INTERSPEECH 2023
20-24 August 2023, Dublin, Ireland

Differential Privacy Enabled Dementia Classification: An Exploration of the Privacy-Accuracy Trade-off in Speech Signal Data

Suhas BN, Sarah Rajtmajer, and Saeed Abdullah

Pennsylvania State University, USA
{suhas,smr48,saeed}@psu.edu

Abstract

Early detection of dementia is critical for effective symptom management. Recent studies have aimed to develop machine learning (ML) models to identify dementia onset and severity using language and speech features. However, existing methods can lead to serious privacy concerns due to sensitive data collected from a vulnerable population. In this work, we aim to establish the privacy-accuracy tradeoff benchmark for dementia classification models using audio and speech features. Specifically, we explore the effects of differential privacy (DP) on the training phase of the audio model. We then compare the classification accuracy of DP and non-DP models using a publicly available dataset. The resultant comparison provides useful insights to make informed decisions about the need for balancing privacy and accuracy tradeoff for dementia classification tasks. Our findings have implications for real-world deployment of ML models to support early detection and effective management of dementia.

Index Terms: speech classification, dementia, differential privacy

1. Introduction

Dementia is a chronic neurodegenerative disorder that leads to cognitive and functional decline [1], including memory loss, cognitive impairment, and worsening communication and language skills. More than 55 million individuals worldwide have dementia, with nearly 10 million new cases diagnosed annually [1]. It is currently the seventh leading cause of mortality among all illnesses and one of the significant causes of impairment and reliance among the elderly [1]. There is currently no cure for dementia. Early detection of dementia is, thus, critical for effective symptom management and delaying cognitive and functional decline [2].

Currently, dementia detection uses different assessment methods, including cognitive assessments (e.g., Mini-Mental State Examination — MMSE [3]), self-report questionnaires, and neuroimaging (e.g., Positron Emission Tomography — PET [4]). However, these diagnosis methods can be infrequent and time-consuming [5], which can hinder the early detection of dementia. Furthermore, the lack of accessible methods can be particularly problematic for individuals living in remote locations. As such, there is an urgent need to develop methods that can get deployed at scale without burdening individuals.

Research shows that speech or language usage changes can indicate an early sign of cognitive decline [6]. Recent studies have leveraged language and speech characteristics to develop novel machine learning-based approaches to identify dementia onset [7, 8, 9, 10, 11, 12]. The AAAI 2022 hackallenge focused on developing methods to identify dementia and mild cognitive impairment using two public datasets including the Pittsburgh (Pitt) corpus [13, 14] and the Wisconsin Longitudinal Study (WLS) corpus [15]. The winning team [16] developed an ensemble called ACOUSTICS using a multimodal speech and text combination. They converted audio data to log mel spectrograms, which allowed them to exploit Spatiotemporal structures and relations in the speech data.They achieved an accuracy of 94.2% for the datasets.

While these methods show early promises, privacy remains a serious concern. For example, the spectrogram-based features can potentially be used to reconstruct speech content [17, 18, 19, 20]. Specifically, it is critical to assess and address the resultant privacy concerns given the data is collected from a vulnerable population. However, there has not been much work yet focusing on how to balance the privacy and accuracy tradeoff for these models. This paper aims to address this gap by exploring. differential privacy (DP) for deep learning (DL) classification. Specifically, we will compare how the results vary if we use a privacy-preserving methodology (DP + DL + spectrograms) versus state-of-the-art (DL + spectrograms) models.

The core principle of Differential Privacy is that model training can be achieved by accessing the gradients of the loss concerning each parameter. If this access preserves the differential privacy of the training data, the resulting model does too, according to the post-processing property of differential privacy. By incorporating noise into the optimizer that examines parameter gradients, the complexity can be concealed. While prior work has explored DP-SGD and similar privacy-accuracy tradeoffs, this study presents two novel contributions: i) demonstrating the feasibility of using DP-SGD for dementia classification with speech data; and ii) investigating the privacy-accuracy benchmark for dementia onset and severity prediction. The focus of this work is to apply Differential Privacy (DP) to understand its impact on performance and the privacy-accuracy tradeoff.

2. Differential Privacy

Differential Privacy (DP) is a mathematical theory that provides guarantees for the privacy of user information [21]. The goal of DP is to minimize the impact of any individual's data on the general outcome so that the same conclusions can be drawn regardless of whether or not an individual's data was included in the analysis's input. DP provides privacy guarantees resistant to a wide range of privacy attacks as data evaluations grow.

