Terbit online pada laman web jurnal: **https://jurnal.plb.ac.id/index.php/tematik/index**

T E M A T I K

Jurnal **Teknologi Informasi Komunikasi (e-Journal)**

Vol. 12 No. 2 (2025) 179 - 185 ISSN Media Elektronik: 2443-3640

Analisis Kinerja Differential Privacy pada Data Resep Medis Menggunakan Laplace dan Gaussian Mechanism

Performance Analysis of Differential Privacy on Medical Prescription Data Using Laplace and Gaussian Mechanisms

[1]Muhammad Akmal Ramadan, [2]Asep Id Hadiana, [3]Edvin Ramadhan
[1]Informatika, FSI, Universitas Jenderal Achmad Yani
[1]akmalramadhan012@gmail.com, [2]asep.hadiana@lecture.unjani.ac.id, [3]edvin.ramadhan@lecture.unjani.ac.id

Abstract

Protecting medical data is a critical priority in the digital era due to the high risk of patient information leakage and misuse. Regulations such as HIPAA, GDPR, and Indonesia's Health Law No. 36 of 2009 mandate strong safeguards, yet technical challenges in implementation persist. Differential Privacy (DP) provides a mathematical framework to ensure privacy by injecting controlled noise, making it difficult to identify individuals while maintaining data utility. This study evaluates the effectiveness of DP on the prescriptions dataset by comparing two widely used mechanisms: Laplace and Gaussian. Four sensitive attributes (row_id, subject_id, hadm_id, icustay_id) were analyzed under privacy budgets ε = {0.1, 0.5, 1.0, 5.0}. Performance was assessed using Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) to capture the trade-off between privacy and accuracy. The results demonstrate that the Laplace mechanism consistently outperforms Gaussian, producing lower RMSE values and exhibiting greater stability, particularly at small to moderate ε. Gaussian tends to yield high errors at low ε and only approaches Laplace performance at high ε. These findings highlight the critical role of mechanism selection and privacy budget in determining the quality of protected medical data. Practically, the study recommends adopting the Laplace mechanism with ε = 0.5–1.0 for implementing Differential Privacy in electronic medical record systems. This configuration provides an optimal balance between patient privacy protection and data utility for healthcare analytics.

Keywords: Differential Privacy, Medical Data Security, Electronic Medical Records, Prescriptions, Patient Privacy

Abstrak

Perlindungan data medis menjadi prioritas utama di era digital karena tingginya risiko kebocoran dan penyalahgunaan informasi pasien. Regulasi seperti HIPAA, GDPR, dan Undang-Undang Kesehatan No. 36 Tahun 2009 mewajibkan penerapan keamanan, namun tantangan teknis dalam implementasi masih besar. Differential Privacy (DP) menawarkan pendekatan matematis untuk menjamin privasi dengan menambahkan noise terkontrol sehingga keberadaan individu sulit diidentifikasi tanpa mengurangi nilai analisis data. Penelitian ini bertujuan mengevaluasi efektivitas DP pada dataset prescriptions. Data yang diuji bersumber dari database rekam medis publik MIMIC-III yang mencakup ribuan catatan resep. Empat atribut sensitif (row_id, subject_id, hadm_id, icustay_id) dianalisis menggunakan variasi parameter ε = {0.1, 0.5, 1.0, 5.0}. Evaluasi dilakukan menggunakan Mean Squared Error (MSE) dan Root Mean Squared Error (RMSE) untuk menilai trade-off antara privasi dan akurasi. Hasil penelitian menunjukkan bahwa Laplace mechanism lebih stabil dibanding Gaussian dengan nilai RMSE konsisten lebih rendah, terutama pada ε kecil hingga sedang. Gaussian menghasilkan error tinggi pada ε kecil dan baru mendekati Laplace pada ε besar. Kebaruan penelitian ini terletak pada analisis kuantitatif langsung menggunakan RMSE untuk membandingkan kinerja mekanisme Laplace dan Gaussian pada atribut-atribut identitas rekam medis, memberikan bukti empiris praktis yang melengkapi studi sebelumnya yang seringkali bersifat teoretis atau tinjauan umum. Temuan ini menegaskan bahwa pemilihan mekanisme dan parameter ε sangat menentukan kualitas data medis yang diproteksi. Secara praktis, penelitian ini merekomendasikan penggunaan Laplace mechanism dengan ε = 0.5–1.0 untuk implementasi Differential Privacy pada sistem rekam medis elektronik. Konfigurasi ini memberikan keseimbangan optimal antara perlindungan privasi pasien dan utilitas data untuk analisis kesehatan.

