Guarding Data Privacy: A Performance Perspective on Differential Privacy

1st Iker Cumplido Esteban
LMU Munich
Munich, Germany
iker.cumplido@campus.lmu.de

2nd Marco Zeulner
LMU Munich
Munich, Germany
marco.zeulner@campus.lmu.de

***Abstract*—Data privacy concerns have become a major obstacle to collecting high-quality survey data. Differential Privacy (DP) offers a promising solution by ensuring that individual records cannot be pinpointed in the published results. In this paper, we compare two DP mechanisms—Laplace and Permute-and-Flip—using the Titanic dataset with four machine learning models: Logistic Regression, Naive Bayes, Random Forest, and Decision Tree. Our experiments reveal a clear trade-off: stronger privacy (lower ϵ) introduces more noise and reduces Accuracy and F1-scores, while weaker privacy (higher ϵ) preserves performance but provides less protection. We conclude by discussing practical challenges, potential attacks on DP implementations, and future directions to make privacy-preserving methods more robust. Overall, our study provides a comprehensive evaluation that bridges theory with practice in DP-enabled machine learning.**

***Index Terms*—Differential Privacy, Data Privacy, Data Security**

I. Introduction

Modern research and data-driven decision making heavily rely on collecting and analyzing large datasets. Surveys continue to be one of the key methods for gathering data; however, a growing reluctance among individuals to participate has been observed over the years [1]. One major reason for this hesitancy is the concern over data privacy [2]. Individuals fear that sharing their personal information could lead to unintended consequences such as identity theft, discrimination, or reputational harm, particularly in an era marked by frequent data breaches.

This concern is not without merit. Anonymizing data by removing direct identifiers (e.g., names or social security numbers) is often insufficient. A well-known case from 1997 demonstrated this vulnerability: a graduate student de-anonymized a supposedly anonymous medical dataset that contained information about then-governor of Massachusetts, William Weld [3]. By cross-referencing anonymized medical records with publicly available voter registration data (including attributes such as ZIP code, date of birth, and gender), she was able to identify Weld's confidential medical details. This incident underscored the limitations of traditional anonymization techniques, especially when auxiliary datasets are available to adversaries.

The growing need for more robust privacy-preserving methods has led to increased interest in Differential Privacy (DP), introduced by Dwork et al. in 2006 [4]. At its core, DP provides a formal mathematical framework that guarantees the protection of individual data by introducing carefully calibrated noise into statistical analyses. This ensures that the inclusion or exclusion of any single individual's data does not significantly change the overall outcome. As a result, individuals are protected from being singled out or harmed by the analysis, while researchers can still extract meaningful insights.

Furthermore, DP has the potential to address the problem of declining survey response rates. When individuals are confident that their personal data cannot be traced back to them, they are more likely to participate in surveys and studies. This increased participation can lead to higher quality and more comprehensive data for research. In this paper, we explore the underlying principles of DP, review state-of-the-art mechanisms, and benchmark various DP methods by applying them to practical machine learning classification tasks. Our aim is to demonstrate how DP can bridge the gap between protecting individual privacy and maintaining data utility. However, despite the growing attention to DP, it remains unclear how different mechanisms compare in a typical classification setting, especially when the privacy budget ϵ varies.

Scientific Question and Motivation. In particular, we address the following main question:

> *How does the choice of DP mechanism and privacy budget ϵ affect classification performance, and what trade-offs arise between privacy and utility?*

We break this down into sub-questions:

1) How do noise-adding DP methods (e.g., Laplace, Permute-and-Flip) differ in their impact on model accuracy and F1-scores?
2) What are the limitations and open challenges of integrating DP into real-world machine learning pipelines?

By answering these questions, we want to clarify both the theoretical and practical implications of using DP for data security, ultimately contributing to more robust practices that mitigate the risks of data reidentification.

II. Definition and Related Work

A. Definition of Differential Privacy

Differential Privacy (DP) is a rigorous mathematical framework that offers strong privacy guarantees when analyzing and sharing statistical data [5]. The key idea behind DP is to ensure that the output of an analysis is not significantly affected by the inclusion or exclusion of any single individual's data. This prevents adversaries from inferring whether a particular individual's data is present in the dataset.

