Optimized Deep Learning for Enhanced Trade-off in Differentially Private Learning

P. Geetha
Department of CSE
Cambridge Institute of Technology
Bengaluru, India
geetharaghuraj@gmail.com

Chandrakant Naikodi
Department of Studies and Research in Computer Science
Davangere University
Bengaluru, India
nadhachandra@gmail.com

L. Suresh
Department of CSE
Cambridge Institute of Technology
Bengaluru, India
suriakls@gmail.com

Abstract-Privacy and data analytics are two conflicting domains that have gained interest due to the advancements of technology in the big data era. Organizations in sectors such as finance, healthcare, and e-commerce take advantage of the data collected, to help them enable innovative decision making and analysis. What is sidelined is the fact that the collected data have associated private data of the individuals involved, and may be exploited and used for unjustified purposes. Defending privacy and performing useful analytics are two sides of the same coin, and hence achieving a good balance between these is a challenging scenario. This paper proposes an optimized differentially private deep learning mechanism that enhances the trade-off between the conflicting objectives of privacy, accuracy, and performance. The goal of this paper is to provide an optimal solution that gives a quantifiable trade-off between these contradictory objectives.

Keywords-privacy; optimization; pareto-optimal; analytics

I. INTRODUCTION

Nowadays, privacy is a tough bargain. With the onset of digitization, online activities are on the rise and so is the increase in the risk of private information disclosure. Online services like shopping, trading, banking, and entertainment are sources of data collection that include sensitive information of the people involved. While not all these services target at the exploitation of personal information, certain applications use them to their benefit. For instance, online browsing information of people is utilized for providing personalized recommendations as a part of the marketing strategy. In healthcare, sensitive information such as disease conditions are used for research and analysis which in turn may be helpful for diagnostic research. Such usage scenarios can be extended to many fields. To safeguard privacy, data transformation methods are employed, which protect sensitive information, while still enabling useful analytics. This is easier said than done, since privacy defense and effective analysis conflict each other. Given the size of big data, the challenge becomes even bigger, rendering it a multi-objective perspective. A privacy preserving analytic system should be able to balance the multiple criteria of privacy-utility-performance. Numerous privacy mechanisms have been proposed that manage privacy preserving analytics for big data. They revolve around privacy algorithms namely k-anonymity [1] and its variants of k-anonymity and l-diversity [2]. K-anonymity methods apply data transformation techniques that make the data unidentifiable. In approaches based on k-anonymity, k determines the degree of anonymity and hence the choice of k is an important decision. Optimizing k can pave the way for better privacy, but at the cost of degradation in data utility. Moreover, optimization approaches have the added limitation of performance overhead.

With anonymization, a compromise solution is acceptable, provided preference is given to one of the objectives and this is attributed to the practical setting of the application. More recently, there has been a growing interest in the mathematical foundation provided by the privacy algorithm called differential privacy [3]. The core algorithm is specifically ε-differential privacy, after which relaxed variants have been proposed [4]. Companies such as Google [5] and Apple [5] have used the algorithm for protecting the privacy of their customers, thereby ensuring that they see only a transformed form of the original data. The basic notion of the algorithm is to protect private information of a user, irrespective of the user's participation or non-participation in data analysis. While the algorithm has been strongly recommended for privacy protection [5], only an equally stronger learning mechanism can provide worthwhile analytical results.

II. PAPER CONTRIBUTION

Deep learning [6] with differential privacy is a recently emergent domain that has many research applications in the

Corresponding author: P. Geetha

field of privacy preserving analysis. Specifically, the most likely developments in the domain may be:

- Optimizing epsilon for trade-off benefit.
- Developing an efficient learning technique to balance trade-off.
- Extending trade-off beyond privacy and quality of data analysis.

The core idea of the current paper is based on bridging the afore-mentioned research gap in differentially private learning. This paper is targeted at the second and third of the above cases. The main contributions of the paper are:

- Firstly, given the strong mathematical background of differential privacy, an optimized deep learning architecture is developed that enhances the efficiency of differentially private learning through effective hyperparameter optimization.
- Secondly, an attempt is made to consider privacy preserving analytics from the performance perspective and the triple trade-off between privacy, utility and performance is enhanced in comparison to the existing techniques.
- Thirdly, a single optimum solution for the problem is identified by adapting a prototypical decision-making strategy which is challenging in any multi-objective problem scenario.