Kata kunci: Differential Privacy, Data Medis, Rekam Medis Elektronik, Laplace Mechanism, Gaussian Mechanism

1. Pendahuluan

Perkembangan teknologi informasi di era digital telah memberikan dampak besar terhadap berbagai sektor, termasuk bidang kesehatan. Salah satu implementasi penting adalah penggunaan Rekam Medis Elektronik (RME) yang menyimpan informasi pasien dalam bentuk digital untuk mendukung diagnosis, perawatan, serta penelitian Kesehatan [1], [2]. Meskipun

Diterima Redaksi: 06-10-2025 | Selesai Revisi: 17-11-2025 | Diterbitkan Online: 19-12-2025

bermanfaat, RME sangat rentan terhadap ancaman kebocoran data dan penyalahgunaan, yang dapat membahayakan privasi pasien [3].

Berbagai regulasi telah ditetapkan untuk menjaga keamanan data medis, seperti Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat, General Data Protection Regulation (GDPR) di Uni Eropa, serta Undang-Undang No. 36 Tahun 2009 tentang Kesehatan di Indonesia [4], [5], [6]. Regulasi tersebut menekankan pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data medis. Namun, perlindungan data berbasis anonimisasi tradisional terbukti masih rentan terhadap serangan rekonstruksi dan linkage attack, yang dapat mengidentifikasi individu dari data yang telah dihapus identitasnya [7], [8].

Differential Privacy (DP) muncul sebagai pendekatan baru yang mampu memberikan jaminan matematis terhadap privasi individu dengan menambahkan noise terkontrol pada data atau hasil analisis [9], [10]. Beberapa penelitian telah mengevaluasi penerapan [11], [12] DP di sektor kesehatan, namun mayoritas menggunakan dataset simulasi atau MIMIC-III. Belum banyak penelitian yang secara spesifik mengevaluasi DP pada dataset prescriptions yang berisi informasi obat dan resep medis [13], [14]. Pemilihan dataset ini didasarkan pada justifikasi ilmiah bahwa data resep memiliki tingkat sensitivitas yang sangat tinggi; data ini tidak hanya mencatat ID pasien, tetapi secara longitudinal mengaitkan individu tersebut dengan kondisi medis spesifik seringkali bersifat rahasia, kronis, atau terkait kesehatan mental melalui obat yang diresepkan. Padahal, dataset ini sangat krusial untuk dianalisis guna mengidentifikasi pola pengobatan pasien [15], [16].

Berdasarkan permasalahan tersebut, penelitian ini dilakukan untuk mengevaluasi efektivitas Laplace Mechanism dan Gaussian Mechanism dalam menjaga privasi data prescriptions dengan variasi parameter ε. Penelitian ini juga mengukur trade-off antara privasi dan akurasi data menggunakan metrik RMSE dan MSE. Hasil penelitian diharapkan dapat memberikan rekomendasi parameter optimal dalam penerapan Differential Privacy pada sistem RME. Secara khusus bagi konteks Indonesia, yang sedang gencar melakukan transformasi digital kesehatan nasional (misalnya melalui platform SATUSEHAT), temuan ini dapat memperkaya implementasi DP dengan memberikan acuan teknis berbasis bukti empiris. Dengan demikian, penelitian ini berkontribusi menjembatani kebutuhan analisis data kesehatan publik dengan kewajiban perlindungan privasi pasien yang diamanatkan dalam UU No. 36 Tahun 2009 [6], sehingga privasi pasien tetap terlindungi tanpa mengorbankan kegunaan data.

2. Metode Penelitian

Diagram alir penelitian ditunjukkan pada Gambar 1. Tahap awal adalah preprocessing dataset prescriptions dengan mengambil sampling 1.014 data, kemudian lanjut pada penerapan noise dengan Laplace atau Gaussian mechanism sesuai variasi ε. Lalu untuk tahap selanjutnya adalah alur validasi, yaitu perhitungan RMSE/MSE, dan terakhir analisis hasil komprehensif dalam bentuk tabel serta visualisasi grafik (line plot, bar, dan boxplot) untuk menarik kesimpulan.

Penelitian ini menggunakan dataset prescriptions yang berisi informasi resep medis dengan atribut numerik dan identitas pasien, antara lain row_id, subject_id, hadm_id, dan icustay_id. Keempat atribut ini dipilih karena mengandung informasi sensitif yang dapat berpotensi menimbulkan pelanggaran privasi apabila tidak dilindungi [9], [10]. Dataset diproses dalam format CSV dan dianalisis menggunakan Python (NumPy, Pandas, Matplotlib).