1) Formal Definition: A randomized algorithm $\mathcal{A}$ is said to provide **ϵ-differential privacy** if the probability of obtaining any given output does not change substantially when a single data point is modified. More formally, for any two datasets D_1 and D_2 that differ in at most one element, and for any subset S of the output space of $\mathcal{A}$, the following inequality holds:

$$\Pr[\mathcal{A}(D_1) \in S] \leq e^{\epsilon} \cdot \Pr[\mathcal{A}(D_2) \in S] \tag{1}$$

Here, ϵ is a non-negative privacy parameter that is commonly referred to as the **privacy budget**. A smaller ϵ signifies stronger privacy protection because it restricts the extent to which the output distributions of $\mathcal{A}(D_1)$ and $\mathcal{A}(D_2)$ can differ [6].

2) Intuition Behind ϵ: To build an intuitive understanding of ϵ, consider a scenario in which a hospital releases statistics about patients' average blood pressure. If the results remain nearly the same whether or not a specific patient's data is included, it becomes difficult to infer that patient's contribution, thereby ensuring privacy. The parameter ϵ quantifies this level of indistinguishability:

- **Small ϵ (e.g., $\epsilon = 0.01$):** Implies very strong privacy. An adversary gains almost no information regarding any individual's participation in the dataset.
- **Large ϵ (e.g., $\epsilon = 5$):** Indicates weaker privacy protection as the influence of an individual's data becomes more pronounced.

In essence, ϵ controls the trade-off between privacy and utility: while smaller values offer stronger protection, they may also lead to increased noise in the outputs, thereby reducing the accuracy of statistical analyses.

B. State-of-the-Art Mechanisms in Differential Privacy

To achieve DP, various noise-adding mechanisms have been developed. These methods ensure that individual data contributions remain hidden while still providing useful aggregated results. In the following, we describe several key mechanisms.

1) Laplace Mechanism: The Laplace Mechanism is one of the foundational techniques for achieving ϵ-DP. It works by adding noise sampled from a Laplace distribution to the true query result [7]. For a function $f : D \to \mathbb{R}$, the differentially private output is given by:

$$\mathcal{A}(D) = f(D) + \text{Lap}(\lambda) \tag{2}$$

where the scale parameter λ is determined by:

$$\lambda = \frac{\Delta f}{\epsilon} \tag{3}$$

and Δf (the sensitivity of f) is defined as:

$$\Delta f = \max_{D_1, D_2} |f(D_1) - f(D_2)| \tag{4}$$

for all datasets D_1 and D_2 differing in a single entry. The Laplace distribution itself is described by:

$$\text{Lap}(x \mid \lambda) = \frac{1}{2\lambda} e^{-|x|/\lambda}. \tag{5}$$

2) Gaussian Mechanism: Another common approach is the Gaussian Mechanism, which adds noise drawn from a Gaussian (normal) distribution. This method is especially useful when multiple DP queries are composed together [7]. It is typically employed in the context of (ϵ, δ)-DP, where δ allows for a small probability of failure to meet the strict ϵ-DP guarantee. For a function $f : D \to \mathbb{R}$, the output is:

$$\mathcal{A}(D) = f(D) + \mathcal{N}(0, \sigma^2) \tag{6}$$

with the variance set as:

$$\sigma^2 = \frac{2 \ln(1.25/\delta)(\Delta f)^2}{\epsilon^2}. \tag{7}$$

3) Exponential Mechanism: The Exponential Mechanism extends DP to non-numeric outputs such as categorical data or rankings. Rather than adding numerical noise, this mechanism selects an output from a set of candidates based on a utility function $u(D, r)$ that scores how desirable each result r is for dataset D [7]. The selection probability is given by:

$$\Pr[\mathcal{A}(D) = r] \propto e^{\frac{\epsilon u(D,r)}{2\Delta u}} \tag{8}$$

where Δu is the sensitivity of the utility function:

$$\Delta u = \max_{D_1, D_2, r} |u(D_1, r) - u(D_2, r)|. \tag{9}$$

4) Permute-and-Flip Mechanism: The Permute-and-Flip Mechanism is an alternative approach to the Exponential Mechanism, particularly effective for selecting items from a set while maintaining DP [8]. Given a set of items $X = \{x_1, x_2, \ldots, x_n\}$ and a utility function $u(D, x)$, the mechanism operates as follows: label=0.