In this work, we use the differentially private stochastic gradient descent (DP-SGD) based on prior works [22, 23, 24]. In this paper, we focus on applying the DP-SGD method to the problem of speech data classification and exploring the effects of DP on the classification accuracy, which has not been thor-

10.21437/Interspeech.2023-575

oughly investigated in previous literature. Typically, the SGD optimizer trains iteratively. A small number of training examples (a.k.a "minibatch") are sampled from the training data at every iteration. The optimizer then computes the average model error on these examples and differentiates this average error concerning each model parameter to obtain a gradient vector. The final step involves updating the model parameters (θ_t) by subtracting this gradient (∇_t) multiplied by the learning rate (η). Mainly, two modifications are performed in DP-SGD to obtain differential privacy:

1. Gradients are computed per sample (rather than averaging over samples) and are clipped to control the sensitivity.
2. Spherical Gaussian noise b_t is added to their sum to obtain the indistinguishability needed for DP.

The update step can be written as follows:

$$\theta_{t+1} \leftarrow \theta_t - \eta \cdot (\nabla_t + b_t) \tag{1}$$

The proposed approach is seen in Fig. 1.

3. Related Work

In recent years, there has been some significant progress in developing machine learning models for assessing dementia onset using audio and text features [7, 8, 9, 10, 11, 12].

Luz et al. [25] developed the ADReSS challenge dataset to support standardized model development and evaluation focusing on dementia assessment. Some works have used this dataset recently [26, 27]. The application of differential privacy has gained a lot of interest in recent years as a way to ensure that sensitive data is protected while still being useful for analysis. Abadi et al. [24] investigated the privacy-utility tradeoff in deep learning, using differentially private stochastic gradient descent to train deep neural networks on MNIST and CIFAR-10. They found that the level of privacy protection provided by differential privacy can be increased by increasing the magnitude of the noise added to the data, but at the cost of decreased accuracy.

Fletcher et al. [28] provide a detailed overview of differential privacy techniques in decision tree classification, focusing on the use of Laplace noise as a privacy mechanism and exploring the effect of different epsilon values on privacy and accuracy. Epsilon (ϵ) is a privacy parameter in differential privacy that controls the strength of privacy guarantees provided by the model. We explain more in section 5 They noted that smaller epsilon values could lead to higher privacy but lower accuracy, while larger epsilon values could result in higher accuracy but lower privacy. Fan et al. [29] investigated the use of local differential privacy in data centers, specifically in privacy-preserving classification tasks. They evaluated the impact of different epsilon values on classification accuracy and find that increasing epsilon values could improve accuracy but at the cost of reduced privacy. Ha et al. [30] provided a comprehensive overview of differential privacy techniques in deep learning, including various methods of injecting noise to safeguard privacy, such as using Gaussian noise. They also examined the effect of different epsilon values on model privacy and accuracy, revealing that increasing epsilon values could lead to a reduction in model privacy while improving accuracy. Zhao et al. [31] conducted a survey of differential privacy techniques for unstructured data content, such as text and multimedia data. They discussed the use of differential privacy in various applications, including data analysis and machine learning, and examine the effect of different privacy parameters, such as delta and sigma, on privacy and accuracy. They found that smaller delta values could result in higher privacy but lower accuracy, while larger delta values could lead to higher accuracy but lower privacy. Finally, Yang et al. [32] proposed a privacy-preserving spoken command classification framework using differential privacy and adversarial autoencoders. They evaluated the effect of different epsilon values on privacy and accuracy and compare their framework with other differential privacy approaches. Their results show that increasing epsilon values could improve classification accuracy but at the expense of reduced privacy.

Overall, selecting specific values for privacy parameters such as epsilon, delta, sigma, and alpha depend on the context of the application, the desired level of privacy protection, and the tradeoff between privacy and accuracy. Privacy parameters can be adjusted to control the strength of privacy guarantees provided by the model, while other parameters can be used to find the balance between privacy and accuracy that best suits the application at hand.

In this work, we build on these studies and investigate the privacy-accuracy tradeoff in the context of speech data classification for dementia detection. We propose a novel approach to classify speech data and explore the effects of DP on the accuracy of the classification results. Our aim is to establish a privacy-accuracy benchmark for this specific use case and provide insights for developing practical AI-based analysis pipelines for identifying dementia and related applications.

