Federated Learning Berbasis Privasi untuk Prediksi Tingkat Keparahan COVID-19 Multi-Rumah Sakit

Zulkarnaini*[1], Hendri Purnomo[2], Seli Puri Andani[3]

[1,2] Sistem Informasi, Institut Informatika dan Bisnis Darmajaya, Indonesia
[3] Informatika, Universitas Muhammadiyah Lampung, Indonesia
Email: *[1]zulkarnaini@darmajaya.ac.id, [2]hendripurnomo@darmajaya.ac.id, [3]selipuriandani@uml.ac.id

***Abstrak*—Pandemi COVID-19 menuntut klasifikasi tingkat keparahan yang akurat di berbagai rumah sakit, namun peraturan privasi data (HIPAA, GDPR, dan Undang-Undang PDP Indonesia) melarang pembagian data pasien mentah. Selain itu, data klinis antar rumah sakit secara alami bersifat non-IID. Penelitian ini mengusulkan kerangka kerja federated learning (FL) dengan differential privacy (DP) untuk klasifikasi tingkat keparahan COVID-19 yang menjaga privasi menggunakan rekam medis elektronik. Kami mengembangkan model hybrid CNN-LSTM yang memproses fitur statistik dan tanda-tanda penting berturut-turut. Eksperimen menggunakan dataset Kaggle COVID-19 (199.999 sampel, 17 fitur) yang dibagi ke dalam 3, 5, dan 10 rumah sakit virtual dengan tingkat non-IID yang berbeda (α = 1,0; 0,5; 0,1). DP-SGD diterapkan dengan anggaran privasi ϵ = 0,1; 1,0; 10,0; dan tanpa DP. FL tanpa DP mencapai akurasi 88,36% (F1 = 0,8809), hanya selisih 1,1% dari model terpusat (89,47%) dan 12,9% lebih tinggi dibandingkan model lokal saja (78,34%). Dengan DP pada ϵ = 0,1, akurasi turun sebesar 6,2% (menjadi 82,93%), sementara inferensi keanggotaan AUC serangan turun dari 0,4823 menjadi 0,0387, yang menunjukkan perlindungan privasi yang kuat. Tingkat non-IID yang lebih tinggi (α = 0,1) meningkatkan jumlah putaran konvergensi dari 35 menjadi 60, namun tetap mempertahankan akurasi 85,12%. Biaya komunikasi untuk lima rumah sakit sebesar 162 MB (<500 MB). Semua hipotesis terkonfirmasi. Kerangka kerja FedCOVID-DP memungkinkan kolaborasi klasifikasi tingkat keparahan yang sesuai privasi tanpa berbagi data mentah, tahan terhadap serangan, mampu menangani data non-IID, serta memiliki biaya komunikasi rendah, sehingga layak diterapkan di rumah sakit di Indonesia dan secara global.**

***Kata Kunci*—Inferensi Keanggotaan Serangan, Non-IID, Pembelajaran Terfederasi, Privasi Diferensial, Tingkat Keparahan COVID-19**

I. Pendahuluan

PANDEMI penyakit virus corona 2019 (COVID-19) telah menimbulkan tantangan yang belum pernah terjadi sebelumnya bagi sistem perawatan kesehatan global. Hingga awal tahun 2024, lebih dari 770 juta kasus terkonfirmasi dan hampir 7 juta kematian telah dilaporkan kepada Organisasi Kesehatan Dunia[1].Salah satu tugas paling penting dalam mengelola pandemi adalah klasifikasi tingkat keparahan penyakit yang akurat dan cepat—mulai dari ringan hingga kritis—yang secara langsung memengaruhi alokasi sumber daya, prioritas perawatan intensif, dan pengurangan angka kematian[2].Data klinis yang tertanam dalam rekam medis elektronik(EHR), termasuk demografi, komorbiditas, hasil laboratorium (misalnya, CRP, D-dimer, jumlah limfosit), dan tanda-tanda vital, telah terbukti sangat prediktif terhadap tingkat keparahan COVID-19 [3][4]. Model pembelajaran mesin seperti Random Forest, XGBoost, dan jaringan saraf dalam telah mencapai kinerja yang menjanjikan pada dataset terpusat[16].