III. BACKGROUND

Differential privacy [3, 7] is a notable algorithm used in the field of privacy preserving analysis. It was proposed in 2006 [3] and has been proven to provide strong mathematical guarantees for efficiently quantifying privacy. The key element behind the working of the algorithm is that the analysis of any dataset is not affected by the participation or non-participation of an individual. Alternately, it conveys the theory that information about any individual learnt from the data, remains effectively the same before and after analysis. Mathematically defining, the algorithm works by adding noise to data. The addition of random noise distorts data, thereby biasing the outcome of the analysis and preserving privacy. It is based on the probabilistic theory and promises that sensitive information of individuals in data is not affected by its use in any type of study. The most popular use of the algorithm is ε-differential privacy [3] in which epsilon (ε) defines a bound on the privacy loss. It can be used to formally quantify privacy loss and is used as the basis for effective analytics.

- Definition

A randomized algorithm *A* gives ε-differential privacy if for all data sets D′ and D″ that have a difference of one instance, and for any S⊆Range (A), (1) stands [3]:

$$\frac{Pr[A(D')\in S]}{Pr[A(D'')\in S]} \leq exp^{\varepsilon} \quad (1)$$

In (1), the datasets D′ and D″ follow the constraint ||D′ - D″|| ≤ 1 and epsilon is a positive real number, which quantifies privacy loss with change in data.

IV. MATHEMATICAL PROBLEM FORMULATION

The mathematical problem formulation is conceived as a multi-objective optimization problem and will be alternately referred to as multi-attribute or multi-criteria problem in the rest of this paper.

A. Mathematical Modeling of the Proposed Model

Consider *M* as the vector space of decision variables. Let *P*(*m*) and *U*(*m*) represent the objective functions to be maximized. Mathematically, the problem can be formulated as:

$$\max_{s.t. m\in M}\{P(m), U(m)\} \quad (2)$$

where *P*(*m*) and *U*(*m*) represent the privacy and utility of the system respectively. In the context of differential privacy, the problem is re-defined as:

$$\text{argmax}_{10^{-2}\leq\varepsilon\leq 10}\{min\varepsilon, acc\} \quad (3)$$

$$\text{where, } min\varepsilon = \frac{Pr[A(D')\in S]}{Pr[A(D'')\in S]} \leq exp^{\varepsilon} \quad (4)$$

$$acc(ni, c) = \frac{c}{Ni} * 100 \quad (5)$$

where *Ni* is the overall number of instances and *c* is the number of correctly classified instances.

B. Pareto-Optimality

When resolving a multi-attribute optimization problem, a solution that simultaneously achieves all objectives is not possible, since maximizing/minimizing one objective degrades the other. Consider a set of solutions $S = \{\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}, \ldots\ldots \overrightarrow{v_n}\}$ to a multi-attribute problem. A solution $\overrightarrow{v_1} \in V$ is said to be better than another solution $\overrightarrow{v_2} \in V$ if it satisfies the following condition:

$$f_i(\overrightarrow{v_1}) \geq f_i(\overrightarrow{v_2}) \forall i \in \{1,2,3 \ldots p\} \quad (6)$$

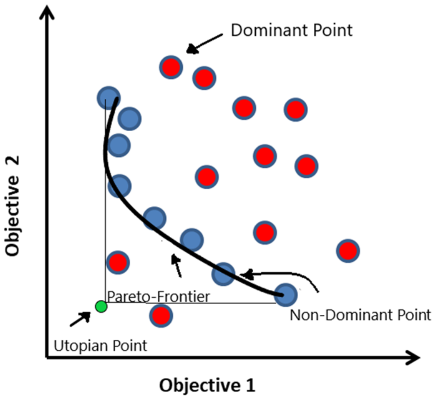

Fig. 1. Visualization of the Pareto-optimal front.

Such a set *S* is called a Pareto-optimal set [8], in which all solutions are possible candidates for becoming an optimal solution, but one cannot dominate the other, without degrading one of the objectives involved. Pareto-optimality is a common occurrence in multi-objective optimization problems. Figure 2 shows the general occurrence of Pareto-optimality in a two-dimensional Euclidean space.