1) Randomly permute the elements of X.
2) Iterate over each element x_i in the permuted order.
3) Compute the probability $p_i = \frac{e^{\epsilon u(D,x_i)/2}}{e^{\epsilon u(D,x_i)/2} + 1}$.
4) Flip a biased coin with success probability p_i.
5) If the coin flip is successful, select x_i and terminate the process.
6) If no element is selected after the iteration, return the last element in the permutation.

This mechanism preserves the core privacy guarantees of DP while often achieving lower expected error than the traditional Exponential Mechanism.

Overall, these mechanisms form the backbone of differentially private systems used in modern applications. They provide both strong privacy guarantees and a measure of utility, though the exact balance between the two depends on the choice of parameters and the application context.

C. Research Gap and Placement of Our Work

Although DP has been widely studied, most existing research focuses on the theoretical aspects of noise-adding mechanisms. In contrast, comprehensive empirical evaluations of DP on standard public datasets (like Titanic) are still limited. We address this gap by:

- Systematically benchmarking multiple DP mechanisms (Laplace vs. Permute-and-Flip) in a typical classification task.
- Comparing these approaches across several common algorithms (Logistic Regression, Naive Bayes, Decision Tree, and Random Forest).
- Evaluating how performance degrades at different privacy budgets ϵ to guide practical parameter selection.

Our work balances theory and practical applications of DP, showing how it can be applied in common machine learning tasks. In the next section, we test different noise mechanisms on a real-world classification problem.

III. Experiments

In this section, we describe our experiments designed to assess the performance of various DP algorithms on the popular Titanic dataset. Specifically, we aim to answer our main research question: *How does the choice of DP mechanism and privacy budget ϵ affect classification performance, and what trade-offs arise between privacy and utility?* To do so, we examine how ϵ influences key classification metrics such as Accuracy and F1-score. Additionally, we compare different DP noise mechanisms (Laplace, Permute-and-Flip) and evaluate how DP models perform relative to their non-private counterparts. All code and corresponding plots are available at *https://github.com/ikumpli/Differential_Privacy*.

A. Experimental Setup

a) Dataset: We use the Titanic dataset[1], a classic benchmark for binary classification. This dataset contains demographic and ticket-related information about passengers, with the target variable indicating whether each passenger survived. To ensure consistency across experiments, we apply several preprocessing steps:

1) **Handling Missing Values:** Missing entries in numerical features (e.g., *Age*) are imputed using the median, while missing categorical entries (e.g., *Embarked*) are filled with the most frequent category.
2) **Encoding:** Categorical variables such as *Sex* and *Embarked* are transformed into numerical values using label encoding.
3) **Standardization:** Numeric features (e.g., *Age* and *Fare*) are standardized to have zero mean and unit variance.

After these preprocessing steps, we retain seven features (*Pclass*, *Sex*, *Age*, *SibSp*, *Parch*, *Fare*, and *Embarked*), with the binary variable *Survived* serving as the target.

b) Private and Non-Private Algorithms: For benchmarking purposes, we utilize standard machine learning models from the *scikit-learn*[2] library as non-private baselines. Their differentially private implementations are provided by IBM's *diffprivlib*[3], which introduces noise into model training and data transformations. Table I summarizes the models used along with the noise mechanisms implemented.

TABLE I

Overview of the private and non-private algorithms used in our experiments, along with their corresponding noise mechanisms.

Model	Noise Mechanism
Logistic Regression	Laplace-based
Naive Bayes	Laplace-based
Random Forest	Permute-and-Flip
Decision Tree	Permute-and-Flip

c) Privacy and Metrics: In our experiments, we vary the privacy budget ϵ over several orders of magnitude. Smaller values of ϵ imply stronger privacy, but they also introduce more noise into the data, potentially degrading model performance. To measure utility, we report the following metrics:

- **Accuracy** $= \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$,
- **Precision** $= \frac{\text{TP}}{\text{TP+FP}}$,
- **Recall** $= \frac{\text{TP}}{\text{TP+FN}}$,
- **F1-Score** $= 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}}$,

where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. We compare these metrics with those of the non-private models to highlight the impact of DP.