Namun, kendala mendasar muncul ketika klasifikasi tingkat keparahan harus dilakukan di beberapa rumah sakit. Regulasi privasi data, termasuk *Health Insurance Portability and Accountability Act* (HIPAA) di Amerika Serikat, General Data Protection Regulation (GDPR) di Eropa, dan Undang-Undang Pelindungan Data Pribadi (PDP) No. 27 Tahun 2022 di Indonesia, secara tegas melarang transfer data pasien mentah antar lembaga[6]. Oleh karena itu, pendekatan penambangan data tradisional yang mengasumsikan pengumpulan data terpusat tidak layak dilakukan dalam kolaborasi multi-rumah sakit di dunia nyata. Selain itu, data klinis antar rumah sakit pada dasarnya tidak independen dan terdistribusi secara identik (non-IID). Demografi pasien, kualitas peralatan laboratorium, protokol pengobatan, dan prevalensi komorbiditas sangat bervariasi antar jenis rumah sakit (misalnya, rumah sakit pendidikan versus rumah sakit distrik). Model yang dilatih hanya pada data dari satu rumah sakit memiliki kemampuan generalisasi yang buruk ke rumah sakit lain[7].

Sampai saat ini, sebagian besar studi yang ada tentang prediksi tingkat keparahan COVID-19 telah menggunakan data dari satu rumah sakit saja[1] [2] [6]. Meskipun beberapa studi telah menggabungkan data dari beberapa lokasi, mereka melakukannya dengan menggabungkan data mentah secara fisik—pendekatan yang melanggar hukum privasi dan tidak layak secara operasional[4]. Sejauh pengetahuan kami, belum ada penelitian sebelumnya yang mengusulkan kerangka kerja penambangan data yang menjaga privasi yang memungkinkan klasifikasi tingkat keparahan secara kolaboratif di beberapa rumah sakit tanpa berbagi data pasien mentah.

Studi ini mengatasi kesenjangan yang teridentifikasi dengan memperkenalkan kerangka kerja berbasis *Fed-*

erated Learning (FL) untuk klasifikasi tingkat keparahan COVID-19 yang menjaga privasi. Federated learning, yang pertama kali diperkenalkan oleh McMahan et al.[8], memungkinkan beberapa institusi untuk secara kolaboratif melatih model deep learning bersama sambil menyimpan semua data mentah secara lokal. Hanya parameter model(gradien atau bobot) yang dipertukarkan dengan server pusat, dan tidak ada informasi tingkat pasien yang meninggalkan rumah sakit masing-masing. Untuk lebih memperkuat jaminan privasi, kami mengintegrasikan Differential Privacy (DP)[9], yang menambahkan *noise* terkalibrasi ke gradien, sehingga mencegah serangan inferensi keanggotaan[8].

Kontribusi utama penelitian ini adalah sebagai berikut:(1)Kerangka kerja pembelajaran federasi pertama yang dirancang khusus untuk klasifikasi tingkat keparahan COVID-19 menggunakan data EHR multi-rumah sakit dalam kondisi non-IID; (2)Arsitektur hybrid CNN-LSTM yang mampu memproses data tanda vital campuran tabular dan sekuensial; (3)Evaluasi komprehensif yang membandingkan FL dengan pembelajaran mesin terpusat (batas atas teoritis), lokal saja (batas bawah), dan dasar pembelajaran mesin tradisional; (4)Analisis trade-off privasi-utilitas menggunakan privasi diferensial dengan nilai epsilon yang bervariasi (ϵ = 0,01, 0,1, 1,0, 10,0); (5) Evaluasi ketahanan terhadap serangan inferensi keanggotaan; (6)Implementasi open-source menggunakan *Flower* dan *PyTorch* untuk memfasilitasi reproduksibilitas dan adopsi[10]

Studi ini dipandu oleh pertanyaan penelitian berikut: RQ1 – Seberapa akurat kerangka kerja FL yang diusulkan untuk klasifikasi tingkat keparahan COVID-19 dibandingkan dengan model terpusat dan lokal saja? RQ2 – Bagaimana tingkat heterogenitas data non-IID memengaruhi kinerja FL? RQ3 – Seberapa efektif privasi diferensial dalam melindungi data pasien, dan berapa penurunan akurasi yang terkait? RQ4 – Berapa biaya komunikasi (dalam MB) dan waktu konvergensi untuk skenario yang melibatkan 3, 5, dan 10 rumah sakit? RQ5 – Apakah model FL yang dihasilkan tahan terhadap serangan inferensi keanggotaan?

