

**PRIVACY PRESERVING COLLABORATIVE DEEP LEARNING
MENGUNAKAN VERIFIABLE
MULTI-SECRET SHARING SCHEME**

TESIS

Oleh:
WULAN SRI LESTARI
NIM. 174211075

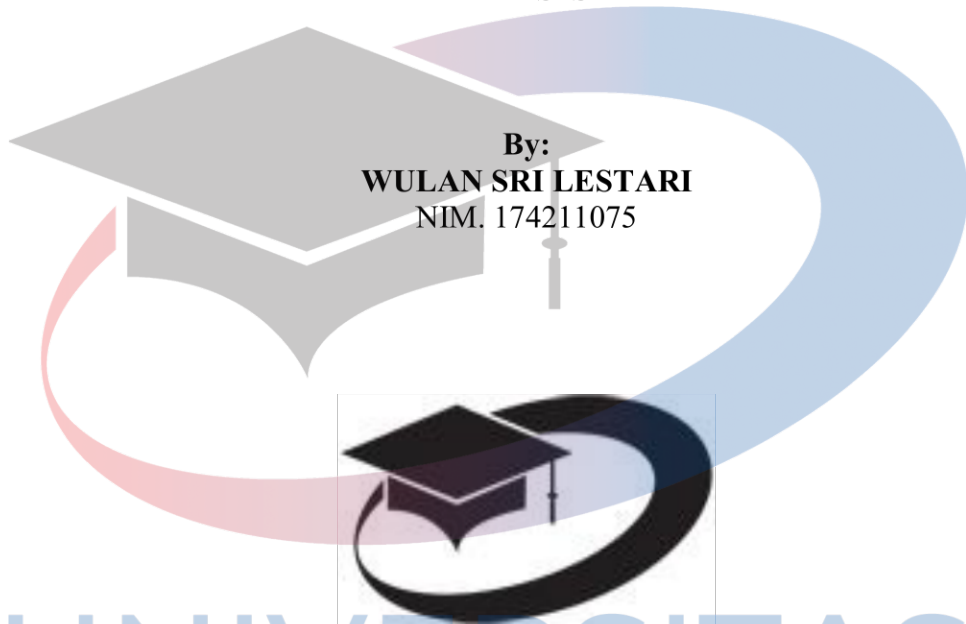


**UNIVERSITAS
MIKROSKIL**

**PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2019**

**PRIVACY PRESERVING COLLABORATIVE DEEP LEARNING USING
VERIFIABLE MULTI-SECRET SHARING SCHEME**

THESIS



**By:
WULAN SRI LESTARI
NIM. 174211075**

**UNIVERSITAS
MIKROSKIL**

**INFORMATION TECHNOLOGY MASTER'S PROGRAM
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2019**

LEMBAR PERNYATAAN

Saya yang membuat pernyataan ini adalah mahasiswa Jurusan/Program Studi S-2 Magister Teknologi Informasi STMIK Mikroskil Medan dengan identitas mahasiswa sebagai berikut:

Nama : Wulan Sri Lestari
Nim : 174211075
Peminatan : Teknologi Informasi

Saya telah melaksanakan penelitian dan penulisan Tesis dengan judul “PRIVACY PRESERVING COLLABORATIVE DEEP LEARNING MENGGUNAKAN VERIFIABLE MULTI-SECRET SHARING SCHEME”, dengan ini saya menyatakan dengan sebenar-benarnya bahwa penelitian dan penulisan Tesis tersebut merupakan hasil karya saya sendiri (tidak meminta orang lain untuk mengerjakannya) dan semua sumber, baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Bila dikemudian hari ternyata terbukti bahwa bukan saya yang mengerjakannya, maka saya bersedia dikenakan sanksi yang telah ditetapkan oleh STMIK Mikroskil Medan, yakni pencabutan ijazah yang telah saya terima dan ijazah tersebut dinyatakan tidak sah.