B. Experiment 1: Logistic Regression at Varying ϵ

In the first experiment, we focus on a single classification model: *Logistic Regression*. The primary goal is to examine the effect of varying ϵ on the performance of a differentially private logistic regression model. The experimental setup includes the following steps:

- **Data Splitting:** The Titanic dataset is randomly divided into 80% training and 20% test data.
- **Model Training:** We train a DP logistic regression model from *diffprivlib* over 300 logarithmically spaced ϵ values ranging from 10^{-2} to 10^4.
- **Baseline Comparison:** A standard (non-private) logistic regression model is trained using *scikit-learn* with default parameters to serve as an upper performance bound.
- **Evaluation:** For each ϵ, we record Accuracy, Precision, Recall, and F1-score on the test set.

[1] https://www.kaggle.com/competitions/titanic/

[2] https://scikit-learn.org/stable/

[3] https://github.com/IBM/differential-privacy-library

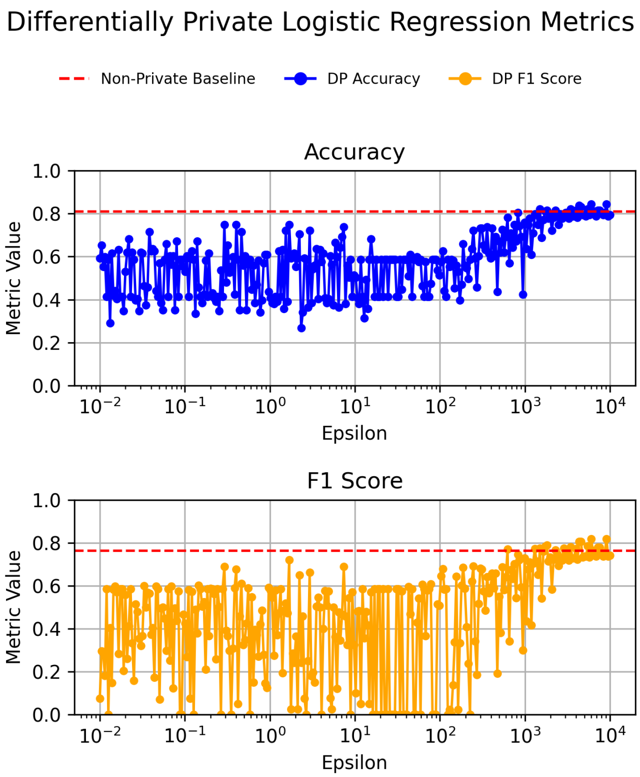

Fig. 1. Comparison of accuracy and F1 scores for differentially private logistic regression models across varying ϵ values (logarithmic scale). The red dashed line corresponds to the non-private baseline performance, while the top and bottom subplots show accuracy and F1 scores, respectively.

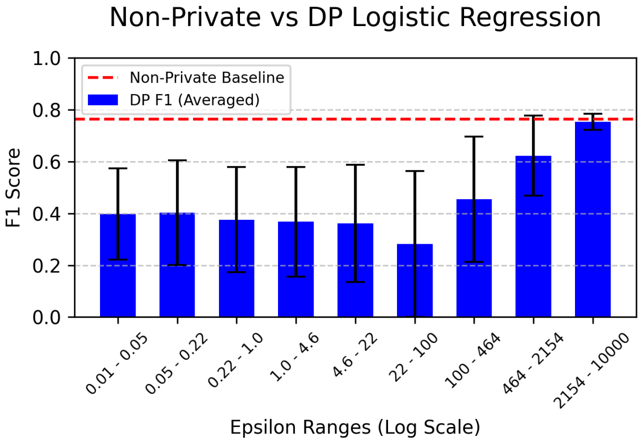

Fig. 2. Comparison of the F1 scores for differentially private logistic regression models across varying ϵ ranges (logarithmic scale). The red dashed line indicates the non-private baseline F1 score, while the blue bars represent the averaged F1 scores for the private models within each ϵ bin. Error bars show the standard deviation of F1 scores, illustrating performance variability with different privacy budgets.

a) Results: Figure 1 illustrates the changes in Accuracy and F1-score of the DP logistic regression model as ϵ varies. At very low ϵ values (e.g., 10^{-2} to 10^{-1}), high noise levels cause substantial variability in both metrics. As ϵ increases, the injected noise diminishes, leading to more stable performance that converges towards the non-private baseline (indicated by the red dashed line). Figure 2 further demonstrates these trends by binning ϵ into ranges and plotting the average F1-scores with corresponding standard deviations. Notably, when ϵ reaches sufficiently high values (e.g., above 464 on the log scale), the DP model's performance approaches that of the non-private model with only a minor loss in F1-score. However, this increase comes at cost of decreasing privacy.