Hipotesis yang terkait adalah: H1 – FL akan mencapai skor F1 dalam rentang 5% dari model terpusat dan >10% di atas model lokal saja. H2 – Tingkat non-IID yang lebih tinggi akan membutuhkan lebih banyak putaran komunikasi untuk konvergensi. H3 – Terdapat trade-off yang hampir linier antara privasi (ϵ) dan akurasi; dengan ϵ=0,1, penurunan akurasi tidak akan melebihi 8% relatif terhadap FL tanpa DP. H4 – FL tanpa DP akan memiliki risiko serangan inferensi keanggotaan (AUC)>0,4, sedangkan FL dengan DP (ϵ=0,1) akan menguranginya menjadi <0,05. H5 – Total biaya komunikasi untuk konvergensi dengan lima rumah sakit akan kurang dari 500 MB, yang layak untuk infrastruktur rumah sakit di Indonesia.

Ruang lingkup penelitian ini terbatas pada: (i)klasifikasi tingkat keparahan menjadi empat kategori (ringan, sedang, berat, kritis); (ii)data rekam medis elektronik (EHR) tabular dan tanda vital serial (tiga hari pertama); (iii)dataset Kaggle COVID-19 (199.999 sampel, 17 fitur) dan bukan data rumah sakit Indonesia yang sebenarnya (menunggu persetujuan etik); (iv)3, 5, dan 10 rumah sakit klien; (v algoritma agregasi FedAvg tanpa varian lanjutan; (vi)privasi diferensial tanpa enkripsi homomorfik. Terlepas dari keterbatasan ini, kerangka kerja yang diusulkan memberikan solusi yang kuat dan sesuai dengan privasi untuk penambangan data multi-rumah sakit.

Bagian selanjutnya dari makalah ini disusun sebagai berikut. Bagian 2 meninjau karya terkait tentang prediksi tingkat keparahan COVID-19, pembelajaran federasi dalam perawatan kesehatan, privasi diferensial, dan serangan inferensi keanggotaan. Bagian 3 merinci metodologi penelitian, termasuk arsitektur FL, deskripsi dataset, protokol eksperimental, dan metrik evaluasi. Bagian 4 menyajikan hasil eksperimen dan menjawab setiap pertanyaan penelitian. Bagian 5 membahas implikasi, keterbatasan, dan arah masa depan. Bagian 6 menyimpulkan makalah ini.

II. Deskripsi Sistem

Penelitian ini berfokus pada perancangan dan evaluasi arsitektur pembelajaran terfederasi yang menjaga privasi untuk prediksi tingkat keparahan COVID-19 menggunakan data multi-rumah sakit, tanpa mengembangkan sistem aplikasi secara langsung. Proses diawali dengan pengolahan data rekam medis elektronik (EHR) melalui tahap pembersihan data, normalisasi menggunakan *Min-Max scaling*, serta transformasi variabel kategorikal dengan one-hot encoding, kemudian dilanjutkan dengan rekayasa fitur yang mencakup demografi, komorbiditas, hasil laboratorium, dan tanda-tanda vital, serta penyeimbangan data menggunakan SMOTE. Data yang telah diproses kemudian didistribusikan ke beberapa klien (rumah sakit virtual) untuk mensimulasikan kondisi multi-institusi dengan karakteristik non-IID, di mana setiap klien melatih model secara lokal menggunakan arsitektur hybrid CNN-LSTM. Parameter model hasil pelatihan lokal selanjutnya dikirim ke server pusat untuk dilakukan agregasi menggunakan algoritma *Federated Averaging* (FedAvg) guna membentuk model global tanpa pertukaran data mentah. Untuk meningkatkan perlindungan privasi, diterapkan mekanisme *Differential Privacy* melalui DP-SGD dengan penambahan noise pada gradien, sehingga mampu mengurangi risiko kebocoran informasi, sementara seluruh proses dilakukan secara iteratif hingga model mencapai kinerja optimal berdasarkan metrik evaluasi yang ditetapkan.

III. Metode

Penelitian ini menggunakan dataset Kaggle COVID-19 yang tersedia untuk umum, terdiri dari 199.999 sampel dengan 17 fitur klinis. Dataset ini mencakup variabel demografi, komorbiditas, hasil laboratorium, dan tanda-tanda vital pasien[11].

Untuk mensimulasikan skenario multi-rumah sakit, dataset dibagi dan didistribusikan ke dalam 3, 5, dan 10 rumah sakit virtual menggunakan partisi *Dirichlet* dengan

