Split Learning

SL, also called SplitNN, introduced by *Vepakomma et al.* [1], is a DCML technique which works by splitting an ML model's architecture into two main parts - a client side and a server side. At the client side, individual clients engage in the training of their models up to a designated cut layer and solely exchange activations and gradients originating from this cut layer to the server side. The server side then performs the remaining training steps and subsequently propagates the gradients back to the clients. By keeping the server and client side separate, SL allows the server-side to handle the most computationally expensive tasks during the training. Also, this partitioning diminishes data breach risks and unauthorized access. Furthermore, SL decreases communication overhead by transmitting only feature representations of cut layer outputs, making it suitable for resource-constrained environments and large-scale distributed systems.

F. Combining Federated and Split Learning

Combinations of FL and SL have emerged to create hybrid approaches that leverage the strengths of both techniques. One such architecture is Splitfed Learning (SFL) [3], which combines FedAvg and SplitNN. In addition to combining both

SL and FL, SFL offers a refined architectural configuration incorporating DP. Other hybrid approaches include Federated Split Learning (FedSL) [13] and Parallel Split Learning (PSL) [32]. In this work, SFL is used.

IV. DP and DCML in Wireless Mobile Communication

Wireless mobile networks are facing increasing challenges in managing resources efficiently to accommodate expanding user sets. Artificial Intelligence (AI) and ML are emerging as powerful tools to address these challenges. AI/ML can be used to improve a variety of functions in wireless networks, such as channel estimation, optimization of massive MIMO configurations, beam management, network slicing, dynamic spectrum allocation, resource and traffic management, Quality of Service (QoS) governance, security reinforcement, and anomaly detection. DCML can improve the accuracy of ML models by enabling learning from a wider range of data. The distributive and collaborative nature of these techniques can enhance the privacy and scalability of ML models by allowing private parallel learning as well as handling large-scale and geographically diverse datasets. Combined with DP, DCML can lead to more trustworthy and safe use of AI and can overcome many vulnerabilities that come with distributed techniques and ML in general, such as back door attacks, reverse engineering, and linking attacks. Also, CSPs can comply with privacy protection laws while still providing the best QoS to their customers.

Threat Model on DCML in Wireless Mobile Networks: In DCML, honest but curious entities can potentially launch attacks, including inference attacks, label leakage, and model inversion as shown in recent research [33]–[35]. These risks can be mitigated through the application of LDP. Adversaries may seek to infer private information which can compromise CSPs. For instance, with carefully crafted inputs related to traffic flow data and by analyzing the model's responses, a curious server can infer sensitive information about specific traffic patterns, potentially compromising traffic management strategies. Also, DP can limit model inversion and label leakage attacks which particularly affect SL models [35]. The aim of this work is to prevent such vulnerabilities which can lead to financial and credibility loss in CSPs and even compromise their users' privacy including disclosing highly sensitive personal information. In the next section, the feasibility of combining DP with network traffic analysis and network slicing in collaborative environments is evaluated in order to assess the potential benefits and challenges.

V. Performance Evaluation

The performance evaluation is done for two major tasks in wireless mobile communication, network traffic analysis, and network slicing.

- **Network Traffic Analysis** is crucial for various domains, including network management, security, and QoS provisioning. Accurate traffic forecasting enables effective resource allocation, optimization of network capacity planning, and improved overall network performance. Additionally, it aids in load balancing, routing optimization, and the detection of anomalous behaviors and security threats, enhancing network security and resilience. DP and DCML can greatly enhance the privacy, security and efficiency of network traffic analysis.
- **Network Slicing** has emerged as a promising model for 5G and beyond networks to support services with diverse and demanding requirements. These requirements can be broadly categorized into at least three groups: Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communications (URLCC), and Massive Machine Type Communication (mMTC) applications [36]. The automation of network operations is necessary to manage the complexity of network slicing, and ML techniques are being positioned as very promising solutions in this regard. From a business standpoint, it is projected that a $200 billion opportunity for CSPs will be generated from network slicing [37], and private and DCML techniques will play a significant role.