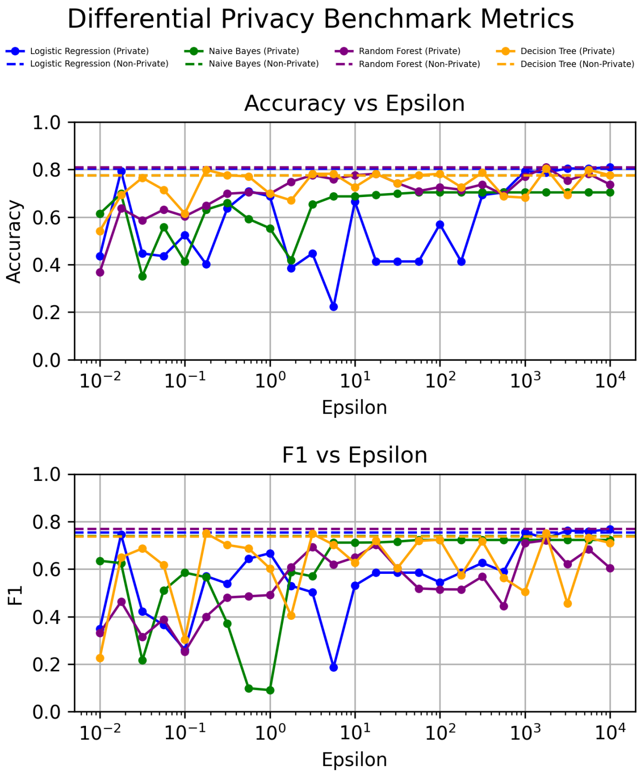

Fig. 3. Benchmark results of DP methods applied to various machine learning models, including Logistic Regression, Naive Bayes, Random Forest, and Decision Trees. The two subplots show Accuracy and F1-score versus ϵ. Solid lines represent the performance of private models, while dashed lines correspond to the non-private baselines. The results illustrate the trade-off between privacy (smaller ϵ) and model performance across different algorithms.

C. Experiment 2: Benchmark Across Multiple Models

The second experiment extends the analysis to a broader set of classification algorithms. In addition to Logistic Regression, we evaluate:

- *Naive Bayes*
- *Random Forest*
- *Decision Tree*

This comparative study is aimed at understanding whether the effects observed with logistic regression generalize across different model architectures.

a) Setup: Similar to Experiment 1, we use an 80/20 train-test split and default hyperparameters for both the DP and non-private versions of each model. In this experiment, ϵ values are sampled logarithmically from 10^{-2} to 10^{4} but with a reduced granularity (25 points) to facilitate clear visualizations, as it allows us to display all methods in a single plot without overcrowding.

b) Results: Figure 3 presents the Accuracy and F1-score for each algorithm as a function of ϵ. Consistent with the logistic regression findings, the DP variants of all models exhibit significant performance degradation at low ϵ values, followed by gradual stabilization as the privacy budget increases. Among the models, Decision Trees tend to retain higher Accuracy and F1-scores even at low ϵ, likely because their hierarchical structure allows them to make robust splits despite added noise. In contrast, Naive Bayes experiences a more significant performance drop at lower ϵ values, highlighting its reliance on precise probability estimates, which are highly sensitive to noise. The Random Forest model shows intermediate behavior, with some loss in utility at small ϵ but a faster convergence to baseline performance compared to Naive Bayes, likely due to the averaging effect of multiple trees.

