10th International Scientific Conference
Technics, Informatics, and Education – TIE 2024
20-22 September 2024

Session: *Computer Sciences and Information Technology*
Professional paper
DOI: 10.46793/TIE24.089I

Privacy-Preserving in Machine Learning: Differential Privacy Case Study

Aleksa Iričanin[1*] [0009-0006-8145-403X], Olga Ristić[1] [0000-0002-1723-0940] and Marjan Milošević[1] [0000-0003-4730-1292]
[1] University of Kragujevac/Faculty of Technical Sciences, Čačak, Serbia
[*] aleksa.iricanin@ftn.kg.ac.rs

Abstract: *The burgeoning field of Machine Learning (ML) has revolutionized various aspects of our lives. However, the reliance on vast amounts of data, often containing personal information, raises concerns about individual privacy. Striking a balance between effective ML model training and protecting sensitive data is crucial for responsible development and ethical implementation. This paper explores the challenges and potential solutions for preserving privacy in ML training, focusing on differential privacy (DP). The advantages of implementing DP in ML training include robust protection of individual data, enabling meaningful insights from large datasets while maintaining privacy. This is essential for ethical and responsible data usage in machine learning applications. However, DP in ML training presents challenges including scalability issues and trade-offs between utility and privacy. The paper also covers the mathematical mechanisms of Laplace and Gaussian* and their *noise addition, followed by a comparative analysis of their efficiency within the dataset.*

Keywords: *ML;* Differential privacy; *Gaussian Mechanism; Laplace Mechanism; data privacy*

1. INTRODUCTION

Machine learning (ML) models, powered by intricate algorithms, require copious amounts of data for training and optimization. While this data fuels innovation, it often necessitates the use of personal information, encompassing details like demographics, health records, or financial transactions. This raises significant concerns about individual privacy, as breaches or misuse of such data can lead to discrimination, profiling, and even identity theft [1].

DP is an advanced technique designed to safeguard individual data while still allowing meaningful insights to be gleaned from large datasets. By introducing precisely controlled noise into the data, DP ensures that the presence or absence of any single individual's data has a minimal impact on the overall analysis results. This method provides a strong privacy guarantee, enabling organizations to analyze and disseminate data without violating individual privacy. In our current era, where data-driven decision-making is paramount, the application of DP is increasingly important. It is especially significant across sectors such as healthcare and finance, where protecting sensitive information while extracting value from data is crucial [2].

It should also be noted that the General Data Protection Regulation (GDPR) has been defined in 2016, which can be found at the following link: https://gdpr-info.eu/. Here are defined main requirements in data privacy laws across Europe.

1.1 Dangers of exposing private data

The consequences of exposing private data in ML training extend far beyond simple inconvenience. Here's a breakdown of some key dangers [3]:

- **Identity Theft:** Exposed data like names, Social Security numbers, or addresses can be weaponized by criminals for impersonation. This can lead to financial losses through fraudulent credit card use, opening new accounts in the victim's name, or even tax return theft.
- **Financial Fraud:** Personal financial information like bank account details or investment holdings, if compromised, can be used for unauthorized transactions, draining savings or incurring significant debt.
- **Discrimination and Social Stigma:** ML models trained on biased or incomplete data can perpetuate discrimination in areas like loan approvals, job hiring, or insurance eligibility. Exposed health records might lead to social stigma or hinder access to insurance.
- **Reputational Damage:** Private information leaks, especially sensitive details, can damage an individual's reputation and cause emotional distress. Public embarrassment or loss of trust could arise from the misuse of personal data.

- **Security Risks:** Data breaches can expose individuals to targeted phishing attacks or malware scams. Criminals might use leaked information to gain the victim's trust and launch further cyber attacks.
- **Reduction of Physical Safety:** Exposing private data like home location, travel and work schedule can lead to theft or vandalism of property. This also can lead to physical assaults on individuals.
- **Diminishment of Freedom of Speech:** Leaks of sensitive information like political or religious beliefs can be used against individuals by revealing unpopular opinions resulting in their hesitation to engage in expressive activities or discouragement in having personal opinion.

Employing security measures is crucial for mitigating the exposure of private data. These measures play a vital role in ensuring a certain level of confidentiality, as safeguarding credentials and controlling access to data are fundamental components of a robust security infrastructure.