Differential Privacy menyediakan jaminan formal bahwa keluaran analisis tidak akan berubah secara signifikan meskipun data individu tertentu ditambahkan atau dihapus dari dataset [20], [23].

Definisi formal DP seperti terlihat pada Rumus 1:

$$\Pr\ [M(D1)\ \epsilon\ S] \leq e^{\epsilon}\ \cdot \Pr\ [M(D2)\epsilon S] \quad (1)$$

untuk semua dataset D1,D2 yang berbeda hanya pada satu entri, semua himpunan keluaran S⊆Range(M), dan mekanisme acak M. Parameter ϵ (epsilon) menentukan tingkat privasi: semakin kecil nilai ϵ, semakin tinggi privasi yang diberikan, namun dengan konsekuensi penurunan akurasi [22].

Penelitian ini membandingkan dua mekanisme paling umum dalam DP:

Pada Laplace Mechanism, noise ditambahkan ke data menggunakan distribusi Laplace dengan skala seperti terlihat pada Rumus 2:

$$b = \frac{\Delta f}{\epsilon} \quad (2)$$

Δf adalah sensitivitas fungsi. Mekanisme ini lebih stabil dan banyak digunakan dalam aplikasi tabular [1], [9].

Pada Gaussian Mechanism, noise diambil dari distribusi Gaussian dengan varians seperti terlihat pada Rumus 3:

$$\sigma^2 = 2\ \mathrm{In}(1.25/\delta)\ .\frac{\Delta f^2}{\epsilon^2} \quad (3)$$

δ adalah parameter tambahan yang mengatur probabilitas kegagalan. Gaussian lebih sering digunakan dalam pembelajaran mesin berbasis gradient descent [2], [3], tetapi performanya dapat menurun drastis pada ε kecil.

Eksperimen dilakukan dengan variasi parameter ϵ\epsilonϵ = {0.1, 0.5, 1.0, 5.0}. Nilai ε kecil (0.1)

DOI: https://doi.org/10.38204/tematik.v12i2.2634

mewakili kondisi privasi tinggi namun akurasi rendah, sedangkan nilai ε besar (5.0) mewakili privasi rendah dengan akurasi tinggi. Nilai sedang (0.5 dan 1.0) dipilih karena dianggap realistis dalam praktik medis [11], [17].

Untuk mengukur trade-off privasi–akurasi, penelitian ini menggunakan dua metrik error utama:

Mean Squared Error (MSE) seperti terlihat pada Rumus 4:

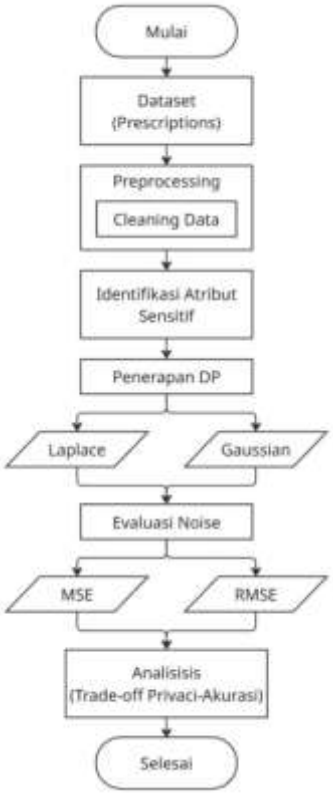
$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_1)^2 \quad (4)$$

Root Mean Squared Error (RMSE) seperti terlihat pada Rumus 5:

$$RMSE = \sqrt{MSE} \quad (5)$$

Kedua metrik ini dipilih karena mampu merepresentasikan seberapa jauh data hasil proteksi berbeda dari data asli. MSE mengukur rata-rata error kuadrat, sedangkan RMSE memberikan nilai error dalam skala yang sama dengan data asli, sehingga lebih mudah diinterpretasikan [12], [19].

Diagram alir penelitian ditunjukkan pada Gambar 1. Tahap awal adalah preprocessing dataset prescriptions, kemudian penerapan noise dengan Laplace atau Gaussian mechanism sesuai variasi ε, dilanjutkan dengan perhitungan RMSE/MSE, dan terakhir analisis hasil dalam bentuk tabel serta visualisasi grafik.



Gambar 1. Alur Penelitian

3. Hasil dan Pembahasan

3.1. Hasil Eksperimen

Penelitian ini mengevaluasi penerapan Differential Privacy (DP) pada dataset prescriptions dengan dua mekanisme, yaitu Laplace dan Gaussian, menggunakan variasi parameter ε = {0.1, 0.5, 1.0, 5.0}. Empat atribut sensitif (row_id, subject_id, hadm_id, icustay_id) dianalisis karena berpotensi mengungkap identitas pasien.