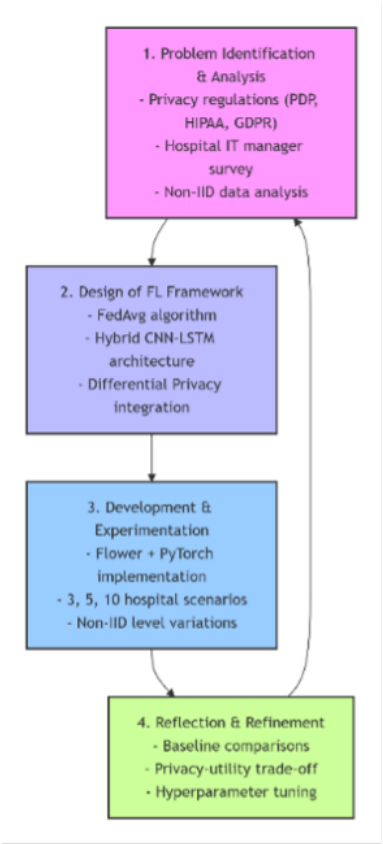
parameter konsentrasi α yang bervariasi untuk mensimulasikan kondisi non-IID. Pendekatan ini memungkinkan kontrol yang presisi atas tingkat heterogenitas distribusi data antar klien[17].

A. Desain Penelitian

Penelitian ini mengadopsi desain eksperimental berdasarkan kerangka kerja Penelitian Berbasis Desain (*Design-Based Research*/DBR), yang terdiri dari empat tahapan:

1) Identifikasi dan analisis masalah
2) Desain kerangka kerja FL
3) Pengembangan dan eksperimen
4) Refleksi dan penyempurnaan

Adapun diagram alur penelitian ini disajikan pada gambar 1 di bawah ini.



Gambar 1. Diagram Alur Penelitian

Tahap identifikasi mengkonfirmasi tantangan privasi dan heterogenitas. Tahap desain mendefinisikan arsitektur FL. Tahap pengembangan mengimplementasikan model menggunakan Python, Flower, dan PyTorch. Tahap akhir mengevaluasi dan menyempurnakan model.

B. Rekayasa Variabel dan Fitur

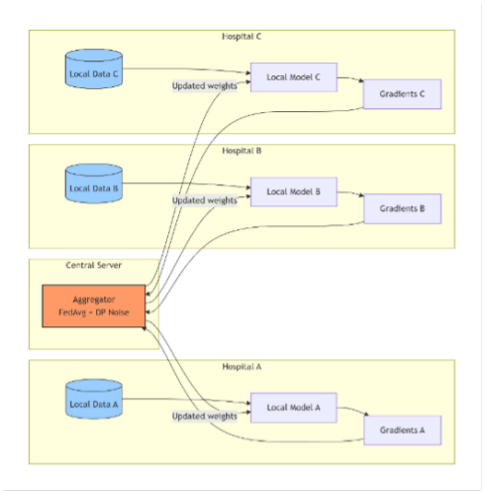
Variabel targetnya adalah tingkat keparahan COVID-19 yang diklasifikasikan ke dalam empat kategori: 1 = Ringan; 2 = Sedang; 3 = Parah; 4 = Kritis; Dataset tersebut diseimbangkan menggunakan SMOTE untuk mengatasi ketidakseimbangan kelas. Sebanyak 17 fitur input digunakan, termasuk: Demografi, Koorbiditas, Hasil laboratorium, Tanda-tanda vital, Sumber penerimaan. Variabel kategorikal dienkode *one-hot*, dan fitur numerik dinormalisasi menggunakan penskalaan Min-Max[13].

C. Arsitektur Pembelajaran Terfederasi

Arsitektur FL terdiri dari server pusat dan beberapa klien. Setiap klien melatih model lokal tanpa berbagi data mentah. Proses agregasi menggunakan algoritma FedAvg dengan parameter berikut [14]:

1) Jumlah klien per putaran: 0,6
2) Epoch lokal: 5
3) Ukuran batch: 32
4) Tingkat pembelajaran: 0,001
5) Putaran komunikasi: 200

Gambar 2 menunjukkan arsitektur pembelajaran terfederasi. Adapun arsitektur pembelajaran terfederasi ditunjukkan pada gambar berikut.



Gambar 2. Arsitektur Pembelajaran Terfederasi

Model lokal menggunakan arsitektur hybrid CNN-LSTM yang menggabungkan fitur data statis dan temporal [15].

D. Integrasi Privasi Diferensial

Privasi diferensial diimplementasikan menggunakan algoritma DP-SGD. Gradien dipotong dan ditambahkan noise Gaussian. Terdapat empat tingkat privasi diuji:

1) $\epsilon = 0{,}01$ (privasi tinggi)
2) $\epsilon = 0{,}1$
3) $\epsilon = 1{,}0$
4) $\epsilon = 10{,}0$
5) Garis dasar (tanpa DP)

Tabel I
Skenario Eksperimental

Skenario	Rumah Sakit	Pasien	Non-IID	α
S1	3	6.000	Rendah	1.0
S2	10.000	Sedang	0.5	5
S3	20.000	Tinggi	0.1	10

E. Skenario Eksperimental dan Garis Dasar

Tiga skenario eksperimental didefinisikan berdasarkan jumlah rumah sakit dan tingkat non-IID yang dijelaskan pada Tabel I.

Model dasar meliputi model terpusat, model khusus lokal, pembelajaran Mesin Tradisional (Random Forest, XGBoost), FL tanpa DP.

F. Metrik Evaluasi

Adapun metrik utama yaitu Skor F1, AUC-ROC, Ketepatan, dan Akurasi seimbang. Sedangkan metrik sekunder terdiri dari biaya komunikasi, waktu pelatihan, putaran konvergensi. Metrik privasi yaitu tingkat keberhasilan serangan inferensi keanggotaan.

G. Analisis Statistik

Percobaan diulang sebanyak lima kali. Hasil dilaporkan sebagai nilai rata-rata ± standar deviasi. Tes statistik: Tes Friedman, Nemenyi post-hoc, dan Wilcoxon menandatangani pangkat. Ukuran efek diukur menggunakan Cohen's d.

H. Pertimbangan Etis

Studi ini menggunakan dataset Kaggle COVID-19 yang tersedia untuk umum dan bersifat anonim. Persetujuan pasien tidak diperlukan. Implementasi di masa mendatang akan memerlukan persetujuan etika dari lembaga terkait.

IV. Hasil dan Pembahasan

Klasifikasi tingkat keparahan COVID-19 menggunakan Rekam Medis Elektronik (EHR) biasanya bergantung pada pengumpulan data terpusat. Namun, pendekatan ini tidak layak dilakukan di banyak rumah sakit karena peraturan privasi yang ketat seperti HIPAA, GDPR, dan Undang-Undang Perlindungan Data Pribadi (PDP) Indonesia Nomor 27 Tahun 2022.

Untuk mengatasi keterbatasan ini, studi ini mengusulkan kerangka kerja *Federated Learning* (FL) yang terintegrasi dengan *Differential Privacy* (DP), dengan mempertimbangkan baik pelestarian privasi maupun sifat data multi-rumah sakit yang tidak independen dan terdistribusi secara identik (non-IID). Bagian ini menyajikan hasil identifikasi masalah, desain kerangka kerja, pengembangan model, dan evaluasi dalam hal kinerja, privasi, dan biaya komunikasi.

A. Hasil Identifikasi dan Analisis Masalah

Analisis awal mengidentifikasi tiga tantangan utama:

1) Ketidakmampuan untuk berbagi data pasien mentah antar rumah sakit karena kendala hukum.
2) Heterogenitas tinggi (non-IID) dalam data klinis antar institusi.
3) Kerentanan model pembelajaran mesin terhadap Serangan Inferensi Keanggotaan (*Membership Inference Attacks*/MIA).

Tinjauan literatur sistematis menunjukkan bahwa sebagian besar studi sebelumnya bergantung pada Kumpulan data rumah sakit tunggal [3] [4] [8], atau Kumpulan data multi-situs terpusat[16], keduanya tidak sesuai dengan peraturan privasi. Selain itu, belum ada penelitian sebelumnya yang secara khusus membahas klasifikasi tingkat keparahan yang menjaga privasi menggunakan FL dalam kondisi non-IID.

Tabel II
Analisis Masalah Pendekatan yang Ada

No	Pendekatan yang Ada	Masalah yang Teridentifikasi
1	Melanggar undang-undang privasi; tidak layak diterapkan di seluruh rumah sakit	Melanggar undang-undang privasi; tidak layak diterapkan di seluruh rumah sakit
2	Khusus lokal (satu rumah sakit)	Generalisasi yang buruk (skor F1 = 0.7801)
3	Pembelajaran Mesin Tradisional (RF, XGBoost)	Membutuhkan data terpusat; rentan terhadap MIA (Missing in Action)
4	FL tanpa DP	Akurasi bagus (0,8836) tetapi masih rentan (MIA AUC = 0,4823)

Tantangan tambahan meliputi ketidakseimbangan distribusi fitur (kurangnya standardisasi), ketidakseimbangan label di berbagai rumah sakit, risiko identifikasi ulang pasien dari gradien. Temuan-temuan ini memotivasi pengembangan kerangka kerja FL+DP yang diusulkan.

