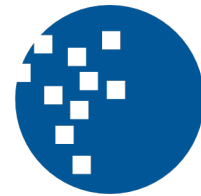


**IMPLEMENTASI SEGMENTED CKKS HOMOMORPHIC
ENCRYPTION PADA FEDERATED LEARNING DENGAN
MODEL RESNET22 UNTUK KLASIFIKASI KANKER
PAYUDARA**



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

SKRIPSI

CHYNTIA IRAWAN
00000067992

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2026

**IMPLEMENTASI SEGMENTED CKKS HOMOMORPHIC
ENCRYPTION PADA FEDERATED LEARNING DENGAN
MODEL RESNET22 UNTUK KLASIFIKASI KANKER
PAYUDARA**



SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh
Gelar Sarjana Komputer (S.Kom.)

**CHYNTIA IRAWAN
00000067992**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2026**

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Chyntia Irawan
Nomor Induk Mahasiswa : 00000067992
Program Studi : Informatika

Skripsi dengan judul:

Implementasi Segmented CKKS Homomorphic Encryption pada Federated Learning dengan Model ResNet22 untuk Klasifikasi Kanker Payudara

merupakan hasil karya saya sendiri bukan plagiat dari laporan karya tulis ilmiah yang ditulis oleh orang lain, dan semua sumber, baik yang dikutip maupun dirujuk, telah saya nyatakan dengan benar serta dicantumkan di Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan maupun dalam penulisan laporan karya tulis ilmiah, saya bersedia menerima konsekuensi dinyatakan TIDAK LULUS untuk mata kuliah yang telah saya tempuh.

Tangerang, 8 Januari 2026



(Chyntia Irawan)

UMM
UNIVERSITAS
MULTIMEDIA
NUSANTARA

HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Chyntia Irawan
NIM : 00000067992
Program Studi : Informatika
Judul Laporan : Implementasi Segmented CKKS Homomorphic Encryption pada Federated Learning dengan Model ResNet22 untuk Klasifikasi Kanker Payudara

Dengan ini saya menyatakan secara jujur menggunakan bantuan Kecerdasan Artifisial (AI) dalam pengerjaan Laporan sebagai berikut:

- ☐ Menggunakan AI sebagaimana diizinkan untuk membantu dalam menghasilkan ide-ide utama saja.
- ☐ Menggunakan AI sebagaimana diizinkan untuk membantu menghasilkan teks pertama saja.
- ☒ Menggunakan AI untuk menyempurnakan sintaksis dan tata bahasa untuk pengumpulan tugas.
- ☐ Karena tidak diizinkan: Tidak menggunakan bantuan AI dengan cara apa pun dalam pembuatan tugas

Saya juga menyatakan bahwa:

- (1) Menyerahkan secara lengkap dan jujur penggunaan perangkat AI yang diperlukan dalam tugas melalui Formulir Penggunaan Perangkat Kecerdasan Artifisial (AI).
- (2) Mengakui telah menggunakan bantuan AI dalam tugas saya baik dalam bentuk kata, parafrase, penyertaan ide, atau fakta penting yang disarankan oleh AI dan telah dicantumkan dalam sitasi serta referensi.
- (3) Terlepas dari pernyataan di atas, tugas ini sepenuhnya merupakan karya saya sendiri.

Tangerang, 8 Januari 2026



(Chyntia Irawan)

HALAMAN PENGESAHAN

Skripsi dengan judul

IMPLEMENTASI SEGMENTED CKKS HOMOMORPHIC ENCRYPTION PADA FEDERATED LEARNING DENGAN MODEL RESNET22 UNTUK KLASIFIKASI KANKER PAYUDARA

oleh

Nama : Chyntia Irawan
NIM : 00000067992
Program Studi : Informatika
Fakultas : Fakultas Teknik dan Informatika