Evaluasi dilakukan dengan menghitung Mean Squared Error (MSE) dan Root Mean Squared Error (RMSE) sebagai ukuran perbedaan antara data asli dengan data hasil privatisasi.

Laplace Mechanism: ε = 0.1 → RMSE ≈ 13–14 (noise tinggi, akurasi rendah); ε = 0.5 → RMSE turun menjadi 2–3, menandakan keseimbangan privasi–akurasi; ε = 1.0 → RMSE ≈ 1.4, akurasi tinggi dengan privasi masih terjaga; ε = 5.0 → RMSE ≈ 0.2, data hampir identik dengan aslinya (privasi lemah).

Gaussian Mechanism: ε = 0.1 → RMSE ≈ 46–50, distorsi data sangat tinggi; ε = 0.5 → RMSE ≈ 9–10, masih jauh lebih besar dari Laplace; ε = 1.0 → RMSE ≈ 5.0; ε = 5.0 → RMSE ≈ 1.0, mirip dengan Laplace.

Tabel 1. RMSE per Kolom dengan Laplace Mechanism

Kolom	ε=0.1	ε=0.5	ε=1.0	ε=5.0
hadm_id	13.20	2.87	1.45	0.29
icustay_id	13.30	3.11	1.45	0.29
row_id	14.82	2.75	1.43	0.28
subject_id	13.91	2.77	1.37	0.28

Tabel 1 menampilkan nilai RMSE hasil penerapan Laplace Mechanism pada empat kolom sensitif. Terlihat bahwa pada ε = 0.1, semua kolom menghasilkan RMSE tinggi (≈ 13–15), menunjukkan noise besar dan akurasi rendah. Namun, ketika ε dinaikkan menjadi 0.5, nilai RMSE turun drastis (≈ 2.7–3.1), dan semakin stabil pada ε = 1.0 (≈ 1.4). Pada ε = 5.0, RMSE hampir mendekati nol (≈ 0.28–0.29), yang menandakan data hampir identik dengan kondisi asli. Pola ini konsisten di semua kolom (row_id, subject_id, hadm_id, icustay_id), menunjukkan bahwa Laplace memberikan hasil yang stabil dan seimbang di seluruh atribut.

Pada Tabel 2, memperlihatkan nilai RMSE dari Gaussian Mechanism. Pada ε = 0.1, RMSE sangat tinggi (≈ 47–49), hampir empat kali lipat lebih buruk dibanding Laplace. Meskipun RMSE menurun saat ε meningkat menjadi 0.5 (≈ 9–10) dan 1.0 (≈ 4.6–5.1), nilainya tetap jauh lebih besar dibandingkan Laplace. Baru pada ε = 5.0, kedua mekanisme menunjukkan hasil yang hampir serupa (RMSE ≈ 0.95).

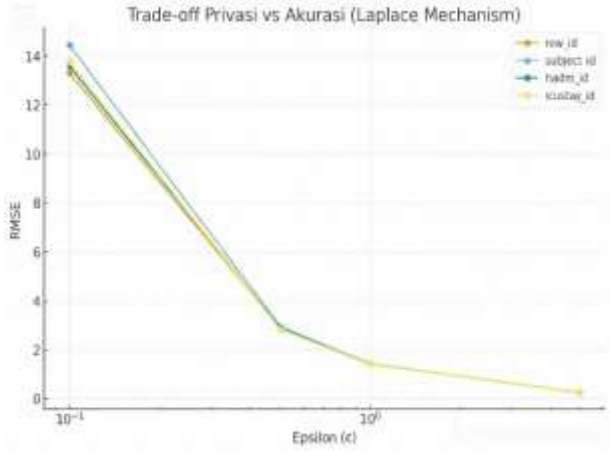
DOI: https://doi.org/10.38204/tematik.v12i2.2634

Tabel 2. RMSE per Kolom dengan Laplace Mechanism

Kolom	ε=0.1	ε=0.5	ε=1.0	ε=5.0
hadm_id	47.81	9.41	4.61	0.95
icustay_id	47.51	9.91	4.85	0.95
row_id	49.18	9.60	4.94	0.96
subject_id	48.54	9.91	5.10	0.97

