BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan data menjadi salah satu prioritas utama dalam pengelolaan informasi diberbagai sektor, termasuk sektor pemerintahan dan swasta. Berdasarkan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi seperti data kepegawaian yang mencakup Nomor Induk Kependudukan (NIK), Nomor Pokok Wajib Pajak (NPWP), Nomor Kartu Keluarga (NO KK), dan Alamat, harus dilindungi dari akses yang tidak sah (Anggen Suari & Sarjana, 2023).

Salah satu solusi yang semakin populer dalam menjaga keamanan data adalah Enkripsi Tingkat Kolom (*Column-Level Encryption*) pada database (Forgy, 2009; Terencio Nathanael, 2023), yang memungkinkan setiap kolom yang berisi data sensitif untuk dienkripsi secara individual, memastikan bahwa data tetap terlindungi bahkan jika terjadi pelanggaran keamanan (Mursalat et al., n.d.).

Dalam konteks arsitektur *microservices*, pengelolaan data sensitif menjadi lebih kompleks karena adanya distribusi layanan yang dapat diakses oleh berbagai komponen sistem. Oleh karena itu, diperlukan algoritma enkripsi yang tidak hanya kuat dari sisi keamanan, tetapi juga optimal dalam hal kinerja dan penggunaan sumber daya.

Penelitian ini didasarkan pada studi kasus PT Indonesia Indicator, sebuah perusahaan yang terlibat dalam berbagai aktivitas bisnis yang berhubungan dengan data dan informasi. PT Indonesia Indicator secara aktif memanfaatkan data dalam kegiatan operasionalnya, sehingga memastikan keamanan data sensitif menjadi aspek krusial. Dengan semakin meningkatnya kebutuhan akan perlindungan data di perusahaan ini, penerapan enkripsi tingkat kolom pada database menjadi solusi penting untuk menjaga kerahasiaan informasi.

Penelitian ini bertujuan untuk mengukur dan membandingkan kinerja kedua algoritma tersebut serta memberikan rekomendasi algoritma enkripsi yang paling sesuai untuk memenuhi kebutuhan keamanan dan kinerja pada sistem *microservices* dan berfokus pada dua algoritma enkripsi populer, yaitu *Blowfish* dan *Advanced Encryption Standard* (AES), yang digunakan dalam implementasi enkripsi tingkat kolom pada database berbasis PostgreSQL.

Melalui penelitian ini, diharapkan dapat memberikan kontribusi signifikan terhadap peningkatan keamanan data sensitif di perusahaan, serta memberikan panduan dalam memilih algoritma enkripsi yang tepat untuk berbagai kebutuhan industri, khususnya pada PT Indonesia Indicator yang bergerak di bidang pengelolaan data dan informasi.

1.2 Deskripsi Pekerjaan

Program magang pada divisi *back-end* PT Indonesia Indicator akan berfokus pada implementasi keamanan data pada sistem kepegawaian perusahaan, dengan fokus utama pada penerapan enkripsi tingkat kolom di database berbasis PostgreSQL.

Dalam magang ini dilibatkan dalam pengembangan dan pengujian sistem enkripsi menggunakan algoritma *Blowfish* dan AES-256 untuk meningkatkan perlindungan data sensitif karyawan, seperti NIK, NPWP, dan informasi pribadi lainnya. Pengembangan ini juga melibatkan pengintegrasian algoritma enkripsi ke dalam arsitektur *microservices* untuk menjaga keamanan data sensitif.

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mengembangkan pemahaman mendalam tentang enkripsi tingkat kolom (*Column-Level Encryption*) pada database.
2. Mempelajari implementasi algoritma *Blowfish* dan AES dalam sistem *microservices*.
3. Mengukur dan membandingkan kinerja kedua algoritma enkripsi dari segi waktu eksekusi.
4. Menghasilkan rekomendasi algoritma enkripsi yang paling sesuai untuk kebutuhan keamanan dan kinerja dalam sistem *microservices*.

1.4 Manfaat

Setelah menyelesaikan kegiatan magang, peserta akan memperoleh manfaat berupa:

1. Perusahaan dapat memastikan perlindungan lebih baik terhadap data sensitif, sehingga risiko kebocoran atau akses tidak sah dapat diminimalkan.
2. Perusahaan memperoleh analisis komparatif antara algoritma *Blowfish* dan AES dari segi kecepatan proses, penggunaan sumber daya, serta tingkat keamanan. Hasil analisis ini dapat menjadi dasar dalam menentukan algoritma enkripsi yang paling sesuai untuk kebutuhan sistem perusahaan.
3. Penerapan solusi enkripsi dalam arsitektur *microservices* memungkinkan perusahaan untuk mengelola keamanan data secara lebih fleksibel dan terdistribusi, tanpa mengganggu performa layanan yang berjalan.
4. Dengan memahami tantangan dalam melindungi data sensitif serta solusi yang diterapkan, perusahaan dapat mengembangkan strategi keamanan yang lebih baik dan berkelanjutan dalam pengelolaan informasi digital.