In summary, our work contributes to the growing body of research on machine learning for dementia detection, with a particular focus on the privacy-accuracy tradeoff in the context of differential privacy. We think that our study provides valuable insights into developing accurate and privacy-preserving models for dementia detection and related healthcare applications.

4. Materials and Methods

4.1. Dataset: DementiaBank Pitt and WLS Corpora

Tradeoffs between privacy and accuracy in DP are well-known to be dependent on the dataset and models. We have tackled this in this work through the use of two different datasets: The Pitt and WLS corpora. The dataset consists of participants' demographic information, including diagnostic data (e.g., MMSE) and audio recordings. The audio comprises of participants conducting the "Cookie Theft" task of the Boston Diagnostic Aphasia Exam [33], in which they were asked to describe everything they saw occurring in the picture. For decades, the "Cookie Theft" task has been used to identify pragmatic markers of diseases with recurrent cognitive-linguistic impairments such as dementia [34, 35, 36]. Metadata from both datasets provide diagnostic information (e.g., diagnostic code, MMSE score, and fluency score).

4.2. Data Pre-processing

For the Pitt corpus labeling, we utilized the Mini-Mental State Examination (MMSE) [3] to differentiate between healthy controls and individuals with dementia. This approach was chosen for two reasons. Firstly, MMSE is a well-established clinical measure of cognitive function for various populations [37]. Secondly, the MMSE variable had fewer missing values than other variables in the dataset. The threshold of 24 for MMSE was chosen based on previous research demonstrating its effectiveness in distinguishing between different cognitive states [16].

The corpus initially contained 292 participants with 552 audio recordings. As some participants' cognitive functions may change over time, we labeled their audio recordings instead of the participants themselves. We removed 93 of 552 audio files with missing MMSE scores, resulting in 242 audio files for healthy controls and 217 for individuals with dementia. We randomly selected 323 audio files (152 dementia and 171 non-dementia) from the Pitt corpus as the training set, while the remaining 136 audio files (65 dementia and 71 non-dementia) were used as the test set. For the WLS corpus labeling, we used verbal fluency to distinguish between healthy controls and individuals with dementia, following a similar approach as in previous work [38]. Participants completed two verbal fluency cognitive tests, naming as many items in a specified category (animals and food in this case) as possible within 1 minute. Research suggests that verbal fluency tests can effectively manifest dementia in clinical settings [39]. To account for age-related declines in fluency, we used progressively decreased cutoff fluency scores for participants of higher age, with cutoffs of 16, 14, and 12 for participants aged less than 60, between 60-79, and over 79, respectively. Using this approach, we identified 23 participants with dementia and 93 healthy controls in the WLS corpus. We used the same train-test split approach for the Pitt corpus, resulting in 79 participants (16 dementia and 63 non-dementia) in the training set, and 37 participants (7 dementia and 30 non-dementia) in the test set.

4.3. Feature Extraction

To preprocess the audio, we first converted the file format from mp3 to wav. The audio data was then downsampled from 44.1 kHz to 16 kHz, which is within the range of human speech (0-8 kHz) and reduces the file size while preserving valuable information. We used the provided timestamp data (i.e., participant start-stop times in .cha files) to trim the corresponding audio files, retaining only the participant's speech information. Finally, we extracted log-mel spectrogram features using overlapping windows with a duration of 1-second [40].

5. Speech Model

5.1. Non-Differentially Private Model

In this work, we use the ResNet-18 model to classify participants based on speech using log-mel spectrogram features. We make use of the Stochastic Gradient Descent (SGD) optimizer. We use a five-fold cross-validation setup for the experiments and the resultant model has an average accuracy of 94.2% (S.D 2.8%), the equal error rate is 0.32, and the AUC score is 0.918.

5.2. Differentially Private Model

The same experiment with spectrograms was conducted using the ResNet-18 architecture for the differential private case. The main difference is using the DP-SGD optimizer instead of the SGD optimizer. We focus on a few hyperparameters for performing the experiments as described below in more detail.