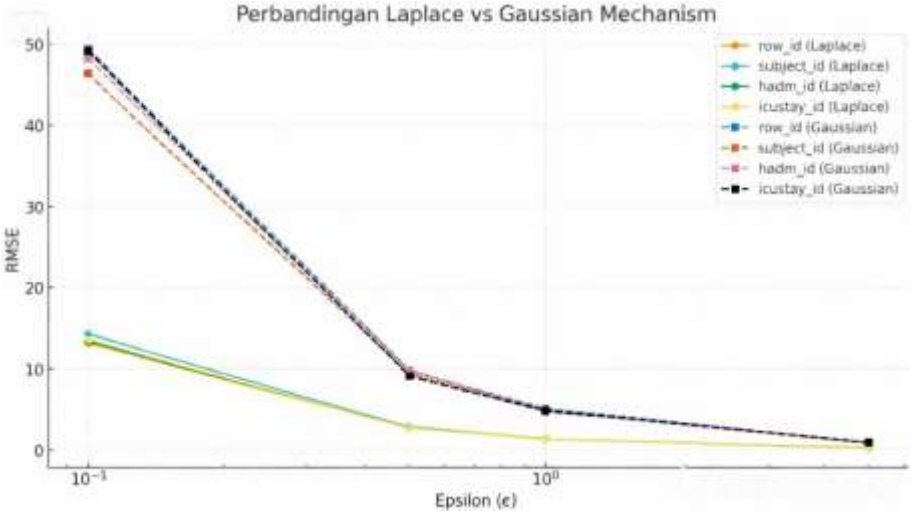
Pola pada Tabel 1 ini menunjukkan bahwa Gaussian cenderung menghasilkan distorsi lebih besar pada ε kecil hingga sedang, sehingga mengurangi utilitas data prescriptions.

Grafik pada Gambar 1 memperlihatkan hubungan antara nilai ε (epsilon) dengan RMSE pada mekanisme Laplace: Semakin kecil ε (0.1) → RMSE tinggi → data semakin "berisik" (privasi kuat, akurasi rendah); Semakin besar ε (5.0) → RMSE rendah → data mirip aslinya (privasi lemah, akurasi tinggi); Semua atribut (row_id, subject_id, hadm_id, icustay_id) menunjukkan pola serupa.



Gambar 1. Trade-off privasi dan akurasi pada Laplace Mechanism

Hal ini menunjukkan hubungan antara nilai ε dengan RMSE pada Laplace Mechanism. Terlihat bahwa semakin besar ε, semakin rendah error, menandakan akurasi meningkat namun privasi menurun.



Gambar 2. Trade-off privasi dan akurasi pada Laplace Mechanism

Grafik pada Gambar 2 memperlihatkan perbandingan Laplace vs Gaussian Mechanism pada dataset prescriptions: Laplace (garis solid, lingkaran) → RMSE lebih rendah di ε kecil hingga sedang → lebih seimbang antara privasi dan akurasi; Gaussian (garis putus-putus, kotak) → RMSE jauh lebih tinggi pada ε kecil → lebih kuat menjaga privasi, tapi data menjadi sangat tidak akurat; Pada ε besar (5.0) → kedua mekanisme hampir sama, error sangat rendah.

Perbedaan kinerja kedua mekanisme divisualisasikan pada Gambar 2, yang menegaskan bahwa Laplace consistently outperform Gaussian pada ε rendah hingga sedang.

DOI: https://doi.org/10.38204/tematik.v12i2.2634

3.2. Ringkasan Perbandingan Laplace vs Gaussian

Tabel 3 menampilkan rata-rata RMSE dari masing-masing mekanisme untuk tiap nilai ε:

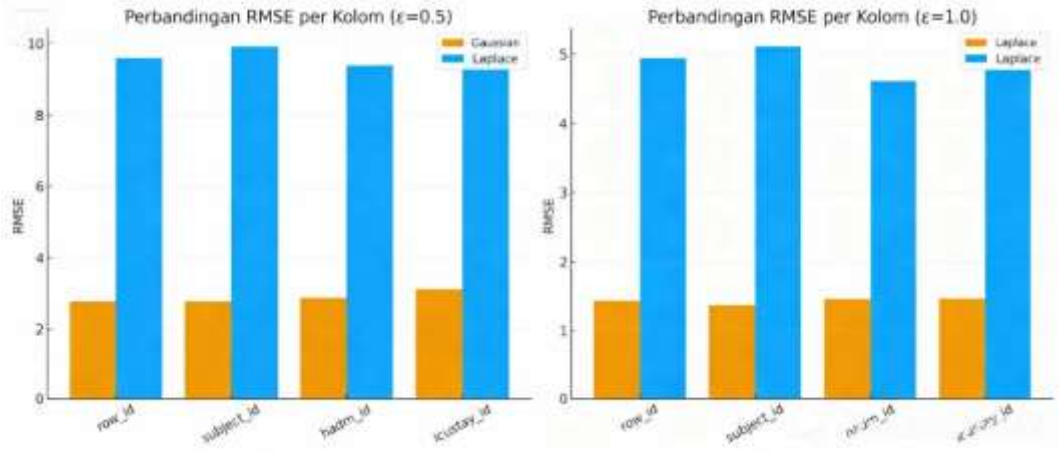
Tabel 3. Perbandingan Rata-rata RMSE Laplace vs Gaussian