IV. Discussion

A. Summary of Experimental Results

The experiments clearly demonstrate a trade-off between privacy and performance in differentially private models. At low ϵ values (high privacy), the models enforce strong privacy guarantees at the cost of introducing significant noise, which leads to a notable drop in Accuracy and F1-score relative to non-private baselines. As ϵ increases, the DP models gradually recover performance, converging toward the results obtained from non-private implementations. Our analysis also reveals that the choice of algorithm plays a crucial role: ensemble methods such as Random Forest are more robust to noise, while models relying on precise probability estimates, such as Naive Bayes, are more affected.

With these results, we can now answer our main research question: We find that while stronger privacy guarantees ($\epsilon \leq 1$) significantly degrade model accuracy, moderate privacy budgets ($\epsilon \approx 10$) provide a reasonable balance between protection and utility. Additionally, the impact of DP mechanisms varies across models, with ensemble methods showing greater resilience to noise injection.

These findings emphasize that selecting an appropriate privacy budget ϵ is essential, and the decision should be informed by both the sensitivity of the data and the acceptable level of performance degradation. Moreover, our experiments indicate that different models react differently to noise injection, which must be considered when deploying DP in real-world applications. Therefore, given our dataset and chosen algorithms, we would recommend the following epsilon values which provide a good balance between privacy and performance:

TABLE II
Overview of the experiment metrics and recommended epsilon ranges.

Model	**Baseline F1 (non-private)**	**Recom. ϵ-range**	**Avg. F1-score in ϵ-range**
Log. Regression	0.755	$[10^{1}$-$10^{2}]$	0.566
Naive Bayes	0.740	$[10^{1}$-$10^{2}]$	0.717
Decision Tree	0.737	$[10^{-1}$-$10^{0}]$	0.609
Random Forest	0.770	$[10^{0}$-$10^{1}]$	0.612

B. Limitations of DP

While DP offers strong theoretical guarantees, practical implementations face several challenges:

- **Privacy-Utility Trade-off:** As proven in the experiments, there is an inherent trade-off between privacy and data utility. Lower ϵ values ensure higher privacy but lead to degraded performance, which may limit the applicability of DP in scenarios requiring high accuracy.
- **Parameter Selection:** Choosing appropriate values for ϵ and δ is non-trivial. In many cases, practitioners lack clear guidelines to determine the amount of privacy protection provided by specific parameter settings.
- **Composition and Budget Exhaustion:** In systems that allow multiple queries, the privacy loss accumulates, necessitating careful management of the overall privacy budget. This can restrict the number of allowable queries and make the data less useful over time.
- **Implementation Vulnerabilities:** Real-world implementations of DP can suffer from bugs or side-channel vulnerabilities. Issues such as floating-point precision errors, incorrect noise calibration, and inefficient privacy budget management can compromise the theoretical guarantees of DP [9], [10].

C. Attacks on DP

Despite its rigorous mathematical framework, DP is not immune to attacks that exploit weaknesses in implementation:

- **Side-Channel Attacks:** Attackers can infer private data by analyzing execution side effects, such as query execution time variations or state-dependent behavior in DP systems. Studies have shown that timing attacks can reveal sensitive information when query execution time correlates with the presence of specific data records [9].
- **Privacy Budget Exploitation:** In our experiment, where we repeatedly perform the same query (i.e., classification), the privacy budget consumption remains constant. However, in a system where queries vary significantly, a dynamic privacy cost is often computed and deducted from a total budget to minimize excessive privacy leakage. An attacker can exploit this mechanism by creating queries whose privacy cost depends on the presence of specific data. By analyzing the remaining budget after execution, the adversary can infer whether certain sensitive records exist, leading to a potential privacy breach [9].

- **Floating-Point Attacks:** Differential privacy mechanisms are typically designed under the assumption of infinite-precision arithmetic. However, real-world implementations rely on finite-precision floating-point numbers, which introduces numerical inaccuracies and potential security vulnerabilities. Recent research has demonstrated that these floating-point errors can be exploited to weaken privacy guarantees by subtly altering the probability distribution of noise mechanisms such as Laplace and Gaussian noise. Although the Diffprivlib library we use implements mitigation techniques to address this issue, studies have shown that it remains susceptible to precision-based attacks [11].

These vulnerabilities underscore the need for robust engineering practices and thorough auditing of DP implementations. Tools such as the auditing framework **Delta-Siege** are being developed to systematically test DP systems for privacy violations and calibration errors [10].