V. DESIGN METHODOLOGY

This section describes the scheme of the proposed system. A differential privacy-based optimized deep learning neural network architecture for implementing privacy preserving learning is suggested. This approach addresses the twin challenges of privacy loss and efficiency of the learning technique. Deep learning frameworks for differential privacy are gaining importance for privacy preserving analytics. An appropriate blend of these techniques will be able to provide robust solutions for the problem of privacy preserving learning, primarily due to two reasons. Firstly, differential privacy is an algorithm that can provide strict data privacy guarantee. Thus, analysis on private data must incorporate complex learning architectures whose outcome can quantitatively substantiate data privacy guarantee. Hence this methodology develops a Bayesian optimized deep neural network architecture for private learning with accounting of epsilon that determines the privacy assurance offered by the model.

A. Overview of System Architecture

A deep neural network is trained on differentially private data, and the intended learning task is classification analysis. The model topology initiates with an embedding layer to handle the categorical parameters of the input data. The transformed input is reshaped, and layers are concatenated before passing to the dense layer. The topology then alternates between dense and normalization layers. Each dense layer has 1000 units. Batch normalization is carried out to stabilize the output structure. This architecture is considered as the standard learner. In the standard learner, these neural net parameters are chosen arbitrarily and they are fixed as the reference model against which the optimized variant will be compared. Since these parameters determine the strength of the learning process, a good combination of the parameters provides significant performance improvement. Specifically, in deep learning parlance, these parameters are known as hyperparameters [7]. Hyperparameter values have a deciding role in the learning process. Selecting optimal values for the hyperparameters is called hyperparameter optimization [7, 9]. Fine-tuning of the hyperparameters of the model can allow the privacy-utility-performance trade-off in a quantitatively principled fashion. In this work, the proposed architecture with tuned hyperparameters is referred to as DPBODL (Differentially Private Bayesian Optimized Deep Learner). The design of the system is shown in Figure 3.

B. Hyperparameter Optimization

Methods such as Grid Search and Random Search [7], search the entire space of available parameters to arrive at optimal values. These methods are costly and training a model using them is challenging. The use of genetic algorithms [10] for efficient optimization has also been reported. Bayesian optimization [7] reduces the time required for the parameter search which in turn limits the model training time, because only a selected set of parameters are chosen for a subsequent iteration, resulting in a search space which has the local optimal values from the previous evaluations. In this way, the method can efficiently select the global optimal hyperparameter set when the search terminates.

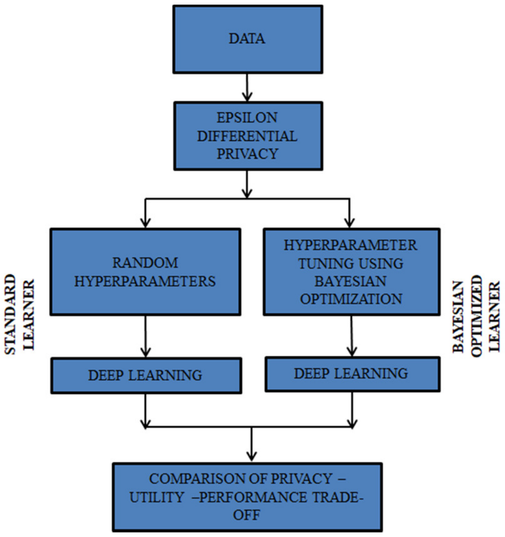
DATA
EPSILON DIFFERENTIAL PRIVACY
STANDARD LEARNER
RANDOM HYPERPARAMETERS
HYPERPARAMETER TUNING USING BAYESIAN OPTIMIZATION
BAYESIAN OPTIMIZED LEARNER
DEEP LEARNING
DEEP LEARNING
COMPARISON OF PRIVACY – UTILITY –PERFORMANCE TRADE-OFF

Fig. 2. DPBODL-design.

Although the hyperparameterized approach for non-private models has been used [11, 12], experimenting its efficiency for private deep learning models has far-reaching research possibilities. The proposed DPBODL exploits this possibility.