ε (Epsilon)	Laplace (Average RMSE)	Gaussian (Average RMSE)
0.1	13.78	48.42
0.5	2.86	9.63
1.0	1.43	4.97
5.0	0.27	0.98

Tabel 3 memperlihatkan bahwa Laplace consistently outperform Gaussian pada nilai ε rendah hingga sedang. Pada ε = 0.1, perbedaan rata-rata RMSE antara Laplace (13.78) dan Gaussian (48.42) sangat signifikan. Hal ini menunjukkan bahwa Gaussian menambahkan noise jauh lebih besar, sehingga mengurangi utilitas data secara drastis.

Pada ε = 0.5 dan ε = 1.0, Laplace kembali menunjukkan performa lebih baik dengan rata-rata RMSE masing-masing 2.86 dan 1.43, jauh lebih rendah dibanding Gaussian sebesar 9.63 dan 4.97. Hal ini membuktikan bahwa Laplace lebih stabil dan seimbang dalam menjaga privasi sekaligus mempertahankan akurasi data prescriptions.

Pada ε besar (5.0), perbedaan antara kedua mekanisme relatif kecil karena noise yang ditambahkan minimal. Kondisi ini menegaskan bahwa semakin besar ε, semakin lemah privasi namun semakin tinggi akurasi data.



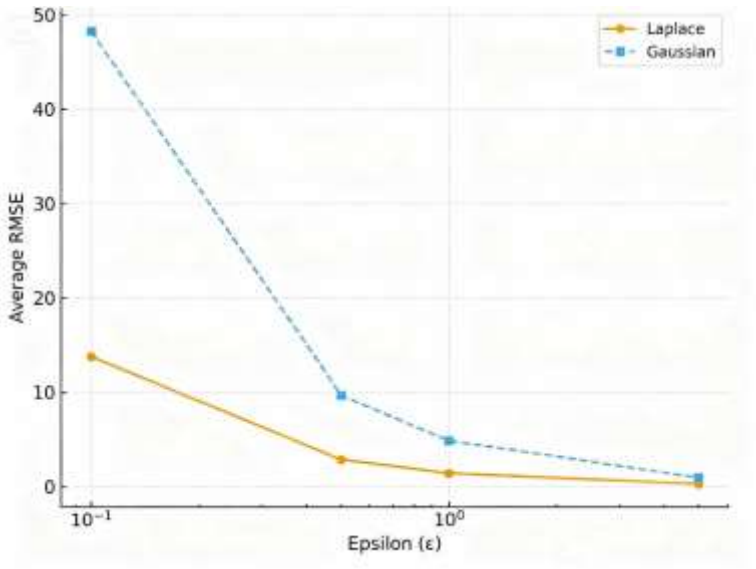
Gambar 3. Perbandingan RMSE per kolom sensitif pada ε = 0.5 dan ε = 1.0

Gambar 3 menampilkan perbandingan RMSE pada empat atribut sensitif (row_id, subject_id, hadm_id, icustay_id) antara Laplace dan Gaussian mechanism, khusus pada nilai ε = 0.5 dan ε = 1.0. Terlihat bahwa pada kedua nilai ε, Laplace consistently menghasilkan error yang lebih rendah dibandingkan Gaussian di semua kolom. Perbedaan paling mencolok terlihat pada ε = 0.5, di mana Gaussian menunjukkan RMSE tiga hingga empat kali lebih besar dibanding Laplace. Hal ini menguatkan bahwa pada privasi tingkat sedang, Laplace mampu menjaga akurasi data lebih baik dibanding Gaussian. Seperti ditunjukkan pada Gambar 3, Laplace menghasilkan RMSE yang lebih rendah secara konsisten di semua kolom, terutama pada ε = 0.5. Hal ini menegaskan stabilitas Laplace mechanism dibandingkan Gaussian dalam konteks data prescriptions.