D. Future Work & Open Questions

Based on our findings and the identified limitations, several ideas for future research emerge:

- **Improved Parameter Selection:** Developing empirical guidelines for setting ϵ and δ based on diverse application scenarios will help standardize DP implementations.
- **Enhanced Auditing Techniques:** Expanding privacy auditing frameworks can help the detection of implementation flaws and prevent subtle privacy leaks.
- **Mitigating Side-Channel Attacks:** Future DP systems should aim to implement constant-time operations and other techniques to timing and other side-channel attacks.
- **Advances in Privacy-Preserving Machine Learning:** Improving methods for integrating DP with machine learning, such as adaptive noise allocation and novel training algorithms, may help reduce the accuracy loss associated with strict privacy settings.

Addressing these challenges will be crucial for the broader adoption of DP in practical applications.

V. Conclusion

In this paper, we have examined the impact of DP on a common machine learning task using the Titanic dataset as a case study. Our experiments demonstrate that lower values of the privacy parameter ϵ provide stronger protection but introduce substantial noise, leading to decreased classification performance. On the contrary, higher ϵ values yield results closer to non-private baselines, although with reduced privacy guarantees. This answers our main research question stated in the introduction.

The results highlight the intrinsic privacy–utility trade-off in DP and emphasize that both the choice of privacy budget and the underlying algorithm significantly influence model performance. Furthermore, we discussed several practical challenges, including parameter selection, budget composition, and vulnerability to various attacks, all of which underline the importance of rigorous implementation and auditing.

Future research should focus on refining parameter selection strategies, developing robust auditing frameworks, and advancing privacy-preserving machine learning techniques to mitigate accuracy losses. Through such improvements, DP can become a more robust and widely applicable solution to the increasing privacy concerns in data collection and analysis.

References

[1] J. Eggleston, "Frequent survey requests and declining response rates: Evidence from the 2020 census and household surveys," *Journal of Survey Statistics and Methodology*, vol. 12, no. 5, pp. 1138–1156, 04 2024. [Online]. Available: https://doi.org/10.1093/jssam/smae022

[2] M. Haan, V. Toepoel, Y. Ongena, and B. Janssen, "Recruiting non-respondents for a conversation about reasons for non-response: A description and evaluation," *Survey Practice*, vol. 17, mar 14 2024.

[3] D. Barth-Jones, "The 're-identification' of governor william weld's medical information: A critical re-examination of health data identification risks and privacy protections, then and now." [Online]. Available: https://papers.ssrn.com/abstract=2076397

[4] 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.

[5] A. Wood, M. Altman, A. Bembenek, M. Bun, M. Gaboardi, J. Honaker, K. Nissim, D. O'Brien, T. Steinke, and S. Vadhan, "Differential privacy: A primer for a non-technical audience." [Online]. Available: https://papers.ssrn.com/abstract=3338027

[6] M. Aitsam, "Differential privacy made easy." [Online]. Available: http://arxiv.org/abs/2201.00099

[7] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," vol. 9, no. 3, pp. 211–407. [Online]. Available: http://www.nowpublishers.com/articles/foundations-and-trends-in-theoretical-computer-science/TCS-042

[8] R. McKenna and D. Sheldon, "Permute-and-flip: a new mechanism for differentially private selection," in *Proceedings of the 34th International Conference on Neural Information Processing Systems*, ser. NIPS '20. Red Hook, NY, USA: Curran Associates Inc., 2020.

[9] A. Haeberlen, B. C. Pierce, and A. Narayan, "Differential privacy under fire," in *Proceedings of the 20th USENIX Conference on Security*, ser. SEC'11. USA: USENIX Association, 2011, p. 33.

[10] J. Lokna, A. Paradis, D. I. Dimitrov, and M. Vechev, "Group and attack: Auditing differential privacy," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 1905–1918. [Online]. Available: https://doi.org/10.1145/3576915.3616607

[11] S. Haney, D. Desfontaines, L. Hartman, R. Shrestha, and M. Hay, "Precision-based attacks and interval refining: how to break, then fix, differential privacy on finite computers," 2022. [Online]. Available: https://arxiv.org/abs/2207.13793