A. Experiments

In the experiment, network traffic data is generated using the Free5GC, a 5G open-source project [38]. The data and model architecture used for the analysis are provided in [39]. In total, there are 20 clients and the performance of the trained models is evaluated through the Mean Squared Error (MSE) (regression). For network slicing, the data and model architecture are from the recent work [40], showing the best Deep Neural Network (DNN) for network slicing. The performance is evaluated through accuracy (classification) and in total, there are 10 clients.

In all the experiments, the number of global epochs/communication rounds is set to 100. FL, SL, SFL, and centralized learning are considered with different levels of privacy. The privacy budgets, ε, are $0.1, 0.3, 0.5, 0.7, 1, 3, 5, 7, 9, 10$, and training with no DP is also considered. The privacy is applied by the participants (LDP) to tackle the threat model through DP-SGD which is (ε, δ)-DP [30]. The choice of the privacy budget follows the recommendation in [41, Section 5.2], with $\varepsilon \leq 1$ considered strong formal privacy guarantees, $1 < \varepsilon \leq 10$, reasonable privacy guarantees, and $\varepsilon > 10$, weak to no formal privacy guarantees. Hence, ε is taken between 0.1 and 10. For all the experiments, $\delta = 10^{-6}$.

B. Results and Discussion

Figure 1 and Figure 2 show the accuracy and MSE values corresponding to each DP-DCML technique and privacy level in the context of network slicing and network traffic analysis

respectively. The centralized learning is used as a baseline for comparison. For network slicing, higher ε values lead to better accuracy eventually matching No DP. Lower ε values result in a drop of about 25% (75% accuracy), indicating a good trade-off between accuracy and that high level of privacy. In network prediction analysis, MSE of the No DP converges to about 2.27. Lower privacy budgets, $\varepsilon = 0.1, 0.3$ yield the highest MSE of 3.06, which is not significantly different from the smallest MSE, 2.27. All these indicate the feasibility of DP in centralized learning.

In FL, for network slicing, all models with DP have similar performance after 20 communication rounds and converge to approximately 75% accuracy level. However, with No DP, the model converges to 100% as in the case of centralized learning. Here again, a high level of privacy can be achieved without the total degradation of the models' performance. This is also the case for network traffic analysis with the introduction of DP showing good performance. In SL, for both network slicing and network traffic analysis, DP makes the models less stable. Although there is an increasing trend in the performance, there are a lot of fluctuations but with the same level of privacy, they even perform better than FL and SFL in general. It is possible that increasing the communication rounds can lead to a stable convergence. This will be investigated in future work. For SFL network traffic analysis, the models achieve comparable results as those of FL, however, those in SFL, converge faster. For network slicing, SFL shows the most promising performance among the DCML approaches, with the models converging to over 80% for even the highest privacy levels.

Among, the three DCML techniques considered, SFL seems to be the most promising. In applications requiring FL, it can still be used as its performance was also good. However, more investigation is needed for SL. Small privacy budgets can be used as larger budgets do not perform significantly better. Overall, it's feasible to combine DP with DCML for robust privacy in collaborative learning. The goal was to investigate how the three DCML approaches react to DP. In the end, FL and SFL are recommended for use. However, it is suggested that more investigations should be done for SL. With respect to computation overhead, no significant difference was observed with the introduction of DP.

VI. Conclusion and Outlook

This work investigated the combination of Differential Privacy (DP) and Distributed Collaborative Machine Learning (DCML) techniques within the context of wireless mobile communication, specifically focusing on network traffic analysis and network slicing. The study aimed to assess the potential of this approach for enhancing both privacy and performance in wireless networks. Federated Learning (FL) and Splitfed Learning (SFL) approaches demonstrated positive outcomes in terms of maintaining data privacy and delivering satisfactory utility. However, it's worth noting that Split Learning (SL) did not exhibit the same level of performance as FL and SFL, suggesting that additional research and refinement are necessary to validate its effectiveness in this specific context. In conclusion, DP combined with DCML, particularly FL and SFL, holds significant potential for advancing network traffic analysis, network slicing, and wireless mobile communication as a whole. These ongoing efforts promise to reshape the future of wireless network security and performance and will be the subject of future studies.

Acknowledgment

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Forderkennzeichen 16KIS1283, AI-NET PROTECT and 16KIS1841K, ALPAKA). The authors alone are responsible for the content of the paper.