A privacy library within PyTorch called Opacus has been used for the experiments. In this work, we focus on three specific parameters:

1. Delta (δ): The target δ of the (ϵ,δ)-differential privacy guarantee. Generally, it is set to be less than the inverse of the size of the training dataset. In this work, δ is 3e-4.
2. Epsilon (ϵ): The maximum distance between a query on dataset I/P and the same query on dataset I/P minus 'X' samples. It is a metric of privacy loss at a differential change in data (i.e., adding or removing one entry). Epsilon is also known as the privacy parameter or the privacy budget. Motivating on prior work [41], we set out to explore the effect of ϵ and on applying it in practice. In this work, we have chosen the following values of epsilon: [0.1, 0.5, 1, 5, 10, 50, 100]. When $\epsilon \rightarrow \infty$, we have a non-differentially private case.
3. Max Grad Norm (C): The maximum L2 norm of per-sample gradients before the averaging step aggregates them. We have chosen the following values: [0.1, 0.5, 1, 5, 10].

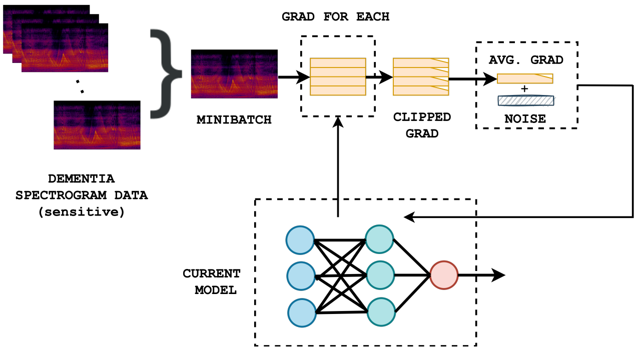

Figure 1: *The Differential Privacy methodology used in this work selects minibatches from the training data, clips the calculated gradients and adds gaussian noise. This is repeated for the duration of the training phase.*

Table 1: *Accuracy for varying values of ϵ and C with constant δ. As ϵ increases, accuracy is observed to improve. Bold numbers show the best performance per ϵ row.*

$\downarrow\epsilon\backslash$C$\rightarrow$	C= 0.1	C= 0.5	C= 1	C= 5	C= 10
ϵ = 0.1	**45.94**	45.35	42.83	44.58	45.34
ϵ = 0.5	46.26	**47.38**	46.72	45.95	46.21
ϵ = 1	48.29	**51.5**	48.62	51.48	48.75
ϵ = 5	**58.98**	57.73	53.41	57.72	55.19
ϵ = 10	60.28	59.72	**60.32**	59.71	59.46
ϵ = 50	65.87	66.44	**67.46**	64.54	65.89
ϵ = 100	67.03	**69.25**	68.78	68.46	68.92

Sigma (σ) is a privacy parameter that controls the amount of noise added to the function being computed in DP. It is calculated based on the desired level of privacy (ϵ), the desired level of confidence (δ), and the sensitivity of the function being computed. The sensitivity is the maximum amount the output can change when a single input is added or removed. σ is defined as the ratio of the sensitivity to ϵ. Another Python script was written to obtain the mean and standard deviation of the dataset. The values are computed with a modest privacy budget. See Section 8 for the code. Based on the above hyperparameter values, we perform a grid search for the best value pair for a fixed delta value of 3e-4 (set as per the dataset size). The results for different values of ϵ and C for a fixed δ are tabulated in Table 1.

5.3. Model Evaluation

For the audio features, we considered all the spectrogram images of a given subject ID, performed a prediction, and obtained a list of predictions for each image — dementia (1) or healthy control (0).

Table 2: *ϵ v/s σ values for the experiments*

ϵ	0.1	0.5	1	5	10	50	100
σ	130	10.78	16.25	2.22	1.37	0.77	0.37
ϵ*σ	13	5.39	16.25	11.1	13.7	38.5	37.2

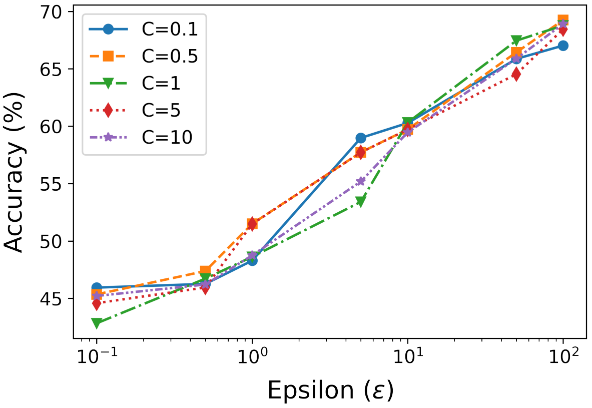

Figure 2: *Privacy-Accuracy Tradeoff in Dementia Prediction using DP-SGD: Investigating Hyperparameter Impact on Combined WLS and Pitt Corpus Datasets*

