BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Penggunaan smartphone saat ini menjadi kebutuhan bagi masyarakat, karena dari aplikasi saat ini yang beredar adalah untuk membantu memenuhi kebutuhan masyarakat sehari – hari. Dari masalah transportasi, komunikasi, keuangan dan pendidikan tersedia pada aplikasi smartphone mereka. Sehingga hal ini menjadi perhatian penting yang perlu dikelola dengan baik, karena sudah terkait kebutuhan masyarakat yang banyak. Terutama dalam masalah terkait keuangan, yang saat ini begitu mudah orang memanfaatkan teknologi keuangan untuk memenuhi kebutuhan hidup mereka sehari hari. Contoh dari transaksi keuangan yang sering dilakukan masyarakat adalah transaksi transfer uang, top up pulsa dan pembayaran lainnya secara online. Dengan melihat tingginya kebutuhan masyarakat dalam penggunaan transaksi keuangan secara online, saat ini bermunculan teknologi dengan istilah *Fintech* (*Financial Technology*). Banyak para pengusaha, berlomba – lomba untuk meraih pasar dalam bidang keuangan ini. Hal ini dibuktikan dengan adanya Asosiasi *Fintech* Indonesia yang jumlah anggotanya ada 366 perusahaan pada tahun 2022. Dengan rincian anggota 102 *Fintech* pinjaman online, 84 *Fintech* inovasi keuangan digital (IKD), 39 *Fintech* sistem pembayaran, 13 *Fintech* mitra teknologi, 6 *Fintech* institusi keuangan, 5 *Fintech* pasar modal, 4 *Fintech* aset digital dan 113 perusahaan *Fintech* lainnya (Annur, 2023).

Berdasarkan data dari OWASP (Open Web Application Security Project) yang merupakan referensi keamanan *Web Application* di dunia menyebutkan bahwa *Cryptographic Failure* yang menyebabkan terjadinya kebocoron data menduduki peringkat nomor 2 di dunia dengan kasus sebanyak 233.788 kasus pada tahun 2021 (OWASP, 2021). OWASP menyarankan beberapa hal pencegahan dari kasus tersebut, diantaranya yaitu memastikan data terenkripsi dan memastikan menggunakan algoritma enkripsi yang kuat sebagai bentuk proteksi data atau yang kita kenal dengan Data Security. *Encryption* merupakan salah satu bagian dari *Data Security* (Devi & Thangamuthu, 2021). *Encryption* adalah teknik mengubah data menjadi format terenkripsi yang hanya dapat dibaca dengan kunci enkripsi yang benar. *Encryption* memberikan kemampuan kepada organisasi untuk melakukan proteksi terhadap data yang sensitif dan data yang rahasia. Secara umum ada 2 jenis enkripsi berdasarkan kunci yang digunakan yaitu enkripsi simetris (kunci yang sama untuk enkripsi dan dekripsi) , yang lainnya yaitu enkripsi asimetris (kunci public untuk enkripsi dan kunci privasi untuk dekripsi) (Calder

& Watkins, 2020). Dari sisi proses data hasil enkripsi dibedakan 2 jenis yaitu proses aritmatika langsung pada *cipher (*hasil enkrispi) dan proses aritmatika *cipher* lewat dekripsi data terlebih dahulu. FHE (*Fully Homomorphic Encryption*) merupakan salah satu contoh algoritma enkripsi yang bisa langsung dilakukan proses aritmatika pada *cipher* sedangkan AES (*Advanced Encryption Standard*) merupakan salah satu contoh dari algoritma enkripsi yang membutuhkan proses dekripsi terlebih dahulu untuk melakukan aritmatika. Kedua algoritma ini telah mendukung Panjang key 256 bit yang artinya kemunkingkinan untuk melakukan *crack* adalah selama 3.31×10^{56} tahun (Marsiani et al., 2021).