C. Steps for Optimizing the Deep Learner

Let H_q be the initial hyperparameter search space and *Acc* the classification accuracy. Let $\theta_{DPDNN}(X, H_q)$ be the objective function of the Differentially Private Deep Neural Network (DPDNN) with *X* as the input space.

- Step 1:

Initialize the search space with default hyperparameters to be tuned. They are chosen randomly at stage one of the iteration. The search space consists of the hyperparameter set : *Hq* = {learning rate, number of iterations, batch size, number of dense layers, number of dense nodes, number of input nodes, decay function}.

- Step 2:

If function values follow a Gaussian distribution, the optimization function is defined as:

$$Acc = \theta_{DPDNN}(X, H_q) \quad (7)$$

$$H_{opt} = \text{argmax}_X\{\theta_{DPDNN}(X, H_q)\} \quad (8)$$

- Step 3:

Calculate the maximum a posteriori hypothesis of the set of hyperparameters $P(Acc|H_{opt})$. The optimizer selects the hyperparameters that maximize the accuracy of the deep learner.

VI. EXPERIMENTAL SETUP

The deep learning model is trained and hyperparametrized using Tensorflow core 2.0 [13]. For the purpose of experimental evaluation, two different types of tabular data varying in size and dimension have been selected. The adult and diabetes datasets adapted from the UCI data repository [14] are used. Adult data are chosen since they are the de-facto benchmark for privacy related studies. The dataset provides 14 inputs that are a combination of categorical, numerical, and ordinal types. The target variable requires classification of data into two salaried classes, those belonging to "less than 50k" group and another belonging to the "greater than 50k" group. Diabetes dataset has 20 attributes containing categorical and numerical data with around 200,000 instances with presence /absence of disease condition as the target. For both the datasets, the optimization ranges of the different hyperparameters considered are shown in Table I.

TABLE I. FINE-TUNED HYPERPARAMETERS

Tuned hyperparameters	Range of values
Learning rate	<1e-4 ,1e-1>
Batch size	<1,28>
Number of dense layers	<1,5>
Number of dense nodes	<1,28>
No of input nodes	<1,512>
Decay function	adam decay
Activation function	<relu,sigmoid>

VII. EVALUATION

In this section, the performance of DPBODL is compared with the standard deep learner's. Epsilon, accuracy, and execution time were noted for both learners. The tabulation (Table II and Table III) shows the values of epsilon, accuracy, and execution time for adult and diabetes datasets respectively. The graphs in Figures 3 and 4 show the comparison of results between the standard learner and DPBODL for the two datasets. Maximizing the privacy and the utility of the analysis in the current context involves minimizing epsilon and maximizing the classification accuracy. The standard learner's performance for the two datasets is shown in Figure 3. Epsilon degrades with increasing accuracy and execution time ranges up to 600s. The DPBODL's performance is shown in Figure 4. The DPBODL achieves enhanced trade-off in comparison with the standard learner with reference to epsilon and accuracy. While DPBODL gives epsilon values ranging between <0.78, 5.34> for adult and <0.87, 8.34> for diabetes, it is apparent that the standard model's learning initiates with larger values for epsilon in the range <5, 11>. Similarly, the enhanced learning speed of the optimized learner is due to the optimization of the number of epochs for the training of the model. It can be observed that, on average, 3-6 epochs are required to give an accuracy of approximately 80% .On the other hand, the standard learner requires at least 10 epochs to give a starting accuracy of 80%. Essentially, DPBODL's enhanced performance is attributed to efficient hyperparameter optimization.