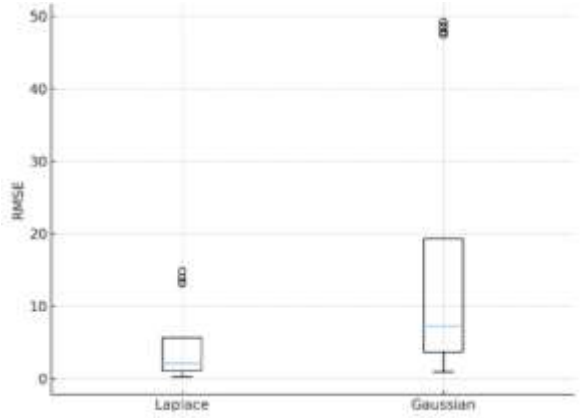
Gambar 4 menyajikan tren rata-rata RMSE untuk kedua mekanisme seiring perubahan nilai ε. Grafik memperlihatkan bahwa ketika ε semakin besar (privasi berkurang), RMSE menurun pada kedua mekanisme. Namun, kurva Laplace cenderung lebih stabil dan konsisten, sedangkan Gaussian mengalami lonjakan error pada ε kecil. Dengan demikian, Laplace menawarkan trade-off privasi–akurasi yang lebih seimbang, khususnya pada rentang ε = 0.5–1.0 yang dianggap relevan untuk aplikasi praktis. Berdasarkan Gambar 4, tren rata-rata RMSE menunjukkan bahwa Laplace lebih stabil dibanding Gaussian. Pada nilai ε kecil, perbedaan kedua mekanisme sangat signifikan, sementara pada ε besar keduanya cenderung konvergen.

Gambar 5 menampilkan distribusi nilai RMSE untuk Laplace dan Gaussian mechanism. Boxplot memperlihatkan bahwa distribusi error Laplace lebih sempit, menandakan stabilitas hasil dengan variasi yang rendah. Sebaliknya, Gaussian menunjukkan sebaran error yang lebih lebar, terutama pada ε kecil, yang mencerminkan variabilitas tinggi dan hasil yang kurang dapat diprediksi. Visualisasi ini memperkuat temuan bahwa Laplace lebih unggul dari sisi konsistensi performa. Seperti terlihat pada Gambar 5, distribusi RMSE pada Laplace lebih sempit dibandingkan Gaussian, menunjukkan bahwa Laplace menghasilkan performa yang lebih stabil. Sebaliknya, Gaussian cenderung fluktuatif dengan variasi error yang lebih tinggi.

DOI: https://doi.org/10.38204/tematik.v12i2.2634



Gambar 4. Rata-rata RMSE terhadap variasi epsilon (Laplace vs Gaussian)



Gambar 5. Distribusi RMSE Laplace vs Gaussian (Boxplot)

3. 2 Pembahasan

Perbandingan Laplace dan Gaussian mechanism menegaskan bahwa pemilihan mekanisme DP harus disesuaikan dengan konteks aplikasi. Temuan bahwa Laplace mechanism secara signifikan lebih stabil untuk kueri ID tabular (subject_id, hadm_id) sejalan dengan tinjauan literatur yang menekankan perlunya kalibrasi noise yang cermat dalam analisis data medis. Penelitian ini memperluas temuan teoretis fundamental Dwork et al dengan memberikan bukti empiris kuantitatif pada data resep medis yang spesifik. Pada sistem rekam medis elektronik (RME), di mana data prescriptions harus tetap akurat untuk kepentingan klinis, Laplace mechanism dengan ε sedang (0.5–1.0) adalah pilihan yang paling rasional. Gaussian mechanism, meskipun menawarkan jaminan privasi (ε,δ) -DP, terbukti kurang praktis pada ε kecil karena error yang dihasilkan terlalu tinggi dan mengurangi utilitas data secara drastis.

Hasil ini memiliki implikasi kebijakan dan integrasi sistem RME yang kuat. Regulasi seperti HIPAA, GDPR, maupun UU Kesehatan Indonesia menekankan pentingnya perlindungan data pasien. Akan tetapi, regulasi ini seringkali bersifat high-level dan tidak memberikan arahan teknis implementasi, sehingga menciptakan kesenjangan antara mandat hukum dan eksekusi teknis. Penelitian ini berkontribusi menjembatani kesenjangan tersebut. Bagi pembuat kebijakan di Indonesia, temuan ini dapat menjadi dasar ilmiah untuk menyusun Standar Prosedur Operasional (SPO) teknis terkait privasi data pada platform digital kesehatan nasional (seperti SATUSEHAT). Secara praktis untuk integrasi RME, rekomendasi ε = 0.5–1.0 dengan Laplace mechanism dapat diterjemahkan menjadi 'konfigurasi default' (default configuration) bagi pengembang sistem. Ini membuktikan bahwa DP bukanlah konsep yang murni teoretis, melainkan dapat diterapkan secara praktis dengan trade-off yang terukur untuk melindungi data resep pasien tanpa menghancurkan nilai analitisnya untuk analisis kesehatan publik.

