BAB I
PENDAHULUAN

1.1. Latar Belakang

Collaborative Deep Learning (CDL) merupakan situasi dimana dua atau lebih peserta dapat mempelajari model *deep learning* bersama-sama dengan mengumpulkan data latih secara terpusat kepada pihak ketiga (*server*) (Zhang, et al., 2018a). Akurasi model *deep learning* sangat dipengaruhi oleh volume dan kualitas data latih yang digunakan (Ma, et al., 2018). CDL hadir untuk meningkatkan akurasi model dengan memasukkan lebih banyak data latih ke dalam proses pembelajaran dibandingkan belajar hanya menggunakan data latih lokal (Kwabena, et al., 2019). Misalnya beberapa rumah sakit dapat berkolaborasi untuk melakukan diagnosa penyakit berdasarkan data-data pasien yang dikumpulkan. Namun pengumpulan data latih secara terpusat dalam CDL menimbulkan masalah kebocoran privasi data yang serius (Zhao, et al., 2018). Privasi data merupakan konsep luas yang berkaitan dengan *accountability*, *secrecy*, *fairness*, *correctness* dan *availability* terkait data peserta (Canetti, 2006). Kebocoran privasi data dapat terjadi karena adanya serangan eksternal dan adanya peserta dan *server honest but curious* yang berusaha mengetahui privasi data.

Untuk mengatasi masalah di atas, Li *et al.* (2017) mengusulkan model *multi-key privacy preserving deep learning* menggunakan *Fully Homomorphic Encryption* (FHE) untuk melindungi privasi data latih dalam CDL dari peserta dan *server honest but curious* dimana para peserta mengenkripsi data mereka sebelum dikirim ke *server* untuk dilatih kedalam *deep learning*. Kekurangan model tersebut adalah mereka berasumsi bahwa peserta tidak akan berkolusi, maka model mereka akan gagal melindungi privasi data dalam skenario dimana para peserta berkolusi. Untuk mencegah para peserta berkolusi, Chahar *et al*. (2017) mengusulkan skema *elliptic-curve cryptosystem* dan *Shamir's Secret Sharing* (SSS) untuk menjamin privasi data. Namun, model berdasarkan *homomorphic encryption* dan SSS tidak menjamin integritas data latih (Attasena, Harbi & Darmont, 2017). Sehingga apabila integritas data latih rusak, hal ini akan

berpengaruh buruk pada hasil *deep learning*. Gao *et al.* (2018) mengusulkan model untuk melakukan verifikasi integritas data menggunakan *Verifiable Secret Sharing Scheme* (VSSS) dengan fungsi *hash*. Proses verifikasi yang dilakukan dalam model tersebut adalah memeriksa kebenaran *share* dan *secret* hasil rekonstruksi. Kekurangan model tersebut adalah VSSS hanya dapat digunakan untuk membentuk dan merekonstruksi *share* dari satu *secret* saja. Sedangkan dalam CDL setiap peserta memiliki banyak *secret*.

Pada penelitian ini kami mengusulkan model menggunakan *Verifiable Multi-Secret Sharing Scheme* (VMSSS) dengan *Elliptic Curve Diffie-Hellman* (ECDH) dan fungsi *hash*. VMSSS merupakan skema yang memungkinkan pembentukan dan rekonstruksi *share* dari banyak *secret* (Chattopadhyay, et al., 2018). Pembentukan *share* dilakukan untuk melindungi privasi data dari pihak yang tidak berwenang dan *share* yang dihasilkan akan disimpan ke dalam *server.* Model yang diusulkan memungkinkan para peserta untuk melakukan verifikasi *share* dan *secret* hasil rekonstruksi untuk memastikan integritas data latih. Selain itu, proses verifikasi juga dibutuhkan untuk mendeteksi peserta yang melakukan kecurangan ataupun kolusi.

Model yang diusulkan akan digunakan dalam CDL untuk melakukan klasifikasi tumor otak. Tumor otak merupakan salah satu kanker yang paling berbahaya dan mematikan bagi pasien. Identifikasi dini dan klasifikasi tumor otak ke dalam jenis yang spesifik merupakan hal yang sangat penting agar dapat melakukan pengobatan yang efektif (Sajjada, et al., 2018). Namun, sensitifitas data latih yang digunakan membutuhkan perlindungan privasi dan jaminan integritas data agar tidak terjadi kesalahan terhadap hasil klasifikasi.

Berdasarkan uraian di atas, maka pada penelitian ini akan diusulkan model yang fokus untuk menyelesaikan masalah dalam CDL dengan memverifikasi data latih menggunakan VMSSS dengan ECDH dan fungsi *hash* untuk melindungi privasi dan integritas data untuk klasifikasi tumor otak dengan judul "**Privacy Preserving Collaborative Deep Learning Menggunakan Verifiable Multi-Secret Sharing Scheme".**

1.2. Masalah Penelitian

Berdasarkan uraian pada latar belakang di atas, maka masalah dalam penelitian ini dapat diuraikan menjadi dua bagian yaitu identifikasi masalah dan rumusan masalah.