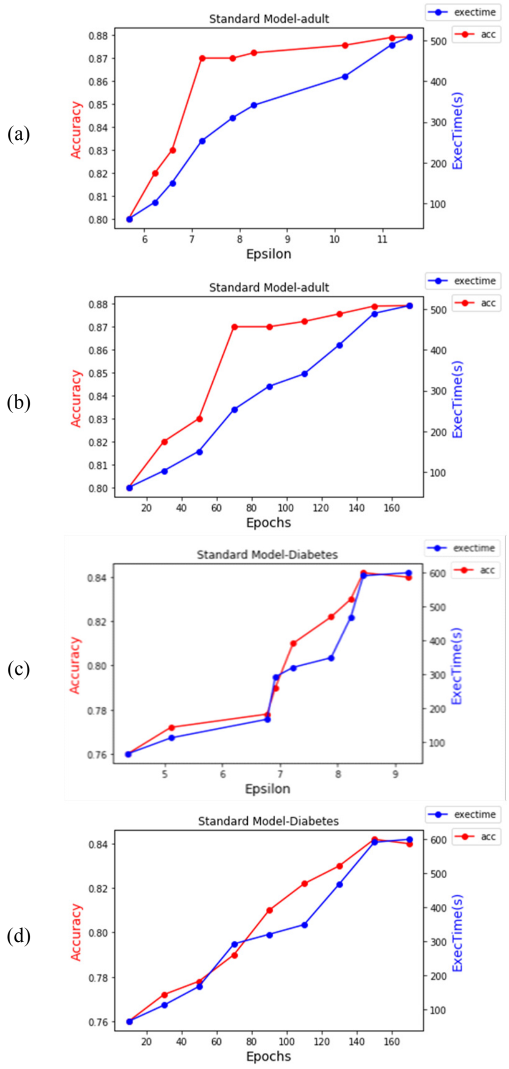

Fig. 3. Privacy-utility performance analysis-standard learner.

TABLE II. TRADE-OFF RESULTS-STANDARD LEARNER

Epochs	Adult data			Diabetes data		
	Epsilon	Classification accuracy	Execution time (s)	Epsilon	Classification accuracy	Execution time (s)
10	5.68	0.81	61.2	4.36	0.76	65.2
30	6.23	0.82	102.3	5.11	0.772	112.3
50	6.59	0.83	150.3	6.78	0.778	167.3
70	7.21	0.87	253.25	6.923	0.79	292.33
90	7.86	0.87	310.32	7.23	0.81	320.32
110	8.3	0.8723	340.89	7.89	0.822	348.77
130	10.21	0.8756	412.12	8.23	0.83	467.82
150	11.19	0.879	490.11	8.45	0.842	590.71
170	11.56	0.8792	509.12	9.23	0.84	599.42

TABLE III. TRADE-OFF RESULTS-DPBODL

Epochs	Adult data			Diabetes data		
	Epsilon	Classification accuracy	Execution time (s)	Epsilon	Classification accuracy	Execution time (s)
1	0.783	0.84	3.2	0.87	0.82	4.8
2	0.891	0.84	4.89	0.899	0.84	5.89
3	0.923	0.842	6.312	0.91	0.83	7.314
4	1.02	0.853	7.89	1.56	0.843	9.89
5	1.15	0.86	8.21	3.78	0.87	10.26
6	2.25	0.87	8.29	5.25	0.88	12.29
7	3.523	0.892	9.35	6.23	0.881	13.37
8	4.563	0.89	9.783	7.563	0.892	14.78
9	5.34	0.89	10.56	8.34	0.897	15.723

