BAB 5
Simpulan dan Saran

5.1 Simpulan

Berdasarkan hasil implementasi dan evaluasi sistem *Federated Learning* (FL) dengan *Packed CKKS Homomorphic Encryption* dan mekanisme *top-k sparsification*, diperoleh simpulan sebagai berikut:

1. *Packed CKKS Homomorphic Encryption* berhasil diimplementasikan pada sistem *Federated Learning* dan berjalan secara *end-to-end*. Enkripsi diterapkan pada komunikasi dan agregasi pembaruan model tanpa mengubah alur dasar pelatihan FL. Pembaruan model yang dikirim klien dan diproses server berada dalam bentuk *ciphertext*, sehingga server tidak mengakses nilai parameter asli (*plaintext*). Sistem tetap menghasilkan model global yang dapat dievaluasi menggunakan metrik Akurasi, AUC dan PR–AUC.

2. Penerapan *Packed CKKS Homomorphic Encryption* meningkatkan privasi dengan konsekuensi peningkatan biaya komputasi dan komunikasi. Dibandingkan mode *plain*, konfigurasi terenkripsi meningkatkan total waktu komputasi sekitar 1,56–1,59$\times$ per ronde serta meningkatkan *data transfer volume* akibat pengiriman pembaruan model dalam bentuk *ciphertext* hasil *packing*. Performa model juga mengalami penurunan yang terukur, dengan penurunan AUC pada kisaran 2,08–2,53% dan PR–AUC pada kisaran 3,88–5,14%, yang menunjukkan adanya *trade-off* antara privasi, utilitas model, dan efisiensi sistem.

3. Integrasi *adversarial alignment* dan *curriculum learning* pada *federated learning* terenkripsi meningkatkan utilitas dibanding pendekatan terenkripsi murni. Perbandingan menunjukkan bahwa kombinasi dalam penelitian ini (*Fed-Align-CL + Top-k + Packed CKKS*) menghasilkan akurasi lebih tinggi daripada *FedPHE* (Nan Yan et al.) yang hanya menerapkan *top-k sparsification* dan *Packed CKKS Homomorphic Encryption* tanpa mekanisme *alignment* dan *curriculum learning*. Temuan ini mengindikasikan bahwa *alignment* dan *curriculum learning* berkontribusi pada peningkatan kualitas pembaruan model pada *federated learning* terenkripsi.

4. Konfigurasi *top-k* 0,2 direkomendasikan karena mampu menjaga utilitas model tetap kompetitif pada skema *federated learning* terenkripsi. Konfigurasi ini menunjukkan selisih utilitas yang relatif kecil dibanding varian terenkripsi lain, sekaligus memberikan *data transfer volume* sekitar 4× lebih rendah dibanding *top-k* 0,8. Dibandingkan mode *plain* (AUC 87,86%, PR–AUC 84,83%), konfigurasi *top-k* 0,2 (AUC 85,54%, PR–AUC 80,95%) menunjukkan penurunan yang terukur namun tidak drastis. Temuan ini mengindikasikan bahwa pengiriman 20% parameter masih mampu mempertahankan performa evaluasi akhir yang kompetitif, meskipun pembaruan model diproses dalam domain terenkripsi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya adalah sebagai berikut:

1. Penelitian selanjutnya dapat mengeksplorasi kombinasi *Packed CKKS Homomorphic Encryption* dengan mekanisme privasi tambahan, seperti *Secure Aggregation* atau *Differential Privacy*, untuk meningkatkan perlindungan privasi serta membandingkan *overhead* sistem secara lebih komprehensif.
2. Evaluasi sistem dapat diperluas dengan melibatkan jumlah klien yang lebih banyak serta distribusi data yang lebih heterogen (*non-IID*), sehingga dapat merepresentasikan skenario *federated learning* yang lebih realistis dan kompleks.
3. Eksperimen lanjutan dapat mengkaji pengaruh variasi parameter CKKS, seperti *polynomial degree* dan skala presisi, terhadap *trade-off* antara performa model, waktu komputasi, dan biaya komunikasi pada sistem *federated learning* terenkripsi.
4. Penelitian lanjutan dapat mengembangkan implementasi *federated learning* yang lebih realistis dengan menjalankan setiap klien sebagai proses terpisah (misalnya satu proses atau terminal untuk setiap klien) agar mendekati skenario *federated learning* nyata.
5. Penelitian selanjutnya dapat menerapkan manajemen kunci yang lebih aman, misalnya melalui *Key Distribution Center* (KDC) dan penggunaan kunci

berbeda untuk tiap klien (bukan *single shared key*), serta memperluas ke arah *distributed key generation*.