References

[1] P. Vepakomma, O. Gupta, T. Swedish, and R. Raskar, "Split learning for health: Distributed deep learning without sharing raw patient data," *CoRR*, vol. abs/1812.00564, 2018. arXiv: 1812.00564. [Online]. Available: http://arxiv.org/abs/1812.00564.

[2] J. Konečnỳ, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[3] C. Thapa, P. C. M. Arachchige, S. Camtepe, and L. Sun, "Splitfed: When federated learning meets split learning," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 36, 2022, pp. 8485–8493.

[4] C. Fung, C. J. Yoon, and I. Beschastnikh, "The limitations of federated learning in sybil settings," in *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, 2020, pp. 301–316.

[5] Z. Zhang, R. Yang, X. Zhang, C. Li, Y. Huang, and L. Yang, "Backdoor federated learning-based mmWave beam selection," *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6563–6578, 2022.

[6] A. Narayanan and V. Shmatikov, "How to break anonymity of the netflix prize dataset," *arXiv preprint cs/0610105*, 2006.

[7] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*, Springer, 2006, pp. 1–12.

[8] Ú. Erlingsson, V. Pihur, and A. Korolova, "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response," in *Proceedings of the 21st ACM Conference on Computer and Communications Security*, Scottsdale, Arizona, 2014. [Online]. Available: https://arxiv.org/abs/1407.6981.

[9] J. Near, "Differential Privacy at Scale: Uber and Berkeley Collaboration," in *Enigma 2018 (Enigma 2018)*, Santa Clara, CA: USENIX Association, Jan. 2018. [Online]. Available: https://www.usenix.org/node/208168.

[10] R. Jarmin, "Census Bureau adopts cutting edge privacy protections for 2020 Census," *Director's Blog*, vol. 15, 2019.

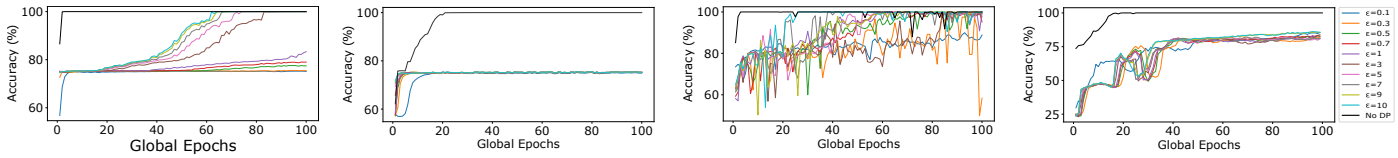
[11] "Learning with Privacy at Scale Differential," 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:43986173.

[12] O. Gupta and R. Raskar, "Distributed learning of deep neural network over multiple agents," *Journal of Network and Computer Applications*, vol. 116, pp. 1–8, 2018.

[13] A. Abedi and S. S. Khan, "Fedsl: Federated split learning on distributed sequential data in recurrent neural networks," *arXiv preprint arXiv:2011.03180*, 2020.

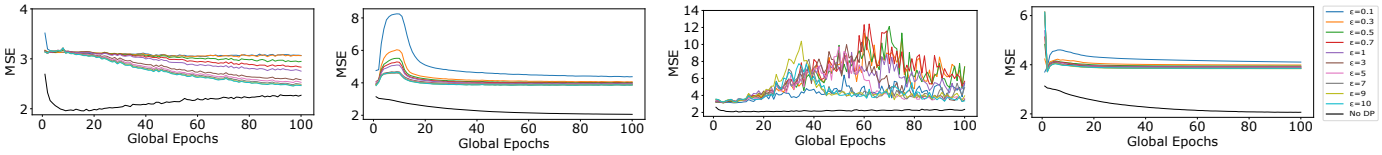
[14] S. P. Sanon, R. Reddy, C. Lipps, and H. D. Schotten, "Secure Federated Learning: An Evaluation of Homomorphic Encrypted Network Traffic Prediction," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 2023. DOI: 10.1109/CCNC51644.2023.10060116.

[15] S. P. Sanon, C. Lipps, and H. D. Schotten, "Fully Homomorphic Encryption: Precision Loss in Wireless Mobile Communication," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2023.



(a) Centralised (b) Federated learning (c) Split learning (d) Split federated learning

Figure. 1: Performance evaluation (accuracy) of DP-DCML methods in network slicing across 100 communication rounds with varying ε values.