Telah diujikan pada hari Selasa, 13 Januari 2026

Pukul 08.00 s/s 10.00 dan dinyatakan

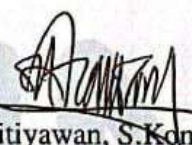
LULUS

Dengan susunan penguji sebagai berikut

Ketua Sidang


(Januar Wahjudi, S.Kom., M.Sc.)
NIDN: 0330017201

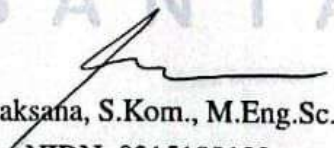
Penguji


(Aditiyawan, S.Komp., M.Si.)
NIDN: 08994550022

Pembimbing


(Arya Wicaksana, S.Kom., M.Eng.Sc., OCA)
NIDN: 0315109103

Ketua Program Studi Informatika,


(Arya Wicaksana, S.Kom., M.Eng.Sc., OCA)
NIDN: 0315109103

HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini:

Nama : Chyntia Irawan
NIM : 00000067992
Program Studi : Informatika
Jenjang : S1
Judul Karya Ilmiah : Implementasi Segmented CKKS
Homomorphic Encryption pada
Federated Learning dengan Model
ResNet22 untuk Klasifikasi Kanker
Payudara

Menyatakan dengan sesungguhnya bahwa saya bersedia (**pilih salah satu**):

- ☒ Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya ke dalam repositori Knowledge Center sehingga dapat diakses oleh Sivitas Akademika UMN/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial.
- ☐ Saya tidak bersedia mempublikasikan hasil karya ilmiah ini ke dalam repositori Knowledge Center, dikarenakan: dalam proses pengajuan publikasi ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*) **.
- ☐ Lainnya, pilih salah satu:
 - Hanya dapat diakses secara internal Universitas Multimedia Nusantara
 - Embargo publikasi karya ilmiah dalam kurun waktu tiga tahun.

Tangerang, 8 Januari 2026

Yang menyatakan

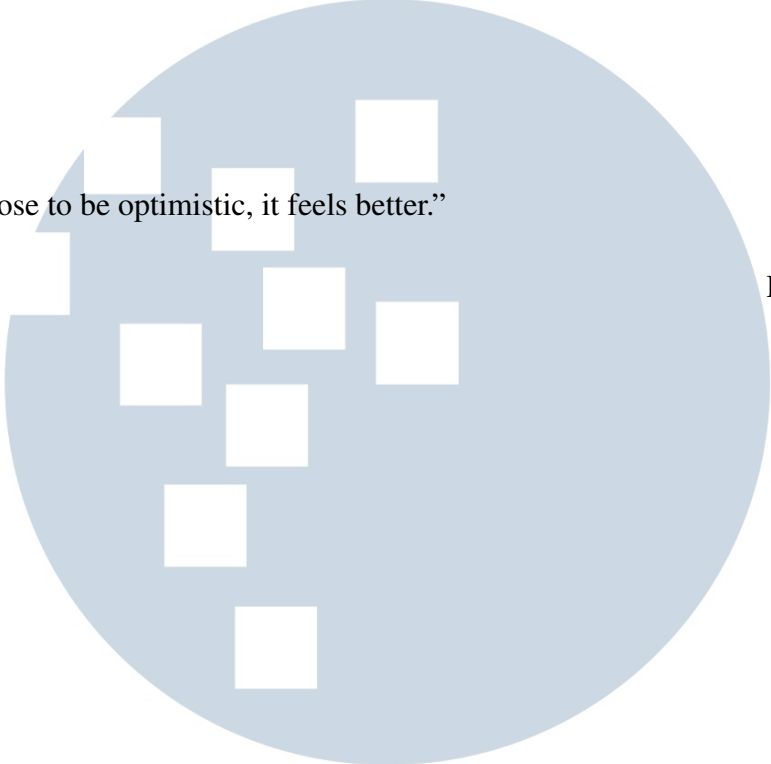


Chyntia Irawan

HALAMAN PERSEMBAHAN / MOTTO

"Choose to be optimistic, it feels better."