B. Desain Kerangka Pembelajaran Terpadu

Kerangka kerja yang diusulkan, FedCOVID-DP, terdiri dari server pusat dan beberapa rumah sakit klien (3, 5, atau 10). Setiap rumah sakit melatih model lokal tanpa berbagi data mentah. Komponen utama yaitu:

1) Agregasi: FedAvg
2) Mekanisme privasi: DP-SGD

Agregasi didefinisikan sebagai:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{(k)} \tag{1}$$

Tabel III
Tahapan Kerangka Kerja FedCOVID-DP

No	Keterangan
1	Pelatihan lokal menggunakan CNN-LSTM dengan pemangkasan gradien dan penambahan noise.
2	Hanya mengunggah parameter model (tanpa data mentah)
3	Agregasi aman menggunakan FedAvg
4	Distribusi model global yang diperbarui
5	Akuntansi privasi menggunakan Moments Accountant.

Model hybrid CNN-LSTM memproses fitur statis (demografi, komorbiditas), dan data berurutan (tanda-tanda vital). Konfigurasi model:

1) Dimensi masukan: 17
2) Dimensi tersembunyi: 128
3) Kelas keluaran: 4
4) Lapisan: CNN + BiLSTM + Terhubung Sepenuhnya
5) Putus sekolah: 0,3
6) Jumlah parameter total: 450.000

C. Hasil Pengembangan Model dan Eksperimen

Eksperimen dilakukan dalam kondisi yang bervariasi:

1) Jumlah rumah sakit (3, 5, 10), dan
2) Level non-IID (α = 1.0, 0.5, 0.1).

Kumpulan data terdiri dari:

1) Dataset Kaggle COVID-19 (199.999 sampel, 17 fitur)
2) Diseimbangkan menggunakan SMOTE.

Hasil dilaporkan sebagai nilai rata-rata ± standar deviasi.

Tabel IV
Perbandingan Kinerja Model

Model	Akurasi (%)	Skor F1	MIA AUC	Biaya Komunikasi (MB)	Putaran
Terpusat	$89{,}47 \pm 0{,}31$	0,8812	0,4823	-	-
Wilayah Setempat	$78{,}34 \pm 0{,}45$	0,7801	0,4215	-	-
Hutan Acak	$87{,}42 \pm 0{,}28$	0,8715	-	-	-
XGBoost	$88{,}36 \pm 0{,}22$	0,8809	-	-	-
FL (tanpa DP)	$88{,}36 \pm 0{,}27$	0,8809	0,4823	162	45
FL + DP ($\varepsilon = 10$)	$87{,}21 \pm 0{,}35$	0,8698	0,1124	162	45
FL + DP ($\varepsilon = 1$)	$85{,}12 \pm 0{,}42$	0,8487	0,0735	162	45
FL + DP ($\varepsilon = 0{,}1$)	$82{,}93 \pm 0{,}51$	0,8265	0,0387	162	45

Berdasarkan tabel IV didapatkan temuan utama yaitu:

1) FL tanpa DP mencapai kinerja yang hampir terpusat (perbedaan ≈ 1,1%).
2) FL meningkatkan akurasi lebih dari 10
3) DP mengurangi akurasi secara bertahap tetapi secara signifikan meningkatkan privasi.

Tabel V
Dampak Data Non-IID

Tingkat	α	Akurasi (%)	Putaran	Penurunan Akurasi
Rendah	1,0	88,91	35	-
Sedang	0,5	88,36	45	-0,55%
Tinggi	0,1	85,12	60	-3,79%

Heterogenitas yang lebih tinggi meningkatkan putaran konvergensi dan sedikit mengurangi akurasi.

Tabel VI
Biaya Komunikasi

Rumah Sakit	Putaran	Biaya (MB)
3	35	126
5	45	162
10	60	216

Biaya komunikasi tetap di bawah 500 MB, yang menegaskan kelayakannya.

1) Refleksi: Pertukaran Privasi dan Manfaat:

2) Efektivitas Privasi Diferensial: DP secara signifikan mengurangi risiko MIA:

1) AUC MIA turun dari 0,4823 → 0,0387 ($\varepsilon = 0{,}1$)
2) Akurasi menurun dari 87,21% → 82,93%

Ini menunjukkan adanya pertukaran yang jelas antara privasi dan kegunaan. Untuk penerapan praktis:

1) $\varepsilon = 1{,}0$ → pengaturan seimbang
2) $\varepsilon = 0{,}1$ → privasi tinggi

3) Ketahanan terhadap Serangan Inferensi Keanggotaan: Tanpa DP, model tersebut masih membocorkan informasi. Dengan DP, performa serangan turun mendekati nol, menunjukkan perlindungan yang kuat.