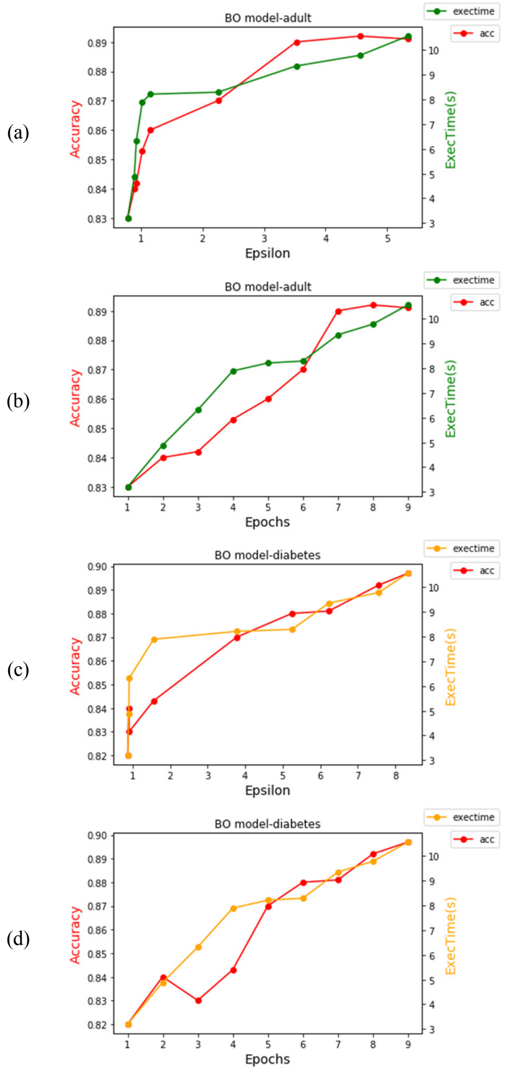

Fig. 4. Privacy-utility performance analysis- DPBODL.

VIII. COMPARATIVE ANALYSIS

This section compares the proposed DPBODL mechanism with the state-of-the-art techniques for privacy preserving analytics. For the purpose of comparative analysis, three different techniques have been chosen, namely Bayesian Optimized Diff Private Pareto (BO-Dpareto)[9], Privacy Preserving Deep Learning (PPDL)[10], and Linear Regression-Diff Private Convex Optimization (LR-DPCO) [15]. Both PPDL and BO-Dparteo have been chosen for the comparative study for two reasons. Primarily, these approaches use deep learning for privacy preserving learning. Secondly, tabular data for analysis are used, in comparison to many other approaches, which predominantly use image data. LR-DPCO uses shallow learning [16], but the algorithm's results are equivalent to many deep learning approaches and including them here ensures a fair comparison. The graph in Figure 5 shows the comparative performance between the present prevailing techniques and DPBODL. PPDL is able to minimize epsilon, but at the cost of decline in classification accuracy. For epsilon values in the range <10^{-2}, 10^{-1}>, PPDL achieves about 63% classification accuracy. As epsilon is compromised (larger values of epsilon), accuracy improves. BO-Dpareto and LR-DPCO have classification accuracies of 75-80% for epsilon range <10^{-2}, 10>. Minimizing privacy as low as 10^{-2} in the existing techniques causes a corresponding reduction in the accuracy of the analysis. Therefore, when considering the epsilon-accuracy compromise, DPBODL approach balances it efficiently, without severely affecting analysis accuracy, and hence is achievable in a practical scenario. It can be argued that the technique gives a fair compromise between the two objectives. Lower epsilon ranges give accuracy of about 80% for both datasets, and it can be noticed that analysis accuracy stabilizes thereafter. For values of epsilon greater than 1, a higher accuracy (85-90%) is achieved with DPBODL, whereas the known state-of-the-art approaches achieve an average accuracy of only 85%. Hence the hyperparameter optimization of the deep learner has resulted in achieving a good balance between privacy and utility.

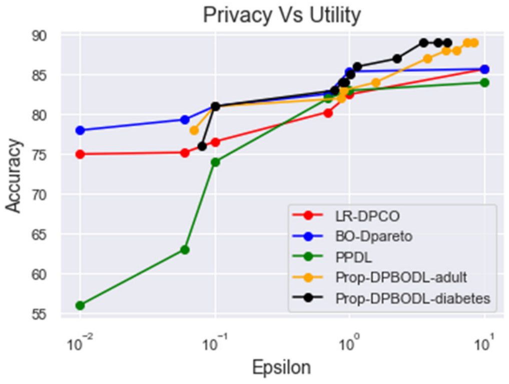

Fig. 5. Comparative analysis.

As far as computational efficiency is concerned a straight comparison between DPBODL and the afore-mentioned algorithms is unreasonable, since they differ by factors such as data size, dimension, and dynamics. Hence its computational efficiency is compared with the standard deep learner. DPBODL performs well in comparison to the standard learner as shown in Figure 6. The comparison shows that the number of epochs required to train a standard learner is much higher than its optimized variant. So, it can be perceived from the comparative analysis that the proposed approach has been able to provide a reasonable performance trade-off.