Penelitian yang dilakukan oleh (Nurdin et al., 2022) merupakan upaya dalam menjaga kerahasiaan data berupa pengamanan terhadap pesan singkat atau kita kenal dengan SMS menggunakan enkripsi 3DES (Triple Data Encryption Standard) yang menghasikan sebuah aplikasi android untuk membaca pesan dan mengirimkan pesan terproteksi ini Sehingga operator seluler pun tidak bisa membaca isi pesan yang dikirimkan menggunakan aplikasi ini. Hal ini sangat bermanfaat untuk masyarakat dalam menjaga kerahasiaan informasi mereka Ketika berkomunikasi. Dan juga penelitian yang dilakukan oleh (Nurdin et al., 2021) terkait upaya pencegahan kejahatan lewat toko online, karena banyaknya kejahatan online yang terjadi. Penelitian lain selanjutnya yang terkait teknik pengamanan data menggunakan AES adalah yang dalam penelitian tersebut menerapkan kriptografi AES untuk mengamankan dokumen dengan hasil yang didapatkan adalah kriptografi AES memiliki kehandalan terhadap pencurian data (Azhari et al., 2022). AES merupakan singkatan dari (*Advanced Encryption Standar*). Yang merupakan kriptografi yang dikeluarkan oleh Pemerintahan Amerika untuk mengamankan data pemerintahan. AES biasanya diimplementasikan pada hardware dan software untuk melakukan enkripsi data yang sifatnya sensitif (Golovko & Tolochyn, 2022). Panjang kunci fleksibel bisa 128-bit, 192-bit dan 256 bit (Hidayat & Mahardiko, 2020). Dalam penelitian yang dilakukan oleh (Marsiani et al., 2021) difokuskan pada kunci 256-bit, karena berdasarkan hasil penelitian menunjukkan bahwa pengamanan data pribadi sangat baik dan aman.

Penelitian lainnya yang terkait pengamanan data dengan kriptografi AES tentang implementasi AES-256 untuk mengamankan data pribadi yang dari penelitian tersebut didapatkan bahwa kriptografi AES keamanan data dapat terjaga karena algoritma tersebut melakukan pengamanan dan penyandian yang berlapis – lapis (Marsiani et al., 2021). Penelitian sebelumnya yang telah dilakukan dalam Upaya pengamanan *Fintech* adalah penelitian (Altaee & Alanezi, 2021) menggunakan Partially Homomorphic Encryption yang

proses enkripsi tersebut menghasilkan hasil enkripsi yang memungkinkan untuk dilakukan aritmatika, namun kekurangan dari Partially Homomorphic Encryption hanya memungkinan satu jenis aritmatika saja. Penelitian tersebut yang merupakan sebuah pengajuan untuk mengamankan data bank yang sangat mirip transaksinya dengan *Fintech*. Penelitian lainnya adalah (Ramtri & Patel, 2020) menggunakan enkripsi RSA yang digunakan untuk mengamankan data pada aplikasi Internet Banking. Penelitian lainnya adalah (Ganeshan et al., 2020) menggunakan AES dalam mengamankan data Internet Banking. Selain terkait dengan pengamanan data jurnal terkait adalah masalah pengujian performa website yang dilakukan oleh (Suhaili Sahibul Muna et al., 2023) terkait pengujian performa menggunakan metode PIECES.

Salah satu Aplikasi *Fintech* yang belum dilakukan pengamanan data adalah Aplikasi Nurapay yang dimiliki oleh PT. Deacas International Trade, belum diterapkannya kriptografi pada *database*. Hal ini jika ada pelaku kejahatan yang berhasil masuk ke dalam server maka akan sangat mudah untuk membaca data yang terdapat dalam *database*. Aplikasi Nurapay inilah yang dijadikan sebagai bahan penelitian dalam penelitian ini. Pentingnya penelitian ini dilakukan adalah untuk mencari Algoritma yang tepat untuk mengamankan data, tanpa harus mengorbankan kecepatan akses Aplikasi Nurapay secara khusus dan Aplikasi *Fintech* secara umum. Dan yang tidak kalah pentingnya dari penelitian ini adalah bagaimana cara implementasi Algoritma AES dan Algoritma FHE yang efisien tanpa harus mengubah struktur aplikasi secara keseluruhan.