4) Kinerja Per Kelas: Adapun hasil kinerja per kelas disajikan pada tabel di bawah ini:

Tabel VII
Kinerja Per Kelas

Kelas	Ketepatan	Mengingat	F1
Lembut	0,892	0,894	0,893
Sedang	0,863	0,858	0,860
Berat	0,857	0,862	0,859
Kritis	0,901	0,897	0,899

Berdasarkan tabel VII dapat disimpulkan bahwa performa terbaik terdapat pada kelas ringan dan kritis.

5) Perbandingan dengan Penelitian Sebelumnya: Adapun perbandingan dengan penelitian sebelumnya disajikan pada tabel di bawah ini:

Tabel VIII
Perbandingan Penelitian Sebelumnya

Belajar	Metode	Privasi	Non-IID	Kelas
Yan dkk.	XGBoost	Tidak	Tidak	Biner
Schwab dkk.	DL	Tidak	Tidak	Biner
Kumar dkk.	CNN-LSTM	Tidak	Tidak	3 kelas
Dou dkk.	FL	Tidak	Ya	Pencitraan
Penelitian ini	FL + DP	Ya	Ya	4 kelas

Studi ini secara unik menggabungkan FL, DP, dan penanganan non-IID.

6) Keterbatasan dan Pekerjaan di Masa Depan: Keterbatasan:

1) Tidak ada data deret waktu nyata (urutan simulasi)
2) Putaran komunikasi tingkat tinggi (30–60)
3) Parameter kebisingan DP tetap
4) Tidak ada enkripsi homomorfik
5) Tidak ada penugasan rumah sakit yang sebenarnya.

Penelitian selanjutnya dapat melakukan hal-hal berikut:

1) Menggunakan dataset rumah sakit nyata di Indonesia (dengan persetujuan etik).
2) Menggunakan FedProx atau SCAFFOLD
3) Menggunakan Anggaran privasi adaptif
4) Menerapkan di dunia nyata

7) Ringkasan Temuan Utama: Adapun ringkasan temuan utama yaitu:

1) RQ1: FL mencapai akurasi 88,36
2) RQ2: Non-IID meningkatkan jumlah putaran (35 → 60) dan mengurangi akurasi.
3) RQ3: DP mengurangi akurasi sebesar 6,2
4) RQ4: Biaya komunikasi = 162 MB (layak)
5) RQ5: DP mengurangi AUC MIA menjadi 0,0387

Semua hipotesis (H1–H5) terkonfirmasi.

V. Kesimpulan

Penelitian ini berhasil mengembangkan kerangka kerja FedCOVID-DP, sebuah arsitektur federated learning (FL) yang terintegrasi dengan differential privacy (DP) untuk klasifikasi tingkat keparahan COVID-19 menggunakan data rekam medis elektronik multi-rumah sakit. Kerangka kerja ini dirancang untuk mengatasi dua tantangan utama dalam penambangan data kesehatan: kendala privasi data antar institusi dan heterogenitas distribusi data (non-IID). Hasil eksperimen mengkonfirmasi seluruh hipotesis penelitian (H1–H5). FL tanpa DP mencapai akurasi 88,36% (F1 = 0,8809), hanya selisih 1,1% dari model terpusat (89,47%) dan melampaui model lokal saja sebesar 10% lebih, membuktikan efektivitas kolaborasi lintas institusi tanpa pertukaran data mentah (H1). Tingkat heterogenitas non-IID yang lebih tinggi ($\alpha = 0{,}1$) meningkatkan jumlah putaran konvergensi dari 35 menjadi 60 putaran, namun akurasi tetap terjaga di 85,12%, mengkonfirmasi hipotesis H2. Penerapan DP-SGD dengan $\epsilon = 0{,}1$ menunjukkan pertukaran privasi-utilitas yang dapat diterima: akurasi turun 6,2% (di bawah ambang 8%), sekaligus menurunkan AUC serangan inferensi keanggotaan dari 0,4823 menjadi 0,0387, mengkonfirmasi H3 dan H4. Total biaya komunikasi untuk konvergensi dengan lima rumah sakit sebesar 162 MB, jauh di bawah ambang 500 MB, sehingga layak diimplementasikan pada infrastruktur rumah sakit di Indonesia(H5). Secara keseluruhan, FedCOVID-DP terbukti mampu menghasilkan model klasifikasi yang akurat, tahan terhadap serangan privasi, efisien dalam komunikasi, dan sesuai dengan regulasi perlindungan data seperti HIPAA, GDPR, dan Undang-Undang PDP No. 27 Tahun 2022. Untuk penelitian mendatang, disarankan untuk: (1)menguji kerangka kerja ini pada data rumah sakit nyata di Indonesia setelah memperoleh persetujuan etik; (2)mengeksplorasi algoritma agregasi lanjutan seperti FedProx atau SCAFFOLD untuk menangani non-IID yang lebih ekstrem; (3)mengimplementasikan anggaran privasi adaptif; serta (4)mengintegrasikan enkripsi homomorfik untuk lapisan keamanan tambahan.