Dali Lama



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga Tugas Akhir berjudul "Implementasi Segmented CKKS Homomorphic Encryption pada Federated Learning dengan Model ResNet22 untuk Klasifikasi Kanker Payudara" dapat terselesaikan dengan baik. Tugas Akhir ini disusun sebagai salah satu syarat kelulusan Program Sarjana Informatika Universitas Multimedia Nusantara. Terima kasih kepada semua pihak yang telah memberikan dukungan dan bantuan selama proses penyusunan. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Arya Wicaksana, S.Kom., M.Eng.Sc., OCA, sebagai Pembimbing pertama yang telah memberikan bimbingan, arahan, dan motivasi atas terselesainya tugas akhir ini.
5. Keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga dapat menyelesaikan tugas akhir ini.
6. Teman-teman yang senantiasa memberikan dukungan, semangat, serta bantuan baik secara langsung maupun tidak langsung.

Semoga karya ilmiah ini dapat memberikan manfaat dan menjadi tambahan pengetahuan. Karya ilmiah ini disadari masih memiliki kekurangan, oleh karena itu saran dan kritik yang membangun sangat diharapkan demi penyempurnaan di masa mendatang.

Tangerang, 8 Januari 2026



Chyntia Irawan

IMPLEMENTASI SEGMENTED CKKS HOMOMORPHIC ENCRYPTION PADA FEDERATED LEARNING DENGAN MODEL RESNET22 UNTUK KLASIFIKASI KANKER PAYUDARA

Chyntia Irawan

ABSTRAK

Kanker payudara merupakan salah satu penyebab utama kematian pada perempuan, sehingga deteksi dini yang akurat sangat diperlukan. Namun, pemanfaatan data medis terdistribusi menghadapi tantangan privasi, sehingga Federated Learning (FL) digunakan untuk memungkinkan pelatihan model tanpa berbagi data mentah. Meskipun demikian, pertukaran parameter model dalam FL tetap berpotensi menimbulkan kebocoran informasi, sehingga penelitian ini menerapkan Segmented CKKS Homomorphic Encryption pada sistem Federated Learning dengan model ResNet22 menggunakan dataset CBIS-DDSM. Evaluasi performa dilakukan menggunakan metrik AUC dan PR-AUC pada berbagai konfigurasi tingkat keamanan dan panjang kunci. Hasil terbaik pada skenario terenkripsi diperoleh pada konfigurasi 192-bit dengan key size 8192, dengan nilai AUC sebesar 0,8545 dan PR-AUC sebesar 0,8136, yang menunjukkan penurunan performa yang relatif kecil dibandingkan model tanpa enkripsi. Hasil ini menunjukkan bahwa Segmented CKKS mampu meningkatkan perlindungan privasi dalam Federated Learning tanpa mengorbankan performa model secara signifikan.

Kata kunci: Federated Learning, Homomorphic Encryption, Kanker Payudara, ResNet22, Segmented CKKS

U M N
U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

**IMPLEMENTATION OF SEGMENTED CKKS HOMOMORPHIC
ENCRYPTION ON FEDERATED LEARNING WITH RESNET22 MODEL
FOR BREAST CANCER CLASSIFICATION**

Chyntia Irawan

ABSTRACT

Breast cancer is one of the leading causes of death among women, making accurate early detection essential. However, the use of distributed medical data raises privacy concerns, motivating the adoption of Federated Learning (FL) to enable collaborative model training without sharing raw data. Despite this, model parameter exchange in FL still poses potential privacy risks, which this study addresses by implementing Segmented CKKS Homomorphic Encryption in a Federated Learning framework using the ResNet22 model on the CBIS-DDSM dataset. Model performance is evaluated using AUC and PR-AUC across different security levels and key sizes. The best encrypted configuration is achieved at 192-bit security with a key size of 8192, yielding an AUC of 0.8545 and a PR-AUC of 0.8136, indicating only a slight performance degradation compared to the non-encrypted model. These results demonstrate that Segmented CKKS effectively enhances privacy protection while maintaining competitive model performance.