6. Discussion

Table 1 and Fig. 2 show that the accuracy increases as we increase the privacy budget ϵ. As $\epsilon \rightarrow \infty$, we have a non-DP case where the accuracy $\rightarrow$ 94.2%. It is, thus, a case of how much of a privacy budget one is willing to allocate for a given task. The table shows the accuracy of a binary classification system for different values of the parameters ϵ and C, where ϵ controls the trade-off between accuracy and privacy, and C controls the regularization of the classification model. The table suggests that the value of ϵ has a significant effect on the accuracy of the system, while the effect of C is less pronounced. At $\epsilon = 100$, the accuracy $\approx$ 70%. The results also suggest that the privacy-accuracy tradeoff may vary depending on the dataset and model used. This highlights the importance of evaluating the trade-off for each case and selecting the best hyperparameters for that specific scenario. Examining the upward trend between ϵ v/s σ in Table 2 leads to the hypothesis: “Increasing θ, the Privacy-Noise Coupling Factor (product of ϵ and σ), may yield higher utility in DP mechanisms.” Investigating this necessitates context-specific analysis of utility-privacy trade-offs and metric evaluation for ϵ (privacy loss) and σ (noise intensity) pairs.

Even though the current method of using DP-SGD for different privacy budgets shows a significant difference in accuracy compared to the non-DP method, there is much scope for future work. Differential Privacy has already been used to protect the data of millions of Americans [42]. While the relationship between privacy and accuracy in differential privacy is well understood, the optimal value of the privacy budget remains a matter of ongoing debate. In this discussion, we examine the implications of varying privacy budgets on the accuracy and privacy of data analysis. One valuable insight is that accurate data analysis and privacy protections are not necessarily mutually exclusive. By carefully designing data analysis systems incorporating privacy-preserving techniques, one can balance the need for accurate analysis with privacy protection. This can help to build trust between researchers and subjects and may encourage more people with dementia to participate in research studies.

A recent work examined the use of different epsilon values (privacy parameters) across different organizational projects and how it affected privacy [43]. It is interesting to note that privacy parameters used in different organizations are either incomplete or not specified, making it challenging to assess the effectiveness of privacy-preserving measures. In some cases, the privacy unit needs to be specified, which makes it difficult to determine how individual users’ data is being protected. Furthermore, some of the privacy parameters used may need to provide more protection for user privacy, given the sensitivity of the data being collected. Research has indicated that data privacy is at risk when ϵ exceeds 1 [24]. News reports have suggested that certain widely-used tech services have epsilon values of 6 and 14, respectively [44, 45]. If a user were to upload medical data, an analyst could determine whether the individual had a particular condition with 50% certainty after just one upload and with virtual certainty after two days of uploads. Similarly, in this work, ϵ = 1 still gave us a 51.5% chance of inferring sensitive information, which, when queried multiple times a day, would compromise user privacy. It is, thus, important to carefully consider the implementation of differential privacy to ensure that user data is protected while still providing valuable insights.

One potential approach to balancing privacy and accuracy could be to use a dynamic privacy budget, which adapts to the sensitivity of the data being analyzed. Similarly, combining differential privacy in conjunction with other privacy-enhancing techniques, such as data masking or homomorphic encryption, could be considered. By combining multiple privacy-enhancing techniques, a better trade-off may be possible. Finally, the choice of privacy budget is not solely dependent on the specific task. Other factors, such as legal and regulatory requirements, may influence the choice of privacy budget.

7. Conclusion

In this paper, we compared differentially private (DP) and non-differentially private (non-DP) methods to classify subjects with dementia and healthy controls using spectrogram images. Our results showed that as the privacy budget increased, the accuracy tended towards the non-DP value, highlighting the need to balance data privacy and accurate analysis. Our study contributes to the growing research on machine learning for dementia detection, demonstrating the effectiveness of differential privacy in preserving sensitive personal information. With careful optimization, differential privacy provides a practical solution for privacy-preserving dementia classification using speech data. Our work has important implications for healthcare, stimulating further research into privacy-accuracy tradeoffs and new ideas for balancing privacy and accuracy in machine learning.