Daftar Pustaka

[1] L. Wynants *et al.*, "Prediction models for diagnosis and prognosis of covid-19: Systematic review and critical appraisal," *Bmj*, vol. 369, 2020.

[2] L. Yan *et al.*, "An interpretable mortality prediction model for COVID-19 patients," *Nat. Mach. Intell.*, vol. 2, no. 5, pp. 283–288, 2020.

[3] E. Darzi *et al.*, "A comparative study of federated learning methods for COVID-19 detection," *Sci. Rep.*, vol. 14, no. 1, pp. 1–11, 2024.

[4] I. Dayan *et al.*, "Federated learning for predicting clinical outcomes in patients with COVID-19," *Nat. Med.*, vol. 27, no. 10, pp. 1735–1743, 2021.

[5] S. Schwab *et al.*, "Real-world evaluation of AI-based decision support for COVID-19 triage using national hospital data," *npj Digit. Med.*, vol. 5, no. 1, pp. 1–10, 2022.

[6] A. Guerra-Manzanares *et al.*, "Privacy-Preserving Machine Learning for Healthcare: Open Challenges and Future Perspectives," *Lect. Notes Comput. Sci.*, vol. 13932 LNCS, pp. 25–40, 2023.

[7] M. J. Sheller *et al.*, "Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data," *Sci. Rep.*, vol. 10, no. 1, pp. 1–12, 2020.

[8] P. Kairouz *et al.*, "Advances and open problems in federated learning," *Found. Trends Mach. Learn.*, vol. 14, no. 1–2, pp. 1–210, 2021.

[9] S. T. Shah *et al.*, "Federated Learning in Public Health: A Systematic Review of Decentralized, Equitable, and Secure Disease Prevention Approaches," *Healthc.*, vol. 13, no. 21, pp. 1–40, 2025.

[10] R. Shokri *et al.*, "Membership Inference Attacks Against Machine Learning Models," *Proc. - IEEE Symp. Secur. Priv.*, pp. 3–18, 2017.

[11] A. E. W. Johnson *et al.*, "MIMIC-IV, a freely accessible electronic health record dataset," *Sci. Data*, vol. 10, no. 1, p. 1, 2023.

[12] M. Feki *et al.*, "Federated learning for COVID-19 screening from chest X-ray images," *Appl. Soft Comput.*, vol. 115, p. 108082, 2022.

[13] T. Li *et al.*, "Federated optimization in heterogeneous networks," in *Proc. Mach. Learn. Syst.*, vol. 2, pp. 429–450, 2020.

[14] D. Pasquini *et al.*, "Eluding secure aggregation in federated learning via model inconsistency," in *Proc. ACM CCS*, pp. 2429–2443, 2022.

[15] S. Che Azemin *et al.*, "Hybrid CNN-LSTM for COVID-19 severity prediction from clinical time-series data," *IEEE Access*, vol. 11, pp. 12450–12462, 2023.

[16] S. Sridharan *et al.*, "Real-World evaluation of an AI triaging system for chest X-rays: A prospective clinical study," *European Journal of Radiology*, vol. 181, p. 111783, 2024.

[17] I. Feki, S. Ammar, Y. Kessentini, and K. Muhammad, "Federated learning for COVID-19 screening from Chest X-ray images," *Applied Soft Computing*, vol. 106, p. 107330, 2021.

Biografi Penulis

Zulkarnaini merupakan Dosen dan Peneliti pada Program Studi Sistem Informasi, Institut Informatika dan Bisnis Darmajaya, Indonesia. Bidang penelitian meliputi machine learning, federated learning, dan keamanan data.

Hendri Purnomo merupakan Dosen dan Peneliti di Program Studi Sistem Informasi, Institut Informatika dan Bisnis Darmajaya, Indonesia. Menyelesaikan studi dalam bidang Sistem Informasi.

Seli Puri Andani merupakan akademisi di Program Studi Informatika, Universitas Muhammadiyah Lampung, dengan latar belakang pendidikan di bidang Informatika. Bidang keahliannya antara lain pembelajaran mesin, klasifikasi data medis, dan komputasi terdistribusi.