BAB 5
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil implementasi dan evaluasi sistem *Federated Learning* dengan *Segmented CKKS Homomorphic Encryption*, diperoleh simpulan sebagai berikut:

1. *Segmented* CKKS Homomorphic Encryption berhasil diimplementasikan pada sistem *Federated Learning* dengan model ResNet22. Mekanisme enkripsi diterapkan pada proses komunikasi dan agregasi parameter antar tiga klien tanpa mengubah alur dasar pelatihan, sehingga sistem tetap berjalan secara *end-to-end* dengan parameter model yang dikomunikasikan dalam bentuk terenkripsi dan performa yang dapat dievaluasi.

2. Penerapan *Segmented CKKS Homomorphic Encryption* meningkatkan waktu pelatihan total dari 1602.77 detik menjadi 1752–2262 detik dan biaya komunikasi dari 11.5 MB menjadi 307.5–459 MB. Dari sisi performa, rata-rata AUC dan PR-AUC mengalami penurunan masing-masing sebesar 2.7–13.1% dan 4.1–16.6% dibandingkan *Plain Federated Learning*. Namun, konfigurasi *security level* 192-bit menghasilkan performa yang lebih tinggi dibandingkan 128-bit, dengan peningkatan AUC sebesar 3.9–4.7% dan PR-AUC sebesar 4.8–8.6% pada seluruh ukuran kunci.

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 pengelolaan kunci enkripsi yang lebih aman, di mana setiap klien dan server memiliki pasangan kunci masing-masing tanpa *shared key*, serta dikombinasikan dengan mekanisme privasi tambahan.

2. Evaluasi sistem dapat diperluas dengan jumlah klien yang lebih banyak dan distribusi data yang lebih heterogen, serta diarahkan pada implementasi *deployment* nyata, bukan hanya simulasi.