2. TECHNIQUES FOR PRIVACY-PRESERVING ML TRAINING

Several techniques offer promising solutions for mitigating privacy risks in ML training [4-6]. In the following sections we provide brief preview of such techniques.

2.1 Anonymization

This technique involves removing or obfuscating personally identifiable information (PII) from the data before training. Common anonymization methods include:

- **Suppression:** Removing sensitive attributes entirely from the data.
- **Generalization:** Replacing specific values with broader categories (e.g., replacing zip code with city).
- **Perturbation:** Adding controlled noise to the data to obscure individual values while preserving statistical properties.
- **Pseudonymization:** Replacing PII with fictitious but unique identifiers, allowing for some re-identification risk.

While anonymization offers a straightforward approach, it comes with limitations:

- **Information Loss:** Removing or modifying data can lead to information loss, potentially impacting the accuracy or generalizability of the trained model.
- **Re-identification Risks:** Depending on the anonymization method and the dataset characteristics, there might still be a possibility of re-identifying individuals, especially when combining anonymized data with other sources.
- **Limited Applicability:** Anonymization may not be suitable for all data types or scenarios. For instance, anonymizing medical records while preserving their utility for analysis can be challenging.

2.2 Differential Privacy

This approach adds controlled noise to the data in a way that guarantees a mathematical bound on the privacy leakage, even if an adversary observes the training data and the trained model. This ensures that learning from the data does not reveal any more information about specific individuals than what can be learned from statistical summaries of the data. DP offers strong privacy guarantees but might lead to a slight reduction in model accuracy, as the added noise can obscure some of the signal in the data.

2.3 Federated Learning

This technique distributes the training process across multiple devices or servers, keeping the raw data decentralized. Only the model updates, not the individual data points, are shared among participants. This significantly reduces the privacy risks associated with sharing sensitive data, as the central server never directly observes the raw data. However, federated learning poses challenges in terms of communication overhead and coordination across distributed devices, and can also be susceptible to privacy attacks if not implemented carefully.

2.4 Homomorphic Encryption

Fully enabling computation on encrypted data, permits basic operations like addition and multiplication, serving as the foundation for more complex functions. However, the expense of frequently bootstrapping the cipher text (refreshing it due to accumulated noise) has led to the predominant use of additive homomorphic encryption schemes in privacy-preserving ML approaches. These schemes support addition operations on encrypted data and multiplication by plaintext.

2.5 Garbled Circuits

This cryptographic technique employed in scenarios involving multiple parties seeking to compute a function on their private inputs. In this process, the function is transformed into a garbled circuit, which is then transmitted along with the corresponding garbled inputs. The key feature is that the party providing the circuit remains unaware of the specifics of the other parties' inputs, achieved through techniques like oblivious transfer. The recipient, upon receiving their garbled input, can employ it with the garbled circuit to calculate the desired function's outcome.

This approach is often integrated with additive homomorphic encryption in privacy-preserving ML methodologies, ensuring secure computation and model creation.

2.6 Secure Processors

This technique is based on processors that are initially designed to safeguard sensitive code from unauthorized access by rogue software at elevated privilege levels like Intel SGX processors which are now being harnessed for privacy-preserving computation. The fundamental concept revolves around collaborative efforts among multiple data owners to execute various ML tasks, with the computation party leveraging an SGX-enabled data center. In such scenarios, even if adversaries gain control over all hardware and software within the data center, they remain unable to compromise the SGX processors utilized for computation.

2.7 Secure multi-party computation (SMPC)

This technique facilitates secure collaboration without the need to trust a third party, as computations are performed on encrypted data without revealing any information about the data or the computed results. SMPC allows organizations like hospitals, research centers, and universities to jointly analyze data for various purposes, such as ML model training or statistical analyses for anti-money laundering efforts. By keeping the data encrypted during transfer, SMPC preserves data usability while providing robust privacy protection, making it a valuable tool for secure and privacy-preserving data analysis across institutions.

2.8 Model Distillation

Introduced as a method for compressing large models into smaller ones while preserving their accuracy, knowledge/model distillation facilitates knowledge transfer between models. This process involves training the smaller model on data labeled with probability vectors generated by the initial model, encapsulating the knowledge derived from training data. This decentralized approach minimizes the risk of data breaches and unauthorized access while still allowing for effective model training and inference.