(a) Centralised (b) Federated learning (c) Split learning (d) Split federated learning

Figure. 2: MSE analysis of DP-DCML methods in network traffic analysis across 100 communication rounds with varying ε values.

[16] Y. Yang, Z. Zhang, Y. Tian, Z. Yang, C. Huang, C. Zhong, and K.-K. Wong, "Over-the-Air Split Machine Learning in Wireless MIMO Networks," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 4, pp. 1007–1022, 2023. DOI: 10.1109/JSAC.2023.3242701.

[17] S. Wang, X. Zhang, H. Uchiyama, and H. Matsuda, "HiveMind: Towards Cellular Native Machine Learning Model Splitting," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 2, pp. 626–640, 2022. DOI: 10.1109/JSAC.2021.3118403.

[18] S. Niknam, H. S. Dhillon, and J. H. Reed, "Federated learning for wireless communications: Motivation, opportunities, and challenges," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.

[19] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[20] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning," *Ieee Network*, vol. 33, no. 5, pp. 156–165, 2019.

[21] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[22] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[23] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*, Springer, 2006, pp. 265–284.

[24] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Advances in Cryptology-EUROCRYPT 2006: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28-June 1, 2006. Proceedings 25*, Springer, 2006, pp. 486–503.

[25] I. Mironov, "Renyi differential privacy," in *2017 IEEE 30th computer security foundations symposium (CSF)*, IEEE, 2017, pp. 263–275.

[26] J. Dong, A. Roth, and W. J. Su, "Gaussian differential privacy," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 84, no. 1, pp. 3–37, 2022.

[27] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, IEEE, 2007, pp. 94–103.

[28] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" *SIAM Journal on Computing*, vol. 40, no. 3, pp. 793–826, 2011.

[29] H. Wang, Q. Zhao, Q. Wu, S. Chopra, A. Khaitan, and H. Wang, "Global and local differential privacy for collaborative bandits," in *Proceedings of the 14th ACM Conference on Recommender Systems*, 2020, pp. 150–159.

[30] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

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

[32] J. Jeon and J. Kim, "Privacy-sensitive parallel split learning," in *2020 International Conference on Information Networking (ICOIN)*, IEEE, 2020, pp. 7–9.

[33] S. Truex, L. Liu, K.-H. Chow, M. E. Gursoy, and W. Wei, "LDP-Fed: Federated learning with local differential privacy," in *Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking*, 2020, pp. 61–66.

[34] D. Pasquini, G. Ateniese, and M. Bernaschi, "Unleashing the tiger: Inference attacks on split learning," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 2113–2129.

[35] O. Li, J. Sun, X. Yang, W. Gao, H. Zhang, J. Xie, V. Smith, and C. Wang, "Label leakage and protection in two-party split learning," *arXiv preprint arXiv:2102.08504*, 2021.

[36] M. Series, "IMT Vision–Framework and overall objectives of the future development of IMT for 2020 and beyond," *Recommendation ITU*, vol. 2083, no. 0, 2015.

[37] M. J. J, *Network slicing: A USD 200 billion opportunity for CSPs*, https://www.ericsson.com/en/blog/2021/5/network-slicing-a-usd-200-billion-opportunity-for-csps, Accessed: 2023-08-25.

[38] *free5gc*, https://www.free5gc.org/, Accessed: 2023-08-02.

[39] S. P. Sanon, J. N. A. Tetteh, and H. D. Schotten, "Distributed Collaborative Learning in Wireless Mobile Communication," in *Proceedings of the 21st ACM International Symposium on Mobility Management and Wireless Access (MobiWac'23)*, 2023, pp. 1–5. DOI: 979-8-4007-0367-6/23/10.

[40] H. U. Rashid and S. H. Jeong, "Deep Learning-based Network Slice Recognition," in *2023 Fourteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2023, pp. 297–299. DOI: 10.1109/ICUFN57995.2023.10199606.

[41] N. Ponomareva, S. Vassilvitskii, Z. Xu, B. McMahan, A. Kurakin, and C. Zhang, "How to DP-fy ML: A Practical Tutorial to Machine Learning with Differential Privacy," in *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2023, pp. 5823–5824.