BAB V
PENUTUP

5.1 Simpulan

Penelitian ini bertujuan untuk menerapkan enkripsi tingkat kolom pada *database* kepegawaian di PT Indonesia Indicator, menggunakan pendekatan arsitektur *microservices*. Implementasi enkripsi ini memanfaatkan algoritma simetris AES dan *Blowfish* untuk melindungi data sensitif seperti NIK, NPWP, NO KK, dan Alamat pegawai. Berdasarkan hasil yang diperoleh, beberapa kesimpulan dapat diambil:

1. Penerapan enkripsi tingkat kolom berhasil menjaga kerahasiaan data sensitif dan keamanan data yang meningkat di lingkungan arsitektur *microservices* PT Indonesia Indicator. Enkripsi ini memastikan bahwa data yang tersimpan di dalam *database* tidak mudah diakses oleh pihak yang tidak berwenang.

2. Pengujian kinerja menunjukkan bahwa algoritma *Blowfish* memiliki keunggulan dalam hal kecepatan enkripsi dan dekripsi, dengan proses yang lebih cepat dibandingkan algoritma AES dengan waktu yang lebih lambat. Namun, pemilihan algoritma tetap harus mempertimbangkan faktor keamanan dari serangan kriptografi *modern* selain performa, mengingat AES-256 dikenal lebih kuat dari segi keamanan kriptografi.

3. Implementasi enkripsi kolom ini terbukti dalam arsitektur *microservices*, di mana data dapat dienkripsi dan didekripsi langsung di tingkat *database*, meminimalkan kompleksitas pada layanan microservices.

4. Berdasarkan hasil penelitian, algoritma *Blowfish* direkomendasikan untuk kebutuhan yang mengutamakan kecepatan enkripsi, karena memiliki waktu proses yang lebih singkat. Namun, jika prioritas utama adalah tingkat keamanan yang lebih tinggi, maka algoritma AES lebih disarankan,

mengingat jumlah putaran (*rounds*) yang lebih banyak, sehingga memberikan perlindungan yang lebih kuat terhadap serangan kriptografi.

Dengan demikian, penelitian ini memberikan kontribusi penting dalam meningkatkan keamanan data di PT Indonesia Indicator, khususnya dalam melindungi data kepegawaian secara aman.

5.2 Saran

Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. Disarankan untuk melakukan pengujian dalam skala besar untuk mengukur kinerja enkripsi dalam volume data yang lebih besar, sehingga sistem dapat dioptimalkan lebih baik dalam situasi nyata.

2. Implementasi rotasi kunci enkripsi perlu dipertimbangkan untuk meningkatkan keamanan data, sehingga kunci yang digunakan dapat diganti secara berkala dan mencegah risiko akses tidak sah.

3. Disarankan untuk melakukan pemantauan kinerja dan keamanan sistem secara berkala, serta mengembangkan metode enkripsi baru jika diperlukan agar sistem tetap aman dari ancaman kriptografi yang terus berkembang.

Penelitian ini diharapkan dapat menjadi referensi dalam pengembangan sistem keamanan data pada organisasi lain, khususnya dalam konteks arsitektur *microservices* dan manajemen data sensitif.