

DAFTAR ISI

HALAMAN PERSEMBAHAN	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR TABEL	viii
DAFTAR KODE	ix
DAFTAR GAMBAR	x
DAFTAR SINGKATAN.....	xi
INTISARI.....	xii
ABSTRACT	xiii
BAB I Pendahuluan	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	4
1.4 Batasan dan Limitasi Penelitian	4
1.4.1 Variabel Penelitian	4
1.4.2 Perumusan Hipotesis.....	4
1.4.3 Batasan Penelitian.....	5
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan.....	6
BAB II Tinjauan Pustaka dan Dasar Teori	7
2.1 Tinjauan Pustaka	7
2.2 Analisis Perbandingan Metode	9
2.2.1 Perbandingan Metode <i>Machine Learning</i>	10
2.2.2 Perbandingan Library <i>Machine Learning</i>	10
2.2.3 Perbandingan Metode <i>Federated Learning</i>	11
2.2.4 Perbandingan Library <i>Federated Learning</i>	12
2.2.5 Perbandingan Metode <i>Differential Privacy</i>	12
2.3 Dasar Teori	13
2.3.1 <i>Credit Card Fraud Activity</i>	13
2.3.2 <i>Federated Learning</i>	14
2.3.2.1 Federated Averaging (FedAvg)	15
2.3.2.2 Differentially Private Federated Averaging (DP-FedAvg)	16
2.3.2.3 Rounds of Communication.....	18
2.3.2.4 Number of Clients	19
2.3.3 <i>Differential Privacy</i>	20
2.3.3.1 Gaussian Mechanism	21

2.3.4	Clipping	22
2.3.4.1	Client-Side Clipping	22
2.3.4.2	Server-Side Clipping	23
2.3.5	<i>Machine Learning</i>	24
2.3.5.1	Convolutional Neural Network (CNN)	25
2.3.6	Data Balancing	26
2.3.6.1	Random Over-Sampling (ROS)	26
2.3.7	Library & Bahasa Pemrograman	27
2.3.7.1	Python	27
2.3.7.2	Flower	27
2.3.7.3	Tensorflow	28
2.3.7.4	Keras	28
2.3.7.5	Pandas	28
2.3.7.6	Numpy	29
2.3.7.7	Sklearn	29
2.3.7.8	Matplotlib	29
2.3.8	Evaluation Metrics	29
2.3.8.1	Accuracy	30
2.3.8.2	Area Under the ROC Curve (AUC)	30
2.3.8.3	DP Noise Standard Deviation	30
2.3.8.4	Clipping Norm	30
2.3.8.5	Privacy Budget	31
2.3.9	Dasar Teori Uji Hipotesis Statistik	31
2.3.9.1	One-Way Analysis of Variance (ANOVA)	31
2.3.9.2	Welch <i>t</i> -Test	32
2.3.9.3	Shapiro–Wilk Test (Uji Normalitas)	32
2.3.9.4	Levene Test (Uji Homogenitas Varians)	32
2.3.9.5	Analysis of Covariance (ANCOVA)	33
BAB III Metode Penelitian		34
3.1	Alat dan Bahan Tugas Akhir	34
3.1.1	Alat Tugas Akhir	34
3.1.2	Bahan Tugas Akhir	34
3.2	Metode Penelitian	35
3.2.1	Metode Pengembangan Algoritma Machine Learning	35
3.2.2	Metode Pengembangan Algoritma Federated Learning	36
3.2.3	Metode Pengembangan Algoritma Differential Privacy	37
3.3	Alur Tugas Akhir	37
3.3.1	Studi Literatur	38
3.3.2	Penentuan Dataset Credit Card	39

3.3.3	Penentuan Metode & Algoritma Federated Learning	42
3.3.4	Penentuan Metode Evaluasi	43
3.3.5	Pengembangan Dummy Stakeholder Berbasis Client & Server	44
3.3.5.1	Pra-proses Data	46
3.3.6	<i>Machine Learning</i> Model.....	47
3.3.7	Pengembangan Algoritma <i>Splitting</i> Antar <i>Client</i>	48
3.3.8	Pengembangan Algoritma Federated Learning berbasis DP	49
3.3.8.1	Algoritma Federated Learning DP — <i>Server-side Adaptive Clipping</i>	49
3.3.8.2	Algoritma Federated Learning DP— <i>Server-side Fixed Clipping</i>	51
3.3.8.3	Algoritma Federated Learning DP— <i>Client-side Adaptive Clipping</i>	52
3.3.8.4	Algoritma Federated Learning DP— <i>Client-side Fixed Clipping</i>	52
3.3.9	Tahap Evaluasi	54
3.3.9.1	Evaluasi Differential Privacy Model	54
3.3.9.2	Evaluasi Performa Model	55
3.3.9.3	Agregasi dan Penyimpanan Metrik	56
3.3.10	Alur Operasional Uji Hipotesis.....	56
BAB IV	Hasil dan Pembahasan.....	58
4.1	Hasil Metriks Prediksi dengan DP-Federated Learning.....	58
4.2	Hasil Metrik Privasi dengan DP-Federated Learning	62
4.2.1	<i>Privacy–Utility Trade-off</i>	65
4.3	Hasil Uji Hipotesis Statistik	67
4.3.1	Persiapan & Statistik Deskriptif	67
4.3.2	Uji Asumsi Parametrik.....	68
4.3.3	H_1 – “Adaptive” vs. “Fixed”	68
4.3.4	H_2 – Kemiringan AUC vs. Privacy-Budget	69
BAB V	Kesimpulan dan Saran.....	71
5.1	Kesimpulan.....	71
5.2	Saran.....	72
DAFTAR PUSTAKA		73
LAMPIRAN		L-1
L.1	<i>Source Code</i>	L-1
L.1.1	<i>Source Code Differential Privacy Server & Client Side Adaptive Clipping</i>	L-1
L.1.2	<i>Source Code Differential Privacy Server & Client Side Fixed Clipping</i>	L-9



UNIVERSITAS
GADJAH MADA

Analisis Komparatif Differential Privacy Pada Federated Learning Melalui Metode Server & Client Clipping Untuk Deteksi Penipuan Kartu Kredit

Bintang Restu Bawono, Dr. Ir. Guntur Dharma Putra, S.T., M.Sc ; Dr.Eng. Ir. Sunu Wibirama, S.T., M.Eng., IPM.

Universitas Gadjah Mada, 2025 | Diunduh dari <http://etd.repository.ugm.ac.id/>

L.1.3	<i>Source Code Differential Privacy Server Side Fixed Clipping</i>	L-16
L.1.4	<i>Github Repository</i>	L-25
L.2	<i>Proof-of-concept Proses Training Federated Learning</i>	L-25