Keywords: Breast Cancer, Federated Learning, Homomorphic Encryption, ResNet22, Segmented CKKS



DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT	ii
HALAMAN PERNYATAAN PENGGUNAAN BANTUAN KECERDASAN ARTIFISIAL (AI)	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH	v
HALAMAN PERSEMBAHAN/MOTO	vi
KATA PENGANTAR	vii
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR KODE	xiv
DAFTAR RUMUS	xv
DAFTAR LAMPIRAN	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Permasalahan	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB 2 LANDASAN TEORI	6
2.1 Klasifikasi Kanker Payudara	6
2.2 Resnet22 CNN	7
2.2.1 Encoder ResNet22	10
2.2.2 Classifier	12
2.3 Federated Learning	13
2.3.1 Federated Learning Berdasarkan Partisi Data	16
2.3.2 Federated Average	17
2.3.3 Curriculum Learning	18
2.3.4 Adversarial Alignment	19
2.4 Segmented CKKS Homomorphic Encryption	21
2.4.1 CKKS Key Generation	25
2.4.2 Segmented Encryption	28
2.4.3 Segmented Decryption	30
2.5 Evaluasi Performa dan Privasi	32
2.5.1 Evaluasi Accuracy, AUC, dan PR-AUC	32
2.5.2 Evaluasi Waktu Komputasi dan Communication Cost	33
BAB 3 METODOLOGI PENELITIAN	35
3.1 Studi Literatur	35
3.2 Arsitektur Model	35
3.2.1 Spesifikasi Perangkat	35
3.2.2 Komponen Utama Model	36
3.2.3 Threat Model	36
3.3 Dataset dan Preprocessing Data	37
3.3.1 Dataset CBIS-DDSM	37

3.3.2	Data Collecting	38
3.3.3	Data Cleaning	39
3.3.4	Data Splitting	40
3.3.5	Image Preprocessing	41
3.4	Perancangan Model	42
3.4.1	Model Federated Learning dengan Segmented CKKS HE . .	42
3.4.2	Perancangan Arsitektur Model	44
3.4.3	Encoder dan Classifier	45
3.4.4	Curriculum Learning Berbasis Kesulitan Sampel	45
3.4.5	Adversarial Domain Alignment	47
3.4.6	Federated Learning Setup	47
3.4.7	Parameter Homomorphic Encryption (HE)	48
3.5	Implementasi Model	50
3.5.1	Inisialisasi Model dan CKKS	50
3.5.2	Pelatihan Lokal pada Setiap Klien	52
3.5.3	Enkripsi Parameter dengan Skema Segmented CKKS	53
3.5.4	Agregasi Parameter Terenkripsi di Server	54
3.5.5	Dekripsi dan Rekonstruksi Parameter Global	54
3.5.6	Evaluasi Model dan Early Stopping	55
BAB 4	HASIL DAN DISKUSI	57
4.1	Hasil Penelitian	57
4.2	Evaluasi Performa FL dengan Segmented CKKS HE	57
4.2.1	Evaluasi Metrik Global	57
4.2.2	Evaluasi Waktu Komputasi	58
4.3	Pengaruh Security Level	60
4.3.1	Pengaruh Security Level terhadap Metrik Global	61
4.3.2	Pengaruh Security Level terhadap Waktu Komputasi	63
4.4	Pembahasan Hasil Model FL dengan Segmented CKKS HE	64
BAB 5	SIMPULAN DAN SARAN	67
5.1	Simpulan	67
5.2	Saran	67
DAFTAR PUSTAKA		68