2.9 Privacy-preserving Generative Adversarial Networks

This technique preserves privacy by incorporating the principle of DP into the training process of Generative Adversarial Networks (GANs). During training, PPGAN adds carefully designed noise to gradients, ensuring that sensitive information in the training data remains obscured. This noise prevents the model from memorizing specific details of the training data, thus safeguarding individuals' privacy. Additionally, by controlling the amount of noise added, PPGAN allows for a balance between privacy protection and the utility of the generated data. Through these mechanisms, PPGAN enables the creation of high-quality synthetic data while minimizing the risk of privacy breaches.

3. ETHICAL CONSIDERATIONS IN ML

Balancing progress with protection in the development and deployment of ML systems requires careful consideration. It involves weighing the potential impact of algorithms on individuals, communities, and society at large. Addressing concerns surrounding privacy, transparency, accountability, and the broader ethical implications of ML technologies is essential to ensure responsible innovation [7].

Alongside potential benefits, there's growing recognition that the utilization of ML carries risks and may result in harm, prompting various ethical inquiries. This segment offers a concise outline of notable concerns during the development of ML models.

3.1 Algorithmic Bias

Data used for training can introduce biases, mirroring societal prejudices and reinforcing existing inequalities. For instance, a hiring algorithm trained on biased historical data may perpetuate discriminatory practices. Identifying and addressing these biases is crucial for achieving fair and equitable outcomes. Identifying and addressing these biases is crucial for achieving fair and equitable outcomes.

3.2 Transparency and Explainability

ML algorithms frequently function as opaque systems, making decisions without offering transparent explanations for their rationale. This opacity can present difficulties in comprehending decision-making processes and undermine confidence in the technology. Guaranteeing transparency and explainability in ML systems is paramount for accountability and mitigating potential harm.

3.3 Privacy

Privacy concerns emerge when sensitive data is gathered, stored, and handled without appropriate consent or security protocols. Given that algorithms handle vast amounts of personal data, there's a looming threat of privacy breaches and unauthorized utilization of sensitive information. Protecting individual privacy rights while leveraging the capabilities of ML necessitates robust data security practices and meticulous adherence to legal and ethical standards.

3.4 Accountability

Achieving a balance between progress and protection in deploying ML systems is paramount, particularly in critical sectors like healthcare and criminal justice. As these systems become more autonomous, ensuring clear accountability for harmful or biased decisions is essential, with stakeholders such as developers and regulatory bodies playing crucial roles. Robust risk assessment processes and adherence to ethical frameworks are vital for maintaining accountability and safeguarding individuals' rights in the face of evolving technology.

4. FUNDAMENTALS OF DP

DP offers a promising method for safeguarding data privacy [8]. Its primary goal is to shield an individual's sensitive data from inference attacks that target the statistics or aggregated data related to that individual. It is widely recognized that simply releasing aggregated data or statistics from a dataset often does not guarantee privacy protection.

DP introduces the concept that statistical outputs or aggregated data (including ML models) should not disclose whether any specific individual is part of the original dataset. DP ensures that the probability of generating certain statistics or aggregate values remains almost unchanged whether the dataset includes an individual's information or not.

In practical terms, DP involves a trusted data curator collecting data from various sources and performing computations on this data, such as calculating mean values or identifying the maximum and minimum values. To prevent anyone from deducing individual data points from the results, the curator adds random noise to the outcomes. This noise ensures that the released data remains stable even if any single sample in the dataset is altered. Since no individual sample can significantly impact the overall distribution, it becomes challenging for adversaries to determine any specific individual's information. Therefore, a mechanism is considered differentially private if the results of computations on the data remain consistent despite changes to any individual sample.

DP has garnered significant attention within the privacy research field over the past few decades. It evaluates the risk of revealing individual data points when computations are performed on a dataset. Refer to Fig. 1. for illustration in a typical DP framework, a trusted data curator collects data from various data owners to create a dataset. The aim is to conduct computations or analyses on the compiled dataset, such as calculating the mean value (e.g., the average salary), ensuring that data users can obtain this information without compromising the privacy of the data owners.

To guarantee that no one can accurately deduce a person's details from the computation outcome, the curator introduces random noise (i.e., DP sanitizer) to the result. This modification ensures that the published result remains unchanged even if a person's information in the underlying data is altered. Because the data of a single person does not substantially impact the distribution, adversaries are unable to confidently deduce information about any specific individual.