Selain itu, demi pengembangan ilmu pengetahuan, saya menyetujui untuk memberikan kepada STMIK Mikroskil Medan Hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty Free Right*) atas Tesis saya beserta perangkat yang ada (jika diperlukan). Dengan hak ini, STMIK Mikroskil Medan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan Tesis saya secara keseluruhan atau hanya elektronik, selama tetap mencantumkan nama saya sebagai penulis/pencipta dan pemilik hak cipta. Menyatakan juga bahwa saya akan mempertahankan hak eksklusif saya untuk menggunakan seluruh atau sebagian isi Tesis saya guna pengembangan karya di masa depan, misalnya dalam bentuk artikel, buku, ataupun perangkat lunak.

Demikian pernyataan ini saya perbuat dengan sungguh-sungguh, dalam keadaan sadar dan tanpa ada tekanan dari pihak manapun.

Medan, 20 Agustus 2019
Saya yang membuat pernyataan,

Wulan Sri Lestari

LEMBARAN PENGESAHAN

PRIVACY PRESERVING COLLABORATIVE DEEP LEARNING
MENGUNAKAN VERIFIABLE
MULTI-SECRET SHARING SCHEME

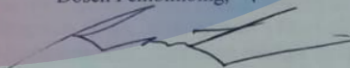
TESIS

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Magister Strata Dua
Program Studi Magister Teknologi Informasi

Oleh:


WULAN SRI LESTARI
NIM. 174211075

Disetujui Oleh:
Dosen Pembimbing,


Dr. Ronsen Purba, M.Sc.

Medan, 20 Agustus 2019
Diketahui dan Disahkan Oleh:

Ketua Program Studi
Magister Teknologi Informasi,


Dr. Ronsen Purba, M.Sc.



ABSTRAK

Collaborative deep learning adalah sebuah pendekatan yang digunakan untuk mengatasi besarnya data latih yang dibutuhkan dalam membangun model *deep learning* yang lebih baik. Dalam *Collaborative deep learning* para peserta mengumpulkan data mereka secara terpusat kepada *server* untuk dilatih kedalam model *deep learning*. Namun, pengumpulan data latih secara terpusat menghadirkan masalah kebocoran privasi yang serius dan rusaknya integritas data latih. Tujuan dari makalah ini adalah memberikan solusi terhadap masalah privasi dan rusaknya integritas data latih dalam *collaborative deep learning* menggunakan *verifiable (k,t,n) multi-secret sharing* (VMSS) berdasarkan *Elliptic Curve Diffie Helman* dan SHA3-256 sebagai fungsi *hash*. Dimana seluruh data latih akan dibentuk menjadi n *shares* menggunakan *session key* yang dihasilkan dari kunci privat dan kunci publik *Elliptic Curve Diffie helman* untuk melindungi privasi dan menghashkan seluruh data latih menggunakan SHA3-256 untuk proses verifikasi sebelum dikirimkan ke *server*. Hasil pengujian menunjukkan integritas data latih yang rusak dan peserta yang berkolusi dapat diverifikasi. Selain itu, akurasi model yang dihasilkan menggunakan atau tanpa menggunakan VMSS memiliki nilai yang sama. Sehingga model yang diusulkan dapat melindungi privasi dan integritas data latih serta mempertahankan akurasi model *deep learning*.

Kata Kunci: *Verifiable Multi-Secret Sharing, Collaborative Deep Learning, Privasi Data, Integritas Data*

UNIVERSITAS
MIKROSKIL

ABSTRACT

Collaborative deep learning is an approach that used to overcome the amount of training data needed in building a better deep learning model. In collaborative deep learning, the central server collects user data and run the deep learning algorithm centrally to get more accurate models. However, centralized training data collection can raise serious of privacy leakage problem and damage to the integrity of training data. In this paper we introduce the privacy preserving collaborative deep learning model using verifiable (k, t, n) multi-secret sharing based on the Elliptic Curve Diffie Helman and SHA3-256 as a hash function. Where all training data will be formed into n shares using a session key generated from the private key and public key Elliptic Curve Diffie helman to protect the privacy and avoid all training data using SHA3-256 for the verification process before sending to server. The test results show the integrity of damaged training data and colluding participants can be verified. In addition, the accuracy of the model produced using or without using VMSS has the same value. Therefore proposed model can protect the privacy and integrity of training data and maintain the accuracy of the deep learning model.

Keyword : Collaborative Deep Learning, Data Privacy, Data Integrity, Verifiable Multi-Secret Sharing

UNIVERSITAS
MIKROSKIL

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Tesis yang berjudul “*Privacy Preserving Collaborative Deep Learning Menggunakan Verifiable Multi-Secret Sharing Scheme*”.

Tesis ini dibuat untuk melengkapi persyaratan kurikulum pada Program Studi Magister Teknologi Informasi Strata Dua, STMIK Mikroskil Medan.

Penulis menyampaikan banyak terima kasih kepada:

1. Bapak Dr. Ronsen Purba, M.Sc., selaku Dosen Pembimbing dan Ketua Program Studi Magister Teknologi Informasi yang telah membimbing penulis dalam proses penyelesaian tesis ini.
2. Bapak Arwin Halim S.Kom., M.Kom., selaku Dosen Pendamping Pembimbing yang telah membimbing penulis dalam proses penyelesaian tesis ini.
3. Bapak Dr. Pahala Sirait, S.T., M.Kom., selaku Ketua STMIK Mikroskil Medan dan selaku Dosen Penguji yang telah memberikan saran dan masukannya.
4. Bapak Djoni, S.Kom., M.T.I., selaku Wakil Ketua I STMIK Mikroskil Medan.
5. Ibu Dr. Elviawaty Muisa Zamzami, M.T., M.M., selaku Dosen Penguji yang telah memberikan saran dan masukannya.
6. Bapak atau Ibu Dosen STMIK Mikroskil Medan yang telah membantu proses penulisan tesis ini.
7. Anggota keluarga, teman, saudara dan semua pihak yang terus memberikan dukungan penuh kepada penulis selama proses penulisan tesis ini.

Penulis menyadari bahwa masih terdapat banyak kekurangan yang ada. Oleh sebab itu, kritik dan saran yang bersifat membangun akan sangat diterima. Akhir kata, semoga Tesis ini dapat bermanfaat bagi masyarakat. Terima kasih.

Medan, 12 Agustus 2019

Penulis

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL	viii
DAFTAR LAMPIRAN	ix
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian	3
1.2.1. Identifikasi Masalah	3
1.2.2. Rumusan Masalah	3
1.3. Tujuan dan Manfaat Penelitian	3
1.4. Batasan Masalah	4
1.5. Metodologi Penelitian	4
1.6. Sistematika Penulisan	5
BAB II KAJIAN LITERATUR	6
2.1. Tinjauan Pustaka	6
2.1.1. Deep Learning	6
2.1.2. Collaborative Deep Learning	10
2.1.3. Privacy Preservation dalam Collaborative Deep Learning	12
2.1.4. Verifiable Multi Secret Sharing Scheme	14
2.1.5. Klasifikasi Tumor Otak	18
2.2. Kerangka Pikir Pemecahan Masalah	21
BAB III METODOLOGI PENELITIAN	23
3.1. Analisis Masalah	23
3.2. Metode Penelitian	24
3.3. Data Yang Digunakan	32
3.4. Alat-Alat Penelitian	33
3.5. Teknik Analisis	34

BAB IV HASIL DAN PEMBAHASAN	36
4.1. Hasil.....	36
4.1.1. Pembentukan Kunci	36
4.1.2. Pembentukan Share.....	40
4.1.3. Rekonstruksi Share	42
4.1.4. Klasifikasi Tumor Otak.....	44
4.1.5. Pengujian.....	50
4.2. Pembahasan	55
4.2.1. Penambahan Noise	55
4.2.2. Peserta Curang	56
4.2.3. Pertukaran Session Key Antar Peserta	56
4.2.4. Pertukaran Secret Shadow.....	56
BAB V KESIMPULAN DAN SARAN.....	57
5.1. Kesimpulan.....	57
5.2. Saran.....	57
DAFTAR PUSTAKA	58