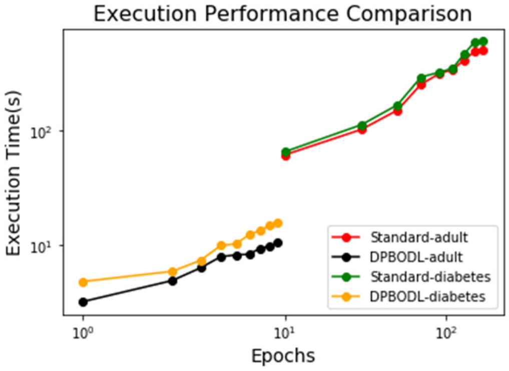

Fig. 6. Performance comparison.

The next section discusses the achieved privacy-utility trade-off in detail by considering the Pareto-front generated by the approach and the extent to which the approach generates optimal solutions.

IX. STATISTICAL ESTIMATION OF OPTIMAL PRIVACY-UTILITY TRADE-OFF

This section makes a statistical assessment of DPBODL's results and computes an optimal privacy-utility trade-off. While selecting an optimal solution, the execution efficiency of the model is considered independent from these primary objectives, but the model does not overlook computational efficiency in the process of identifying a compromising solution. From the objective space consisting of a set of optimal solutions, as shown by the Pareto-front in Figure 7, an optimal solution is identified. The statistical analysis is carried out for the adult dataset. The utopian method [8] is employed to determine this optimum point. It is a decision-making strategy, which involves determining the near optimal <epsilon, accuracy> pair by comparing all data points to the ideal point called utopian point.

Let the conflicting objective functions in the current setting be defined as $P(m)$ and $U(m)$ (defined in Section IV) .While $P(m)$ determines privacy measured by epsilon, $U(m)$ indicates the utility measured by the accuracy of classification analysis. The objective is to maximize both privacy and utility. Maximizing privacy in the context of differential privacy involves achieving smaller values of epsilon, while maximizing accuracy of analysis. The objective space is shown as a scatter plot in Figure 7. The plane shows the relationship between data points. The utopian point is positioned at (0.783, 89) indicating the ideal values for epsilon and classification accuracy. After estimating the distance measures of all points from the utopian point, the closest one is chosen as the final optimal solution, justifying the ideal trade-off between the objectives of the problem. The results of this calculation are shown in Table IV. In this problem setting, a point with an epsilon value of 0.783 with corresponding classification accuracy of 84% is found to be the closest. Table V shows the comparison in trade-off between the existing and the proposed technique. The {epsilon, accuracy} pair shows enhanced trade-off in comparison to the existing techniques. Computational efficiency has been experimented only by PPDL, and results show that DPBODL is executed in a reduced number of epochs in comparison with PPDL for a corresponding epsilon value.

TABLE IV. STATISTICAL ESTIMATION OF OTPIMUM TRADE-OFF

Epsilon	Classification accuracy	Distance measure
0.783	0.84	0.063
0.891	0.84	0.1212023102
0.923	0.842	0.149939988
1.02	0.853	0.2413379373
1.15	0.86	0.3694766569
2.25	0.87	1.468180166
3.523	0.89	2.741001642
4.563	0.892	3.781000132
5.34	0.893	4.558

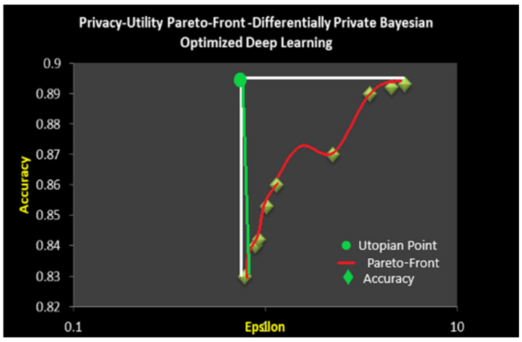

Fig. 7. Optimal trade-off computation.

TABLE V. TRADE-OFF COMPARISON

Privacy technique/ learning technique		Algorithms	Optimal trade-off (epsilon, accuracy %)	Performance (average number of epochs)
Differential privacy/ deep learning	Proposed	DPBODL	(0.783,84)	3-8
	Existing	BO-Dpareto	(0.7,79)	-
		PPDL	(0.7,63)	10

X. CONCLUSIONS

In this paper, an optimization of deep learning technique for differentially private learning is proposed. Conceptualizing private learning as a multi-objective optimization problem, the proposed method aims to find an enhanced privacy-utility-performance trade-off for private learning. Although it is challenging to find a single optimal solution, that is mathematically best, for a multi-objective problem, the proposed method substantiates this trade-off by employing an appropriate decision-making approach. Firstly, various trade-off solutions are generated with the optimized learner. For a decision to be made with reference to the optimum point, Pareto-optimal decision-making is done. The results show that the trade-off achieved is a quantifiable enhancement over the existing techniques. The proposed method has also considered execution efficiency which was not experimented by many of the existing techniques.

REFERENCES

[1] L. Sweeney, "Achieving *k*-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 571–588, Oct. 2002, https://doi.org/10.1142/S021848850200165X.

[2] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "*L*-diversity: Privacy beyond *k*-anonymity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, Mar. 2007, Art. no. 3-es, https://doi.org/10.1145/1217299.1217302.

[3] C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, Aug. 2014, https://doi.org/10.1561/0400000042.

[4] I. Mironov, "Renyi Differential Privacy," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, Aug. 2017, pp. 263–275, https://doi.org/10.1109/CSF.2017.11.

[5] "Google’s Differential Privacy May be Better Than Apple’s," *The Mac Observer*, Sep. 15, 2017. https://www.macobserver.com/analysis/google-apple-differential-privacy/ (accessed Jan. 17, 2021).

[6] M. Abadi *et al.*, "Deep Learning with Differential Privacy," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA, Oct. 2016, pp. 308–318, https://doi.org/10.1145/2976749.2978318.

[7] G. Naya, "Available hyperparameter optimization techniques," *Medium*, Jan. 08, 2020. https://towardsdatascience.com/available-hyperparameter-optimization-techniques-dc60fb836264 (accessed Jan. 17, 2021).

[8] N. Gunantara, "A review of multi-objective optimization: Methods and its applications," *Cogent Engineering*, vol. 5, no. 1, p. 1502242, Jan. 2018, https://doi.org/10.1080/23311916.2018.1502242.

[9] I. A. Kandhro, S. Z. Jumani, F. Ali, Z. U. Shaikh, M. A. Arain, and A. A. Shaikh, "Performance Analysis of Hyperparameters on a Sentiment Analysis Model," *Engineering, Technology & Applied Science Research*, vol. 10, no. 4, pp. 6016–6020, Aug. 2020, https://doi.org/10.48084/etasr.3549.

[10] V. Kumar and S. K. Dhull, "Genetic Algorithm based Optimization of Uniform Circular Array," *Engineering, Technology & Applied Science Research*, vol. 10, no. 6, pp. 6403–6409, Dec. 2020, https://doi.org/10.48084/etasr.3792.

[11] B. Avent, J. Gonzalez, T. Diethe, A. Paleyes, and B. Balle, "Automatic Discovery of Privacy-Utility Pareto Fronts," in *Proceedings on Privacy Enhancing Technologies 2020*, Jul. 2020, vol. 4, pp. 5–23, Accessed: Jan. 17, 2021. [Online]. Available: http://arxiv.org/abs/1905.10862.

[12] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, Sep. 2015, pp. 909–910, https://doi.org/10.1109/ALLERTON.2015.7447103.

[13] "Google Just Open Sourced TensorFlow, Its Artificial Intelligence Engine | WIRED." https://www.wired.com/2015/11/google-open-sources-its-artificial-intelligence-engine/ (accessed Jan. 17, 2021).

[14] D. Dua and C. Graff, *UCI Machine Learning Repository*. Irvine, CA, USA: University of California, School of Information and Computer Science, 2019.

[15] R. Iyengar, J. P. Near, D. Song, O. Thakkar, A. Thakurta, and L. Wang, "Towards Practical Differentially Private Convex Optimization," in *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 299–316, https://doi.org/10.1109/SP.2019.00001.

[16] T. Handhayani, J. Hendryli, and L. Hiryanto, "Comparison of shallow and deep learning models for classification of Lasem batik patterns," in *2017 1st International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, Indonesia, Nov. 2017, pp. 11–16, https://doi.org/10.1109/ICICOS.2017.8276330.