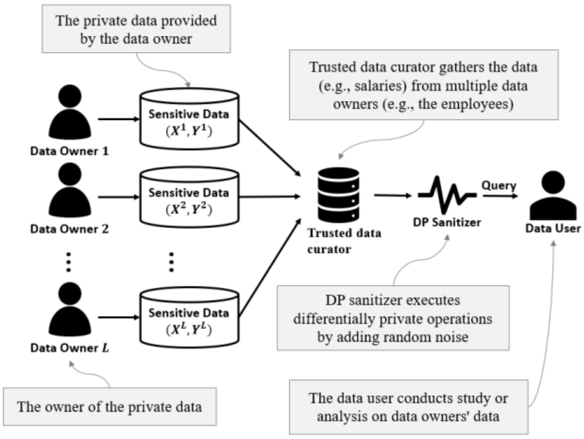
The private data provided by the data owner
Trusted data curator gathers the data (e.g., salaries) from multiple data owners (e.g., the employees)
Sensitive Data (X^1, Y^1)
Data Owner 1
Sensitive Data (X^2, Y^2)
Data Owner 2
Sensitive Data (X^L, Y^L)
Data Owner L
Trusted data curator
DP Sanitizer
Query
Data User
DP sanitizer executes differentially private operations by adding random noise
The owner of the private data
The data user conducts study or analysis on data owners' data

Figure 1. *Differential Privacy framework [1]*

5. MECHANISMS FOR DP

This part covers two widely-used mechanisms in DP, which serves as the foundation for numerous differentially private ML algorithms Laplace and Gaussian mechanism [9].

5.1 Laplace Mechanism

Laplace mechanism achieves DP by adding random noise from a Laplace distribution to the target queries or functions. In the previous section, we introduced the Laplace mechanism through the scenario described in Fig. 1. This section will provide a more systematic explanation of the Laplace mechanism and present additional examples that utilize it.

Based on the Laplace mechanism's design, given a query function f(x) that returns a numerical value, the following perturbed function [10]:

$$\mathrm{M_L}(\mathrm{x}, \mathrm{f}(\cdot), \epsilon). \tag{1}$$

meets ϵ-DP requirements:

$$\mathrm{M_L}(\mathrm{x}, \mathrm{f}(\cdot), \epsilon) = \mathrm{f}(\mathrm{x}) + \mathrm{Lap}(\triangle \mathrm{f}/\epsilon) \tag{2}$$

where $\triangle f$ is the sensitivity of query function $f(x)$, and $Lap(\triangle f/\epsilon)$ denotes the random noise drawn from the Laplace distribution with center 0 and scale $\triangle f/\epsilon$.

A histogram query can be viewed as a distinct type of counting query, in which the entirety of the data is segregated into separate sections, and the inquiry is regarding the quantity of database entries within each section.

In the example presented in Fig. 2, it can be seen a histogram with ranges for the number of employees in organizations based on specified boundaries and intervals with the number of organizations in each range without using DP.

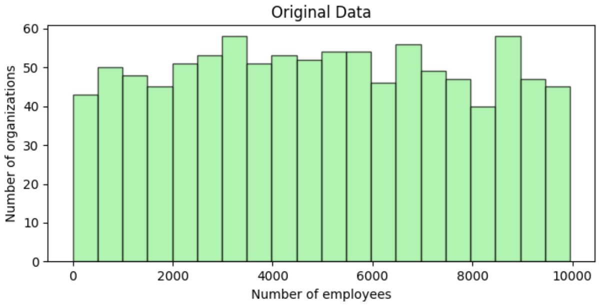

Figure 2. *Histogram of organizations by number of employees without using DP*

In order to implement DP on such a histogram query, it becomes necessary to compute the sensitivity initially. In case where the sensitivity equals 1, incorporating perturbation from $\mathrm{Lap}(1/\epsilon)$ into each of the histogram sections before disclosure is imperative, with ϵ representing the privacy allocation stipulated by the data proprietors.

In example presented on Fig. 3, a histogram illustrates the incorporation of DP by showcasing data with added noise. The epsilon value used in this instance is 0.5.