DAFTAR TABEL

Tabel 2.1	Arsitektur ResNet22 CNN [5]	8
Tabel 2.2	Penelitian Federated Learning dalam Bidang Kesehatan Sebelumnya	15
Tabel 3.1	Distribusi Dataset CBIS-DDSM dan Pembagian Data pada Setiap Klien	40
Tabel 3.2	Konfigurasi parameter <i>federated learning</i>	47
Tabel 3.3	Parameter CKKS yang Digunakan dalam Model	49
Tabel 4.1	Perbandingan nilai akhir Avg AUC dan Avg PR-AUC pada security level 128	58
Tabel 4.2	Tabel Waktu Komputasi <i>Federated Learning</i> dengan <i>Segmented</i> CKKS HE (<i>Security Level</i> 128-bit)	59
Tabel 4.3	Perbandingan AUC dan PR-AUC pada Berbagai <i>key</i> <i>length</i> dan <i>Security Level</i>	62
Tabel 4.4	Perbandingan Waktu Komputasi pada Berbagai <i>key length</i> dan <i>Security Level</i>	63
Tabel 4.5	Perbandingan Performa Berdasarkan <i>Security Level</i> dan <i>Key Size</i>	64



DAFTAR GAMBAR

Gambar 2.1	Contoh gambar kanker payudara	6
Gambar 2.2	Struktur Umum CNN untuk Klasifikasi Gambar	7
Gambar 2.3	Arsitektur Umum ResNet [13]	8
Gambar 2.4	Gambar Konsep Federated Learning [16]	14
Gambar 2.5	Horizontal Federated Learning	16
Gambar 2.6	Alur kerja umum skema CKKS, meliputi proses inisialisasi hingga <i>decoding</i> . [30]	23
Gambar 2.7	Proses Encryption Segmented CKKS	28
Gambar 3.1	<i>Image Dataset CBIS-DDSM Mammography</i>	38
Gambar 3.2	Alur kerja data collecting	38
Gambar 3.3	Alur kerja data cleaning	39
Gambar 3.4	Alur kerja data splitting	40
Gambar 3.5	Alur kerja data image preprocessing	41
Gambar 3.6	Diagram alur proses <i>Federated Learning</i> dengan <i>Segmented CKKS</i>	42
Gambar 3.7	Alur kerja Curriculum Learning	46
Gambar 3.8	Log inisialisasi konteks dan kunci CKKS pada awal pelatihan.	50
Gambar 3.9	Informasi jumlah data <i>train</i> , <i>validation</i> , dan <i>test</i> pada setiap klien.	51
Gambar 3.10	Log pelatihan lokal berbasis <i>pace</i> dan pemicu agregasi FedAvg.	52
Gambar 3.11	Log nilai <i>generator loss</i> dan <i>discriminator loss</i> setelah aktivasi <i>adversarial</i> domain alignment pada epoch ke-10.	52
Gambar 3.12	Contoh hasil <i>print</i> terminal segmentasi layer pada proses enkripsi CKKS	53
Gambar 3.13	Contoh hasil segmentasi layer pada proses enkripsi CKKS	53
Gambar 3.14	Contoh log terminal hasil agregasi homomorfik CKKS di server.	54
Gambar 3.15	Contoh log terminal hasil dekripsi dan rekonstruksi parameter global di sisi klien.	55
Gambar 3.16	Contoh hasil <i>print</i> terminal mekanisme <i>early stopping</i>	56
Gambar 4.1	Perbandingan kurva Avg Acc per epoch pada security level 128	58
Gambar 4.2	Perbandingan waktu epoch antara <i>Plain FL</i> dan <i>FL + Segmented CKKS HE</i>	59
Gambar 4.3	Grafik Waktu Komputasi <i>Segmented CKKS HE Federated Learning</i>	60
Gambar 4.4	Perbandingan kurva Avg Accuracy pada validation set antara security level 128-bit dan 192-bit pada berbagai <i>key length</i>	61
Gambar 4.5	Grafik Perbandingan Waktu Komputasi pada Berbagai <i>key length</i> dan <i>Security Level</i>	63
Gambar 4.6	Grafik Perbandingan Akurasi pada Model Federated Learning	65