8. Data and Code

1. Data can be requested from DementiaBank [13]
2. Code: `https://github.com/suhasbn/SpeechDP`

9. References

[1] World Health Organization, “Dementia Fact Sheet kernel description,” https://www.who.int/news-room/fact-sheets/detail/dementia, 2021, accessed: 2022-04-20.

[2] R. Briggs, S. P. Kennelly, and D. O’Neill, “Drug treatments in alzheimer’s disease,” *Clinical medicine*, vol. 16, p. 247, 2016.

[3] M. F. Folstein *et al.*, "The mini-mental state examination," *Archives of general psychiatry*, vol. 40, no. 7, pp. 812–812, 1983.

[4] I. G. Stiell *et al.*, "The canadian c-spine rule for radiography in alert and stable trauma patients," *Jama*, vol. 286, 2001.

[5] G. Prabhakaran, R. Bakshi *et al.*, "Analysis of structure and cost in a longitudinal study of alzheimer's disease," *Journal of Health Care Finance*, vol. 44, no. 3, 2018.

[6] M. Antonsson, K. Lundholm Fors *et al.*, "Using a discourse task to explore semantic ability in persons with cognitive impairment," *Frontiers in Aging Neuroscience*, p. 495, 2021.

[7] J. Weiner *et al.*, "Speech-based detection of alzheimer's disease in conversational german." in *Interspeech*, 2016, pp. 1938–1942.

[8] A. Balagopalan, B. Eyre *et al.*, "To bert or not to bert: comparing speech and language-based approaches for alzheimer's disease detection," *arXiv preprint arXiv:2008.01551*, 2020.

[9] F. Haider, S. De La Fuente, and S. Luz, "An assessment of paralinguistic acoustic features for detection of alzheimer's dementia in spontaneous speech," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 2, pp. 272–281, 2019.

[10] L. Chen, H. H. Dodge, and M. Asgari, "Topic-based measures of conversation for detecting mild cognitive impairment," in *Proceedings of the conference. Association for Computational Linguistics. Meeting*, vol. 2020. NIH Public Access, 2020, p. 63.

[11] S. de la Fuente Garcia, C. W. Ritchie, and S. Luz, "Artificial intelligence, speech, and language processing approaches to monitoring alzheimer's disease: a systematic review," *Journal of Alzheimer's Disease*, vol. 78, no. 4, pp. 1547–1574, 2020.

[12] B. Eyre *et al.*, "Fantastic features and where to find them: detecting cognitive impairment with a subsequence classification guided approach," *arXiv preprint arXiv:2010.06579*, 2020.

[13] J. T. Becker *et al.*, "The natural history of alzheimer's disease: description of study cohort and accuracy of diagnosis," *Archives of neurology*, vol. 51, no. 6, pp. 585–594, 1994.

[14] H. Goodglass and E. Kaplan, *Boston diagnostic aphasia examination booklet*. Lea & Febiger, 1983.

[15] P. Herd *et al.*, "Cohort profile: Wisconsin longitudinal study (wls)," *International journal of epidemiology*, vol. 43, 2014.

[16] H. J. Han, B. N. Suhas, L. Qiu, and S. Abdullah, "Automatic classification of dementia using text and speech data," in *Multimodal AI in healthcare: A paradigm shift in health intelligence*. Springer, 2022, pp. 399–407.

[17] D. Griffin and J. Lim, "Signal estimation from modified short-time fourier transform," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 32, no. 2, pp. 236–243, 1984.

[18] N. Perraudin, P. Balazs, and P. L. Søndergaard, "A fast griffin-lim algorithm," in *2013 IEEE Workshop on Applications of Signal Processing to Audio and Acoustics*. IEEE, 2013, pp. 1–4.

[19] S. Ö. Arık, H. Jun, and G. Diamos, "Fast spectrogram inversion using multi-head convolutional neural networks," *IEEE Signal Processing Letters*, vol. 26, no. 1, pp. 94–98, 2018.

[20] P. Magron and T. Virtanen, "Online spectrogram inversion for low-latency audio source separation," *IEEE Signal Processing Letters*, vol. 27, pp. 306–310, 2020.

[21] C. Dwork *et al.*, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference, 2006.* Springer, 2006, pp. 265–284.

[22] S. Song *et al.*, "Stochastic gradient descent with differentially private updates," in *2013 IEEE Global Conference on Signal and Information Processing*. IEEE, 2013, pp. 245–248.