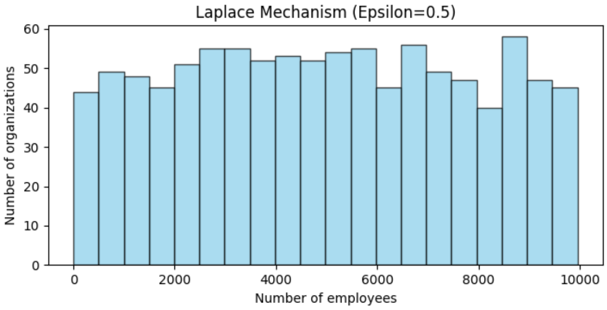

Figure 3. *Histogram of organizations by number of employees with using DP Laplace mechanism*

5.2 Gaussian mechanism

The Gaussian mechanism presents an alternative to the Laplace mechanism. Instead of introducing Laplace noise, it introduces Gaussian noise, offering a somewhat eased privacy assurance.

Given a numerical query function f:

$$\mathbb{N}^{|x|} \rightarrow \mathbb{R}^{k} \tag{3}$$

for all pairs of databases, $x \in \mathbb{N}^{|x|}$, and the privacy budget ϵ and δ, the Gaussian mechanism is defined as:

$$\mathrm{M_{GM}}(\mathrm{x}, \mathrm{f}(\cdot), \epsilon, \delta) = \mathrm{f}(\mathrm{x}) + (\mathrm{Y_1}, \mathrm{Y_{2,}}, \ldots, \mathrm{Y_k}) \tag{4}$$

In this scenario, Y_i represents a set of random variables that are independent and identically distributed, originating from a Gaussian distribution:

$$\mathrm{N}(0, \tau^2), \tau = \Delta\mathrm{f}\sqrt{2\ln{(1.25/\delta)}}\,/\epsilon \tag{5}$$

and Δf is the sensitivity of query function f.

In comparison to alternative arbitrary sounds, incorporating Gaussian disturbance offers two benefits:

- Gaussian interference aligns with numerous other noise origins (for instance, the white noise present in communication channels)
- The aggregate of Gaussian stochastic variables yields a fresh Gaussian stochastic variable. These benefits facilitate the examination and rectification of privacy-preserving ML methodologies employing the Gaussian mechanism.

In the following instance, the Gaussian mechanism is evidently observable, showcasing its inherent effectiveness in preserving privacy while maintaining data utility.

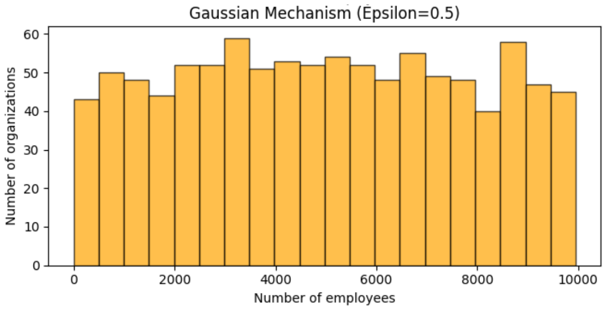

Figure 4. *Histogram of organizations by number of employees with using DP Gaussian mechanism*

5.3 Comparison

From examples above, it's apparent that both the Gaussian and Laplace mechanisms play crucial roles in privacy-preserving data analysis. While the Gaussian mechanism operates based on a normal distribution, the Laplace mechanism relies on a Laplace distribution. Despite these foundational differences, the ultimate results achieved in the given example remain notably similar, highlighting the versatility of both methods in ensuring privacy without compromising analytical outcomes.

Using MSE (Mean Squared Error) as a measure, different epsilon values are applied to the privatized data obtained from the original dataset. For each epsilon value, a data sample is generated from the original dataset, followed by applying the Laplace and Gaussian mechanisms to the sample. Then, MSE values for privatized data are calculated for both mechanisms. Finally, the results are displayed in the console, allowing for comparison of privacy mechanisms' performance across different epsilon values. This process helps understand how DP parameters affect the quality of privatized data and provides insights into the effectiveness of various privacy protection mechanisms.

In the analysis of DP mechanisms, the MSE of the Laplace and Gaussian mechanisms was conducted using different epsilon values. The results, as presented in the Table 1 for Laplace mechanism and in Table 2 for Gaussian mechanism, offer a detailed view of the MSE for each mechanism across various epsilon values. Below is a summary of the MSE for epsilon values from 0.1 to 1 with increment of 0.05.