Maka dari itu dalam upaya untuk mengurangi dampak dari *Cryptographic Failure* dilakukan penelitian berupa membandingkan 2 algoritma pengamanan untuk mencapai efisiensi dalam pengamanan data finansial ke dalam bentuk tugas akhir dengan judul **"***Analisis Komparatif antara Enkripsi AES (Advanced Encryption Standard) dengan Enkripsi FHE (Fully Homomorphic Encryption) dalam mengamankan data pada Aplikasi Fintech***".**

1.2 Rumusan Masalah

Dari latar belakang yang telah disampaikan di atas, maka berikut ini penulis rumuskan beberapa permasalahan yaitu :

1. Bagaimana merancang sebuah sistem untuk memperkuat pengamanan pada aplikasi *Fintech* yang efisien ?
2. Bagaimana cara mengimplementasikan metode AES (*Advanced Encryption Standard*) dan FHE (*Fully Homomorphic Encryption*) ke dalam Aplikasi *Fintech*?

1.3 Batasan Masalah

Mengenai ruang lingkup dalam penelitian ini adalah sebagai berikut ini :

1. Penelitian ini bertujuan untuk menguji metode AES (*Advanced Encryption Standard*) dan FHE (*Fully Homomorphic Encryption*) dalam mengamankan data Aplikasi *Fintech* yang akan diterapkan ke dalam Aplikasi Nurapay sebagai contoh kasus dari Aplikasi *Fintech*.
2. Pada penelitian ini peneliti mengambil data sampel dari Aplikasi Nurapay berupa Data Pelanggan, Data Produk dan Data Transaksi. Data ini diperoleh berdasarkan izin dari pemilik Aplikasi Nurapay yaitu PT. Deacas International Trade. Dalam kesepakatan data yang diberikan oleh mereka harus disamarkan, karena terkait kerahasiaan data pelanggan mereka. Maka peneliti nantinya, dari data tersebut mengolah dan menyamarkan data yang telah diberikan dengan tetap memperhatikan tipe data yang digunakan.
3. Sampel data yang digunakan di dalam penelitian ini adalah 1000 Data pelanggan, 1000 Data Produk dan 1000 Data Transaksi yang diambil dan diolah kembali dari Aplikasi Nurapay.
4. Adapun kriteria data yang digunakan adalah Data Pelanggan berupa field nama, email, nomor telepon, saldo, pin, nomor kartu keluarga dan nomor kartu tanda penduduk. Untuk Data Produk yaitu kode, nama, deskripsi, harga dan kategori. Untuk Data Transaksi yaitu nomor tujuan transaksi, user, hasil transaksi, harga, keuntungan, status, tanggal dan jam transaksi.

1.4 Tujuan Penelitian

Adapun tujuan adanya penelitian ini dilakukan adalah

1. Menganalisa hasil perbandingan antara Algoritma AES dan Algoritma FHE yang efisien berdasarkan waktu dan konsumsi sumber daya untuk kemudian menjadi panduan untuk dirancang dan diciptakan sistem pengamanan data.
2. Menciptakan sebuah sistem untuk memperkuat pengamanan data aplikasi *Fintech* dengan mengimplementasikan metode enkripsi AES dan FHE pada Aplikasi Nurapay.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini dilakukan adalah sebagai berikut ini :

1. Dengan adanya sistem ini, diharapkan para pelaku usaha *Fintech* dapat menerapkan konsep pengamanan data dari hasil penelitian ini, sehingga bisa memperkecil kemungkinan data dicuri.

2. Dapat menjadi referensi bagi pengembang aplikasi yang memiliki kemiripan data dengan penelitian ini seperti aplikasi Bank, Koperasi, Kasir dan aplikasi keuangan lainnya.
3. Dapat menjadi referensi bagi peneliti selanjutnya yang ingin melakukan penelitian sejenis.
4. Hasil penelitian ini diharapkan dapat memberikan rekomendasi performa yang terbaik antara 2 algoritma tersebut.