Dari sisi metodologi penelitian ini terbatas pada evaluasi tabular data prescriptions dengan metrik RMSE/MSE. Arah penelitian lanjutan terbuka lebar, mencakup penerapan DP pada deep learning medis melalui DP-SGD dan integrasinya dengan federated learning untuk kolaborasi aman antar-rumah sakit. Selain itu, penting untuk mengeksplorasi mekanisme hybrid yang lebih optimal dan melakukan validasi menggunakan dataset medis lokal Indonesia untuk meningkatkan relevansi kontekstual. Evaluasi di masa depan juga harus diperluas melampaui RMSE/MSE dengan menggunakan multi-metrik yang lebih komprehensif, seperti utility loss atau akurasi model prediktif, untuk mendapatkan gambaran dampak privasi yang lebih utuh.

DOI: https://doi.org/10.38204/tematik.v12i2.2634

4. Kesimpulan

Penelitian ini menemukan bahwa Laplace mechanism secara konsisten lebih unggul daripada Gaussian mechanism untuk proteksi data resep medis, dengan menunjukkan stabilitas dan error (RMSE) yang jauh lebih rendah, terutama pada nilai ε kecil hingga sedang. Implikasi praktis utamanya adalah rekomendasi penggunaan Laplace mechanism dengan ε = 0.5–1.0 sebagai konfigurasi optimal pada sistem rekam medis elektronik (RME) untuk menyeimbangkan privasi pasien dan utilitas data. Arah penelitian selanjutnya mencakup eksplorasi mekanisme hybrid, integrasi DP dengan federated learning untuk kolaborasi antar-rumah sakit, serta validasi menggunakan dataset medis lokal Indonesia.

Daftar Rujukan

[1] W. K. Liu, Y. Zhang, H. Yang, and Q. Meng, "A Survey on Differential Privacy for Medical Data Analysis," 2024. doi: 10.1007/s40745-023-00475-3.

[2] A. Dyda *et al.*, "Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality," 2021. doi: 10.1016/j.patter.2021.100366.

[3] F. K. Dankar and K. El Emam, "Practicing differential privacy in health care: A review," 2013.

[4] J. F. A. Murphy, "The General Data Protection Regulation (GDPR)," 2018. doi: 10.26512/lstr.v13i2.37425.

[5] R. M. Caplan, "HIPAA. Health Insurance Portability and Accountability Act of 1996.," *Dent Assist*, vol. 72, no. 2, 2003.

[6] D. L. F. Salim, "AKSESIBILITAS PEMBIAYAAN KESEHATAN DALAM PROGRAM JAMINAN KESEHATAN NASIONAL," *LEX ET SOCIETATIS*, vol. 8, no. 4, 2020, doi: 10.35796/les.v8i4.30915.

[7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006. doi: 10.1007/11681878_14.

[8] D. Roy and S. Kumar Jena, "Determining t in t-closeness using Multiple Sensitive Attributes," *Int J Comput Appl*, vol. 70, no. 19, 2013, doi: 10.5120/12179-8291.

[9] A. El Ouadrhiri and A. Abdelhadi, "Differential Privacy for Deep and Federated Learning: A Survey," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3151670.

[10] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, 2013, doi: 10.1561/0400000042.

[11] Y. Wang, Q. Wang, L. Zhao, and C. Wang, "Differential privacy in deep learning: Privacy and beyond," 2023. doi: 10.1016/j.future.2023.06.010.

[12] J. Zhao, Y. Chen, and W. Zhang, "Differential Privacy Preservation in Deep Learning: Challenges, Opportunities and Solutions," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2909559.

[13] S. Zhang and X. Li, "Differential privacy medical data publishing method based on attribute correlation," *Sci Rep*, vol. 12, no. 1, 2022, doi: 10.1038/s41598-022-19544-3.

[14] L. A. Waller, "Global and local impacts of differential privacy on estimates of health care inequity," 2022. doi: 10.1111/1475-6773.14080.

[15] A. Ziller, D. Usynin, R. Braren, M. Makowski, D. Rueckert, and G. Kaissis, "Medical imaging deep learning with differential privacy," *Sci Rep*, vol. 11, no. 1, 2021, doi: 10.1038/s41598-021-93030-0.

[16] R. Subramanian, "Applications of Differential Privacy to Healthcare," *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4005908.

DOI: https://doi.org/10.38204/tematik.v12i2.2634