The data illustrates a distinct difference between the Laplace and Gaussian mechanisms for different epsilon values (Fig. 5) measured by MSE.

Based on the results from the previous illustration detailing the MSE values for the Laplace mechanism demonstrate a notable fluctuation as epsilon increases. Specifically, at epsilon values of 0.1 and 0.25, relatively low MSE values. However, a significant escalation in MSE occurs at epsilon values of 0.2, 0.45, and 0.7, where the MSE peaks. Notably, at epsilon 0.8 and 0.95, the MSE diminishes to 0.0. This erratic pattern suggests that the Laplace mechanism's performance is particularly sensitive to changes in epsilon, with certain values leading to significantly increased error rates, while others result in minimal error.

Table 1. *Detailed view of the MSE for Laplace mechanism across various configuration*

MSE values for Laplace mechanism	
EPSILON	**MSE**
0.1	0.42
0.15	2.12
0.2	15.07
0.25	0.25
0.3	1.6
0.35	4.69
0.4	3.38
0.45	15.7
0.5	14.08
0.55	4.95
0.6	2.85
0.65	2.8
0.7	19.72
0.75	3.61
0.8	0.0
0.85	0.36
0.9	3.21
0.95	0.0
1	2.04

On the other hand, the MSE values for the Gaussian mechanism exhibit a more gradual increase with epsilon. Notable deviations occur at epsilon 0.2, 0.5 and 0.85. However, the overall trend indicates a relatively stable performance compared to the Laplace mechanism, with fewer instances of drastic fluctuations in error rates.

When epsilon is set to 0.5, both mechanisms exhibit relatively high MSE values, with the Laplace mechanism recording almost double MSE than the Gaussian mechanism. That difference can be seen in Fig. 3. and Fig 4.

Table 2. *Detailed view of the MSE for Gaussian mechanism across various configuration*

MSE values for Gaussian mechanism	
EPSILON	**MSE**
0.1	7.47
0.15	0.75
0.2	27.86
0.25	10.1
0.3	4.41
0.35	0.14
0.4	0.11
0.45	1.45
0.5	7.15
0.55	2.0
0.6	0.1
0.65	0.61
0.7	0.06
0.75	0.27
0.8	0.25
0.85	4.29
0.9	0.01
0.95	0.03
1	0.12

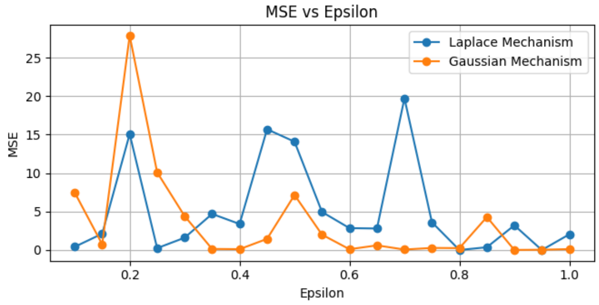

Figure 5. *MSE for different epsilon values*

As shown in Table 3 the Laplace mechanism demonstrates a higher average MSE of 5.1 compared to the Gaussian mechanism's average of 3.54. This suggests that, on average, the Gaussian mechanism provides more accurate data in contrast to Laplace mechanism which provides slightly higher privacy protection.

Table 3. *Comparison the results of Laplace and Gaussian MSE gain for different epsilon values*

Laplace and Gaussian MSE comparison	
MSE for Laplace mechanism	5.1
MSE for Gaussin mechanism	3.54

6. CHALLENGES AND LIMITATIONS

6.1 Scalability issues

Privacy-preserving algorithms like DP often need to be more accurate than their non-private counterparts, which can be particularly challenging when scaling up data processing [11].

6.2 Utility vs. privacy trade-offs

- **Multiple Queries**: With DP, the privacy guarantee for a database weakens as an algorithm is run multiple times over it. As a result, it can be difficult to maintain a reasonable balance between privacy and accuracy when multiple queries are required.
- **Dataset Size**: The inaccuracy introduced by DP through noise addition can be manageable for large datasets but problematic for small ones. This trade-off between privacy and utility becomes more pronounced with varying dataset sizes.
- **Adding Noise**: Adding noise to ensure privacy can decrease the accuracy of results. Finding the right balance between privacy and utility can be complex.
- **Suitability for Data Types**: DP may not be suitable for all types of data or queries, as some data characteristics may make it difficult to achieve a good privacy-utility balance.