[23] R. Bassily, A. Smith, and A. Thakurta, "Private empirical risk minimization: Efficient algorithms and tight error bounds," in *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*. IEEE, 2014, pp. 464–473.

[24] M. Abadi *et al.*, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.

[25] S. Luz, F. Haider, S. de la Fuente *et al.*, "Alzheimer's dementia recognition through spontaneous speech: The adress challenge," *arXiv preprint arXiv:2004.06833*, 2020.

[26] R. Haulcy and J. Glass, "Classifying alzheimer's disease using audio and text-based representations of speech," *Frontiers in Psychology*, vol. 11, p. 624137, 2021.

[27] Z. Shah *et al.*, "Learning language and acoustic models for identifying alzheimer's dementia from speech," *Frontiers in Computer Science*, p. 4, 2021.

[28] S. Fletcher and M. Z. Islam, "Decision tree classification with differential privacy: A survey," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–33, 2019.

[29] W. Fan, J. He, M. Guo, P. Li, Z. Han, and R. Wang, "Privacy preserving classification on local differential privacy in data centers," *Journal of Parallel and Distributed Computing*, pp. 70–82, 2020.

[30] T. Ha, T. K. Dang *et al.*, "Differential privacy in deep learning: an overview," in *2019 International Conference on Advanced Computing and Applications (ACOMP)*. IEEE, 2019, pp. 97–102.

[31] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Computing Surveys (CSUR)*, vol. 54, no. 10s, pp. 1–28, 2022.

[32] C.-H. H. Yang *et al.*, "Pate-aae: Incorporating adversarial autoencoder into private aggregation of teacher ensembles for spoken command classification," *arXiv preprint arXiv:2104.01271*, 2021.

[33] H. Goodglass *et al.*, *BDAE: The Boston Diagnostic Aphasia Examination*. Lippincott Williams & Wilkins, 2001.

[34] L. Cummings, "Describing the cookie theft picture: sources of breakdown in alzheimer's dementia," *Pragmatics and Society*, vol. 10, no. 2, pp. 153–176, 2019.

[35] E. Giles *et al.*, "Performance on the boston cookie theft picture description task in patients with early dementia of the alzheimer's type: missing information," *Aphasiology*, vol. 10, 1996.

[36] H. Bird, M. A. L. Ralph *et al.*, "The rise and fall of frequency and imageability: Noun and verb production in semantic dementia," *Brain and language*, vol. 73, no. 1, pp. 17–49, 2000.

[37] T. N. Tombaugh and N. J. McIntyre, "The mini-mental state examination: a comprehensive review," *Journal of the American Geriatrics Society*, vol. 40, no. 9, pp. 922–935, 1992.

[38] Y. Guo *et al.*, "Crossing the "cookie theft" corpus chasm: applying what bert learns from outside data to the adress challenge dementia detection task," *Frontiers in Computer Science*, 2021.

[39] J. D. Henry, J. R. Crawford, and L. H. Phillips, "Verbal fluency performance in dementia of the alzheimer's type: a meta-analysis," *Neuropsychologia*, vol. 42, no. 9, pp. 1212–1222, 2004.

[40] B. N. Suhas and S. Abdullah, "Privacy Sensitive Speech Analysis using Federated Learning to Assess Depression," in *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2022, pp. 6272–6276.

[41] J. Lee and C. Clifton, "How much is enough? choosing ε for differential privacy," in *Information Security: 14th International Conference, ISC 2011, Xi'an, China, October 26-29, 2011. Proceedings 14*. Springer, 2011, pp. 325–340.

[42] J. Ficek, W. Wang, H. Chen *et al.*, "Differential privacy in health research: A scoping review," *Journal of the American Medical Informatics Association*, vol. 28, no. 10, pp. 2269–2276, 2021.

[43] D. Desfontaines, "A list of real-world uses of differential privacy," https://desfontain.es/privacy/real-world-differential-privacy.html, 2022, accessed: 2022-10-20.

[44] 9to5Mac, "Apple taking an 'immense risk' with user data thanks to poor implementation of differential privacy, say academics," https://9to5mac.com/2017/09/18/how-secure-is-apples-differential-privacy/, accessed: 2023-03-07.

[45] WIRED, "How One of Apple's Key Privacy Safeguards Falls Short," https://www.wired.com/story/apple-differential-privacy-shortcomings/, accessed: 2023-03-07.