DAFTAR KODE

Kode 2.1	Kode ResNet22	10
Kode 2.2	Kode Encoder ResNet22	11
Kode 2.3	Kelas Classifier pada arsitektur ResNet22	13
Kode 2.4	Proses <i>adversarial alignment</i> pada pelatihan federated learning .	20
Kode 2.5	Pemanggilan fungsi <code>generate_ckks_key()</code> pada mode CKKS di FedSHE	26
Kode 2.6	Implementasi fungsi <code>generate_ckks_key()</code> pada FedSHE	27
Kode 2.7	Pemanggilan fungsi <code>seg_enc_vector()</code> pada mode CKKS di <code>client.py</code>	29
Kode 2.8	Implementasi fungsi <code>enc_vector()</code> dan <code>seg_enc_vector()</code> di <code>SegCKKS.py</code>	29
Kode 2.9	Implementasi Segmented Decryption pada <code>client.py</code>	31
Kode 3.1	Snippet build data train, val, dan test client	51
Kode 3.2	Snippet inisialisasi CKKS, model global, dan klien.	51
Kode 3.3	Implementasi mekanisme adversarial alignment	52
Kode 3.4	Pemanggilan fungsi agregasi homomorfik CKKS di server.	54
Kode 3.5	Pemanggilan fungsi dekripsi dan rekonstruksi parameter global pada sisi klien.	55
Kode 3.6	Pemantauan early stopping berdasarkan <i>validation loss</i> pada server.	55
Kode 3.7	Evaluasi akhir model global menggunakan <i>test set</i> pada masing- masing site.	56
Kode 3.8	Penghitungan rata-rata performa akhir dari seluruh site.	56



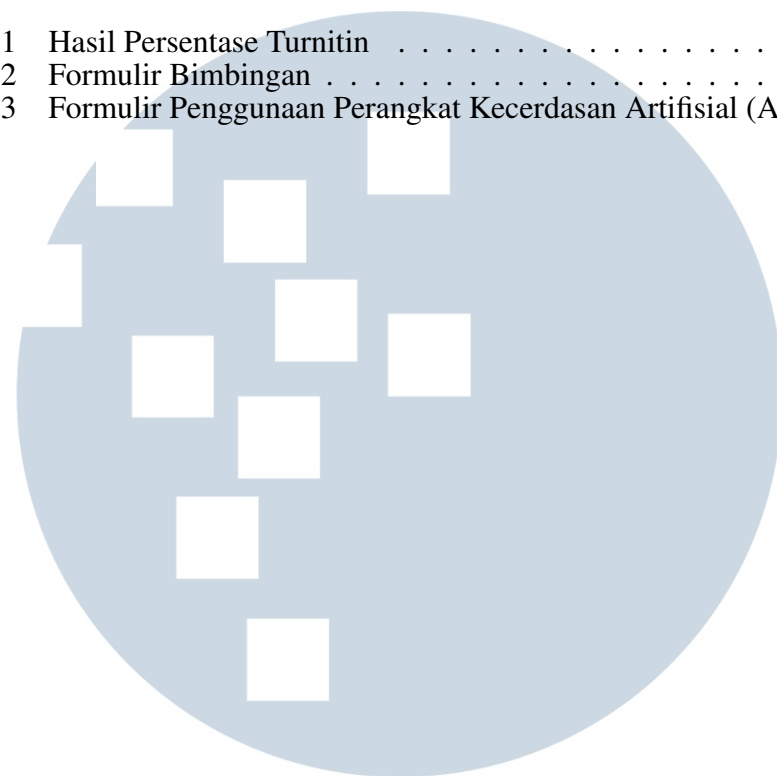
DAFTAR RUMUS

Rumus 2.1	<i>Accuracy</i>	32
Rumus 2.2	TPR dan FPR	32
Rumus 2.3	AUC	32
Rumus 2.4	<i>Precision dan Recall</i>	33
Rumus 2.5	PR-AUC	33
Rumus 2.6	<i>Total Time</i> Komputasi	33
Rumus 2.7	<i>Communication Cost</i> CKKS	34



DAFTAR LAMPIRAN

Lampiran 1	Hasil Persentase Turnitin	72
Lampiran 2	Formulir Bimbingan	73
Lampiran 3	Formulir Penggunaan Perangkat Kecerdasan Artifisial (AI) . .	75



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA