

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Federated Learning (FL) merupakan paradigma pembelajaran mesin terdistribusi yang memungkinkan pelatihan model secara kolaboratif tanpa mengirimkan data mentah ke server pusat [1]. Pada metode FL konvensional seperti *Federated Averaging* (FedAvg) [2], setiap klien melatih model secara lokal, kemudian mengirimkan parameter atau pembaruan model ke server untuk diagregasi menjadi model global. Meskipun mampu menjaga data tetap berada di sisi klien, FL konvensional masih menghadapi tantangan berupa biaya komunikasi yang tinggi, heterogenitas model dan perangkat, serta penurunan performa ketika distribusi data antar klien bersifat tidak identik [3]. Oleh karena itu, diperlukan pendekatan alternatif yang dapat mengurangi beban komunikasi, mendukung heterogenitas model, dan tetap mempertahankan kinerja model [4].

Salah satu pendekatan alternatif dalam FL adalah *distillation-based Federated Learning* atau *Federated Distillation* (FD), yaitu pendekatan yang memanfaatkan proses transfer pengetahuan antar model melalui pertukaran output model, seperti *logits* atau *soft-label*, antara klien dan server. Berbeda dengan FL konvensional yang mengirimkan parameter model, FD memungkinkan klien membagikan informasi berupa prediksi yang lebih ringkas tanpa harus mengirimkan keseluruhan parameter model [5]. FD dapat mendukung penggunaan arsitektur model yang heterogen antar klien dan menurunkan risiko terbukanya informasi sensitif dibandingkan pendekatan yang membagikan parameter atau gradients secara langsung [6, 7]. Namun, FD masih memiliki keterbatasan dari sisi efisiensi komunikasi dan mekanisme agregasi *soft-label*. Salah satu keterbatasannya adalah pengiriman *soft-label* yang berulang pada beberapa *communication round* untuk sampel data publik yang sama [8]. Selain itu, metode agregasi berbasis entropi konvensional, seperti *Entropy Reduction Aggregation* (ERA) [9], masih memiliki ketidakstabilan karena parameter *temperature* sensitif terhadap variasi entropi input.

Sejalan dengan kebutuhan efisiensi komunikasi dalam FD, Azuma et al. [10] mengembangkan SCARLET, yaitu *framework Federated Distillation* yang mengintegrasikan mekanisme *soft-label caching* dan *Enhanced Entropy Reduction*

Aggregation (Enhanced ERA). Mekanisme *soft-label caching* digunakan untuk menyimpan dan menggunakan kembali *soft-label* yang telah tersedia pada *cache*, sehingga klien hanya perlu mengirimkan *soft-label* untuk data publik yang belum tersimpan. Dengan mekanisme *soft-label caching*, komunikasi yang redundan dapat dikurangi untuk mengurangi beban komunikasi. Selain itu, *Enhanced ERA* digunakan untuk mengatur tingkat ketajaman hasil agregasi *soft-label* secara lebih stabil dibandingkan pendekatan berbasis *temperature* konvensional. Pengaturan ketajaman tersebut dilakukan melalui parameter β , di mana peningkatan nilai β menghasilkan distribusi *soft-label* yang lebih tajam. Meskipun nilai β statis pada *Enhanced ERA* mampu menghasilkan performa yang mendekati optimal, penelitian SCARLET menyebutkan bahwa otomatisasi penyesuaian β secara adaptif masih menjadi arah pengembangan lebih lanjut dengan memanfaatkan entropi *soft-label* hasil agregasi yang tersedia pada server.

Nilai entropi yang dihitung secara berurutan dapat mengandung variansi sehingga perubahan nilainya tidak selalu sepenuhnya merepresentasikan perubahan kondisi yang sebenarnya [11]. Costa et al. [12] menerapkan *Exponential Moving Average* (EMA) untuk menghaluskan perubahan temporal pada indikator berbasis entropi sebelum indikator tersebut digunakan dalam proses deteksi perubahan distribusi data. Peleg et al. [13] menjelaskan bahwa EMA memberikan bobot yang menurun secara eksponensial terhadap observasi sebelumnya sehingga dapat menyeimbangkan pengurangan noise dan pemeliharaan tren pada data berurutan. Berdasarkan prinsip tersebut, penelitian ini menggunakan EMA untuk menghaluskan nilai entropi yang sudah dinormalisasi di setiap ronde sebelum nilai tersebut dibandingkan dengan nilai ambang dalam penentuan parameter β .

Penelitian ini berfokus pada pengembangan *Adaptive β* berbasis *Exponential Moving Average* (EMA) dari entropi *soft-label* pada *Enhanced Entropy Reduction Aggregation* (ERA) dalam SCARLET untuk *Federated Distillation* menggunakan model *LeNet-5*. Nilai *Shannon entropy* dihitung dari hasil agregasi *soft-label*, kemudian dinormalisasi dan dihaluskan menggunakan EMA untuk mengurangi pengaruh fluktuasi nilai entropi antar-*round*. Nilai EMA entropi selanjutnya digunakan sebagai dasar penentuan parameter β secara adaptif dalam proses penajaman *soft-label*. Evaluasi dilakukan berdasarkan *accuracy* dan *loss* model global dengan membandingkan penerapan *Adaptive β* terhadap beberapa konfigurasi β statis.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana pengembangan *Adaptive β* berbasis entropi *soft-label* pada *Enhanced Entropy Reduction Aggregation* (Enhanced ERA) dalam SCARLET untuk *Federated Distillation* dengan model LeNet-5?
2. Bagaimana pengaruh *Adaptive β* berbasis entropi *soft-label* terhadap performa model (*accuracy* dan *loss*) pada SCARLET?

1.3 Batasan Permasalahan

Batasan permasalahan dalam penelitian ini ditetapkan agar kajian tetap terarah dan tidak meluas dari fokus utama penelitian. Adapun batasan dalam penelitian ini adalah sebagai berikut:

1. Dataset yang digunakan pada penelitian ini terbatas pada MNIST sebagai *private dataset* dan EMNIST Letters sebagai *public dataset* dalam skema *Federated Distillation*.
2. Penelitian difokuskan pada pengembangan *Adaptive β* berbasis entropi *soft-label* pada mekanisme *Enhanced Entropy Reduction Aggregation* (Enhanced ERA) dalam SCARLET.
3. Model yang digunakan pada sisi klien dan server dibatasi pada arsitektur LeNet-5.
4. Pengukuran hasil penelitian dibatasi pada performa model (*accuracy* dan *loss*).
5. Mekanisme *Adaptive β* dikembangkan berdasarkan entropi *soft-label* yang diperoleh dari proses agregasi pada data publik untuk menyesuaikan tingkat penajaman *soft-label* pada Enhanced ERA.
6. Simulasi federasi dijalankan secara lokal pada satu perangkat, sehingga komunikasi antar klien dan server direpresentasikan melalui proses simulasi tanpa jaringan nyata.

7. Penelitian ini tidak membahas aspek keamanan, serangan privasi, enkripsi, maupun mekanisme perlindungan data tambahan di luar konsep dasar *Federated Learning* dan *Federated Distillation*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan *Adaptive β* berbasis entropi *soft-label* pada *Enhanced Entropy Reduction Aggregation* (Enhanced ERA) dalam SCARLET untuk *Federated Distillation* dengan model LeNet-5.
2. Mengevaluasi pengaruh *Adaptive β* terhadap performa model (*accuracy* dan *loss*) pada SCARLET.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan kontribusi akademis dalam pengembangan *Federated Distillation*, khususnya pada mekanisme agregasi *soft-label* yang adaptif melalui penerapan *Adaptive β* berbasis entropi.
2. Menjadi referensi bagi penerapan SCARLET dengan *Enhanced Entropy Reduction Aggregation* (Enhanced ERA) dalam lingkungan federasi yang memiliki variasi distribusi data antar klien.
3. Mendemonstrasikan penerapan *Adaptive β* berbasis entropi *soft-label* pada SCARLET dengan model LeNet-5, serta memberikan analisis terhadap performa model (*accuracy* dan *loss*).

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun ke dalam lima bab yang saling berkaitan, yaitu:

1. Bab 1 PENDAHULUAN

Bab ini menguraikan latar belakang penelitian, rumusan masalah, batasan permasalahan, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

2. **Bab 2 LANDASAN TEORI**

Bab ini memaparkan teori dan konsep yang relevan dengan penelitian, meliputi *Federated Learning*, *Federated Distillation*, *Knowledge Distillation*, SCARLET, *Enhanced Entropy Reduction Aggregation* (Enhanced ERA), *Exponential Moving Average* (EMA), entropi *soft-label*, serta penelitian terdahulu yang menjadi dasar pengembangan *Adaptive β* .

3. **Bab 3 METODOLOGI PENELITIAN**

Bab ini menjelaskan metodologi penelitian, meliputi konfigurasi eksperimen pada SCARLET, pengembangan mekanisme *Adaptive β* berbasis entropi *soft-label*, penggunaan dataset dan model, skenario distribusi data, serta metode evaluasi yang digunakan.

4. **Bab 4 HASIL DAN DISKUSI**

Bab ini menyajikan hasil eksperimen dan pembahasan terhadap penerapan *Adaptive β* pada SCARLET. Analisis dilakukan terhadap performa model dan perubahan entropi *soft-label* selama proses pelatihan.

5. **Bab 5 KESIMPULAN DAN SARAN**

Bab ini berisi simpulan dari hasil penelitian serta saran untuk pengembangan penelitian selanjutnya.