1.2.1. Identifikasi Masalah

Adapun identifikasi masalah pada latar belakang di atas adalah sebagai berikut:

1. Adanya kebocoran privasi data latih dalam CDL akibat serangan eksternal.
2. Adanya *server* dan peserta *honest but curious* yang berusaha mengetahui privasi data latih.
3. Adanya peserta yang berkolusi untuk mengetahui privasi data latih.
4. Proses verifikasi dibutuhkan untuk menjamin integritas data latih dalam melakukan klasifikasi tumor otak.

1.2.2. Rumusan Masalah

Berdasarkan identifikasi masalah yang ada, maka rumusan masalah pada penelitian ini adalah bagaimana manghasilkan model untuk memverifikasi data latih untuk melindungi privasi dan integritas data, mencegah terjadinya kolusi antar peserta dan mencegah kesalahan dalam proses klasifikasi tumor otak.

1.3. Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah menghasilkan model untuk memverifikasi data latih yang digunakan dalam proses CDL untuk klasifikasi tumor otak menggunakan VMSSS dengan ECDH dan fungsi *hash* sehingga privasi dan integritas data latih tetap terjaga.

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Model ini dapat menjadi alternatif untuk melakukan CDL tanpa harus khawatir privasi akan bocor dari *server* dan peserta *honest but curios* dan integritas data latih rusak.
2. Model ini dapat digunakan oleh beberapa Rumah Sakit untuk berkolaborasi mendiagnosa penyakit tanpa melanggar aturan privasi yang ada.

3. Hasil penelitian dapat digunakan sebagai referensi untuk penelitian lebih lanjut di bidang *privacy preserving* dalam CDL.

1.4. Batasan Masalah

Adapun batasan dari penelitian ini adalah sebagai berikut:

1. *Dataset* yang digunakan adalah citra medis otak MRI yang diambil dari *figshare* Cheng *Brain Tumor Dataset* yang berisi 3 jenis tumor seperti *meningioma*, *glioma*, *pituitary*. *Dataset* tersedia secara umum dan dapat diakses pada *link* https://figshare.com/articles/brain_tumor_dataset/1512427.
2. Citra medis otak yang digunakan terdiri dari 600 citra yang terdiri dari 3 kategori yaitu 200 citra medis tumor *meningioma,* 200 citra medis tumor *glioma* dan 200 citra medis tumor *pituitary*.
3. Metode *deep learning* yang digunakan adalah *Convolution Neural Network* (CNN).
4. Skema VMSSS yang digunakan adalah skema (k, t, n) VMSSS dimana $k > t$ dan $k = n$.
5. Fungsi *hash* yang digunakan adalah SHA3-256.

1.5. Metodologi Penelitian

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi literatur

   Pada tahap ini dilakukan proses untuk memahami bagaimana konsep *privacy preserving* dalam CDL, masalah yang ada pada CDL, proses klasifikasi tumor otak dan metode yang sudah ada.
2. Analisis masalah

   Pada tahap ini dilakukan analisis berdasarkan hasil studi literatur untuk mengidentifikasi masalah yang harus diselesaikan, data yang dibutuhkan, dan menentukan metode yang diusulkan untuk menyelesaikan masalah.
3. Perancangan model

   Pada tahap ini dilakukan perancangan model dengan membuat *activity diagram* yang menggambarkan proses penerapan VMSSS dengan ECDH dan

fungsi *hash* untuk *verfiable privacy preserving* dalam CDL untuk klasifikasi tumor otak.

4. Pengujian
   a. Melakukan pengujian penambahan *noise* terhadap *share* yang digunakan untuk mengetahui apakah *k secret* kembali atau tidak pada proses rekonstruksi.
   b. Melakukan pengujian *correctness* dengan verifikasi *session key* dan *secrets* untuk melindungi integritas data latih.
   c. Melakukan pengujian verifikasi peserta yang berkolusi dengan menukarkan *session key* yang digunakan pada proses rekonstruksi.
   d. Melakukan pengujian verifikasi *dealer* yang curang dengan menukarkan *secret shadow* peserta.
5. Menarik kesimpulan dari hasil pengujian
6. Menyusun laporan Tesis

1.6. Sistematika Penulisan

Sistematika penulisan laporan penelitian ini terdiri dari 5 bab, dimana secara garis besar masing-masing bab membahas hal – hal berikut ini. Bab 1 Pendahuluan, berisi penjelasan umum, masalah dan solusi yang sudah ada dan akan dilakukan. Bab 2 berisi studi literatur dan tinjauan pustaka terkait masalah dan metode yang berhubungan dengan penelitian yang akan dilakukan. Bab 3 Metodologi Penelitian, berisi identifikasi masalah, langkah-langkah dari metode yang diusulkan, data yang digunakan, alat-alat penelitian dan metode analisis. Bab 4 Hasil dan Pengujian, berisi hasil yang diperoleh dari model yang dibangun dan pengujian yang dilakukan. Bab 5 Kesimpulan dan Saran, berisi kesimpulan yang diperoleh dari hasil dan pengujian penelitian yang dilakukan dan saran yang dapat dilakukan untuk hasil yang lebih baik pada penelitian selanjutnya.