UNIVERSITAS MIKROSKIL

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur CNN	7
Gambar 2. 2 Direct Collaborative Deep Learning	11
Gambar 2. 3 Indirect Collaborative Deep Learning	12
Gambar 2. 4 Model Multi-Key Privacy Preserving Deep Learning	13
Gambar 2. 5 Tumor Otak Glioma	20
Gambar 2. 6 Tumor Otak Meningioma.....	20
Gambar 2. 7 Tumor Otak Pituitary	21
Gambar 3. 1 Flowchart Metode Penelitian	24
Gambar 3. 2 Activity Diagram Model VMSSS dalam CDL untuk Klasifikasi Tumor Otak.....	25
Gambar 3. 3 Flowchart Pembentukan Kunci Peserta.....	26
Gambar 3. 4 Flowchart Pembentukan Kunci Dealer	27
Gambar 3. 5 Flowchart Pembentukan Share.....	28
Gambar 3. 6 Flowchart Rekonstruksi Share	29
Gambar 3. 7 Flowchart Klasifikasi Tumor Otak.....	30
Gambar 4. 1 Tampilan Utama Model	36
Gambar 4. 2 Kunci Privat dan Kunci Publik Peserta.....	37
Gambar 4. 3 Kunci Privat dan Kunci Publik Dealer.....	38
Gambar 4. 4 Secret Shadow Peserta	38
Gambar 4. 5 Secret Shadow dan Zi Peserta Oleh Dealer.....	39
Gambar 4. 6 k Secret Citra Tumor Otak Meningioma.....	39
Gambar 4. 7 Nilai Hash k Secret (M)	40
Gambar 4. 8 Session Key Peserta	40
Gambar 4. 9 Share.....	41
Gambar 4. 10 Nilai b_i dan $g(r_i)$	41
Gambar 4. 11 Nilai y_i	41
Gambar 4. 12 Nilai c_i	41
Gambar 4. 13 Verifikasi $f(r_i)$ dan $g(r_i)$	42
Gambar 4. 14 Share Proses Rekonstruksi	42
Gambar 4. 15 Verifikasi Session Key.....	44
Gambar 4. 16 Rekonstruksi Share.....	44
Gambar 4. 17 Directory Dataset.....	45
Gambar 4. 18 Parameter CNN	45
Gambar 4. 19 Model CNN.....	46
Gambar 4. 20 Proses Preprocessing Citra.....	46
Gambar 4. 21 Proses Klasifikasi Training	47
Gambar 4. 22 Grafik Akurasi dan Loss Training dan Validation	47
Gambar 4. 23 Pemanggilan Model Klasifikasi	48
Gambar 4. 24 Proses Klasifikasi Testing	48
Gambar 4. 25 Klasifikasi Tumor Otak.....	49
Gambar 4. 26 Pengujian Noise.....	50

Gambar 4. 27 Pengujian Session Key Peserta Curang.....	52
Gambar 4. 28 Share Pengujian Pertukaran Session Key	52
Gambar 4. 29 Pengujian Pertukaran Session Key.....	53
Gambar 4. 30 Pertukaran Secret Shadow.....	55



UNIVERSITAS MIKROSKIL

DAFTAR TABEL

Tabel 3. 1. Perbedaan Model.....	30
Tabel 3. 2. Skenario Simulasi	32
Tabel 3. 3. Rincian Dataset CE-MRI	33
Tabel 3. 4. Confusion Matrix	35
Tabel 4. 1 Confusion Matrix	49
Tabel 4. 2 Pengujian Noise	50



UNIVERSITAS MIKROSKIL

DAFTAR LAMPIRAN

Lampiran 1 : DAFTAR ISTILAH.....	59
Lampiran 2 : DAFTAR RIWAYAT HIDUP.....	60



UNIVERSITAS MIKROSKIL