6.3 Potential weaknesses

As with any definition, DP also has some weaknesses.

Its weaknesses include:

- **Data Insight Limitation**: The restructured data resulting from the application of DP algorithms can hinder organization analysts from extracting valuable insights, potentially limiting the practical usefulness of the data.
- **Accuracy Cost for Specific Queries**: Ensuring privacy often results in decreased accuracy compared to the non-private version of an algorithm. For some queries, this accuracy cost can be very large. For instance, releasing the maximum value in a database with a large possible range can lead to significant accuracy loss when made private.
- **Weakened Guarantees with Repeated Queries**: Running an algorithm multiple times over the same database weakens the privacy guarantees, complicating the balance between privacy and accuracy when multiple queries are necessary.

7. CONCLUSION

The integration of ML into various sectors has transformed data-driven decision-making but also introduced significant privacy risks. Exposing sensitive information during ML training can lead to identity theft, financial fraud, and discrimination. DP addresses these risks by adding controlled noise to datasets, ensuring individual data protection while enabling meaningful analysis. Techniques like anonymization, federated learning, and homomorphic encryption complement DP but come with their own challenges. The Laplace and Gaussian mechanisms within DP effectively balance privacy and utility, with the Laplace mechanism often preserving data quality better. However, scalability issues, utility versus privacy trade-offs, and accuracy costs for specific queries remain significant challenges. The ongoing development of privacy-preserving techniques is essential to overcome these limitations. By refining these methods, we can protect individual privacy while leveraging ML's potential. Achieving this balance is crucial for fostering trust and enabling responsible innovation in data-driven technologies. Continuous research and improvement are necessary to maintain this balance and address emerging challenges.

ACKNOWLEDGEMENTS

This study was supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and these results are parts of Grant No. 451-03-66 / 2024-03 / 200132 with the University of Kragujevac - Faculty of Technical Sciences Čačak.

REFERENCES

[1] *Morris Chang, J., Zhuang, D. & Dumindu Samaraweera, G. (2022). Privacy-Preserving Machine Learning. New York.*

[2] Rao Aravilli, S. (2024). *Privacy-Preserving Machine Learning*, Packt Publishing, UK.

[3] Huang, T. & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous and Pseudonymous Data, *IEEE Access,* 11, 12. https://doi.org/10.1109/ACCESS.2023.3321578

[4] El Mestari, S. Z., Lenzini, G., Demirci, H. (2024). Preserving data privacy in machine learning systems, *Computers & Security,* 137, 103605. https://doi.org/10.1016/j.cose.2023.103605

[5] Moshawrab, M., Adda, M., Bouzouane, A., Ibrahim, H., Raad, A. (2023). Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives. *Electronics*, 12, 2287. https://doi.org/10.3390/electronics12102287

[6] Majeed, A. & Lee, S.(2021). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey, *IEEE Acces,* 9, 8512-8545. https://doi.org/10.1109/ACCESS.2020.3045700

[7] Li, D., Wang, J., Tan, Z., Li, X., & Hu, Y. (2020). Differential Privacy Preservation in Interpretable Feedforward - Designed Convolutional Neural Networks. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).* https://doi.org/10.1109/trustcom50675.2020.00089

[8] Huang, T. & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous and Pseudonymous Data, *IEEE Access*, 11, https://doi.org/10.1109/ACCESS. 2023.3321578

[9] Iqbal, M., Tariq, A. , Adnan, M. Ud Din, I. & Qayyum, T. (2023). FL-ODP: An Optimized Differential Privacy Enabled Privacy Preserving Federated Learning, *IEEE Access*, 11, 116674-116683. https://doi.org/10.1109/ACCESS.2023.3325396.

[10] Song, H., Shen, H. Zhao, N., He, Z., Xiong, W., Wu, M., Zhang, M.(2024). Adaptive personalized privacy-preserving data collection scheme with local differential privacy, *Journal of King Saud University - Computer and Information Sciences*, 36(4), 102042.https://doi.org/10.1016/j.jksuci.2024.102042