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

TESIS

Oleh:
WULAN SRI LESTARI
NIM. 174211075

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

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, mengelolah 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 MENGGUNAKAN 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 meng*hash*kan 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

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*

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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN