

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan keamanan informasi menjadi semakin penting seiring meningkatnya kebutuhan akan penyimpanan dan pengiriman data secara elektronik. Keamanan informasi merupakan proses, prosedur, dan kebijakan yang bertujuan melindungi data dari akses yang tidak sah [1]. Tantangan dalam menjaga keamanan informasi semakin kompleks karena pelaku serangan siber kini menggunakan metode yang lebih terstruktur dan canggih untuk menembus sistem [2]. Oleh karena itu, penting untuk memastikan bahwa perlindungan data pribadi konsumen dikelola secara aman dan sesuai regulasi, seiring pesatnya perkembangan teknologi digital dan meningkatnya penggunaan layanan berbasis elektronik.

Perkembangan teknologi informasi saat ini memberikan berbagai kemudahan dalam proses pengolahan, penyimpanan, serta pengiriman data. Salah satu layanan yang banyak memanfaatkan teknologi informasi adalah penyedia layanan internet/WiFi, di mana proses pendaftaran pelanggan umumnya mewajibkan pencantuman data pribadi seperti nama, alamat, nomor telepon, hingga NIK untuk keperluan verifikasi. Data tersebut bersifat sensitif dan memerlukan perlindungan yang baik karena dapat menimbulkan risiko penyalahgunaan apabila dikelola tanpa sistem keamanan yang memadai. Tingginya penggunaan layanan internet di Indonesia yang mencapai lebih dari 80,66% populasi pada 2025 semakin menuntut pengelolaan data pelanggan yang aman dan terstandar [3].

Perlindungan data pribadi juga menjadi kewajiban hukum yang harus dipenuhi oleh setiap Penyelenggara Sistem Elektronik (PSE), termasuk penyedia layanan internet atau provider WiFi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa setiap pengendali data wajib menjaga keamanan data pribadi, mencegah akses tidak sah, serta memastikan bahwa pemrosesan data dilakukan berdasarkan persetujuan yang sah dari pemilik data [4]. Oleh

karena itu, penyedia layanan internet wajib menerapkan sistem pengamanan data yang memadai untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

Namun, pada kenyataannya, masih ada penyedia layanan WiFi lokal dan berskala kecil yang belum menerapkan sistem pengamanan data yang optimal. Salah satunya adalah provider layanan WiFi Zix's Com yang telah menggunakan sistem dalam pengelolaan data pelanggan. Data pelanggan disimpan dalam basis data sistem aplikasi tersebut, yang membantu proses administrasi dan layanan. Namun, metode kriptografi yang digunakan untuk melindungi data pelanggan belum diterapkan dengan jelas dan belum didokumentasikan dengan baik. Akibatnya, jika seseorang mendapatkan akses tidak sah ke basis data aplikasi, itu dapat menimbulkan risiko keamanan data. Selain menyebabkan kerugian bagi pelanggan, situasi tersebut juga dapat mengurangi kepercayaan masyarakat terhadap layanan internet yang ditawarkan.

Selain ancaman dari pihak luar, penyalahgunaan akses data oleh pihak internal juga menjadi perhatian dalam keamanan informasi. Adanya kasus akses data pelanggan oleh oknum karyawan menunjukkan bahwa data pribadi masih dapat diakses oleh pihak yang tidak memiliki kewenangan penuh dalam pengelolaan data, padahal informasi tersebut seharusnya hanya dapat diakses oleh admin atau pemilik layanan (*owner*) [5]. Kondisi ini menunjukkan pentingnya penerapan sistem keamanan data yang tidak hanya mampu melindungi data dari serangan eksternal, tetapi juga membatasi hak akses pengguna sesuai dengan perannya dalam sistem.

Untuk mengatasi permasalahan tersebut, diperlukan sistem yang mampu melindungi data pelanggan. Salah satu metode yang dapat diterapkan adalah kriptografi. Kriptografi merupakan teknik untuk mengamankan data dengan cara mengubah data asli menjadi bentuk yang tidak dapat dibaca tanpa kunci tertentu. Dari beberapa algoritma kriptografi yang ada, *Advanced Encryption Standard* (AES) merupakan algoritma

kriptografi simetris yang memiliki tingkat keamanan tinggi, proses enkripsi yang cepat, dan telah ditetapkan sebagai standar enkripsi internasional [6]. Penelitian terdahulu menyebutkan bahwa meskipun AES menawarkan perlindungan yang kuat terhadap serangan, proses enkripsinya cenderung lebih lambat dibandingkan algoritma *Blowfish* yang lebih ringan dalam pemrosesan [7]. Di sisi lain, DES diketahui memiliki kekurangan penting karena panjang kunci yang pendek, sehingga mudah diserang dan tidak lagi direkomendasikan untuk pengamanan data modern [7].

Berdasarkan pertimbangan tersebut, penelitian ini memilih algoritma AES-128 dengan mode *Cipher Block Chaining* (CBC) karena mampu memberikan keseimbangan antara tingkat keamanan dan efisiensi komputasi. Hasil penelitian Pratama dan Yuana menunjukkan bahwa AES-128 memiliki waktu eksekusi paling cepat, diikuti oleh AES-192, sedangkan AES-256 membutuhkan waktu pemrosesan paling lama. Perbedaan tersebut disebabkan oleh jumlah putaran (*round*) yang digunakan, yaitu 10 putaran pada AES-128, 12 putaran pada AES-192, dan 14 putaran pada AES-256, sehingga AES-128 memiliki beban komputasi yang lebih ringan [8].

Oleh karena itu, AES-128 dipilih dalam penelitian ini karena dianggap paling relevan dan aman untuk diterapkan dalam pengamanan data pelanggan layanan internet/WiFi. Pada penelitian ini, algoritma yang digunakan adalah AES-128 dengan mode *Cipher Block Chaining* (CBC). Pada mode ini, setiap blok *plaintext* akan dikombinasikan terlebih dahulu dengan blok *ciphertext* sebelumnya, sedangkan pada blok pertama digunakan *Initialization Vector* (IV) sebagai nilai awal. Penggunaan IV bertujuan untuk menghasilkan *ciphertext* yang berbeda meskipun data yang dienkripsi sama, sehingga pola data menjadi lebih sulit dikenali dan tingkat keamanan semakin meningkat. Dengan penerapan AES-128 mode CBC, data pelanggan akan dienkripsi sebelum disimpan ke dalam basis data. Oleh karena itu, data pelanggan disimpan dalam bentuk *ciphertext* sehingga tidak dapat dibaca secara langsung ketika diakses melalui basis data. Penerapan AES-128 mode CBC diharapkan dapat meningkatkan keamanan

penyimpanan data pelanggan dibandingkan penyimpanan data dalam bentuk *plaintext*. Dengan demikian, penerapan AES-128 mode CBC diharapkan mampu meningkatkan keamanan data pelanggan dan mengurangi risiko penyalahgunaan informasi.

1.2 Rumusan Masalah

1. Bagaimana cara menerapkan algoritma kriptografi AES-128 pada proses pengamanan data pelanggan layanan wifi?
2. Bagaimana proses enkripsi dan dekripsi data pelanggan menggunakan algoritma AES-128?

1.3 Tujuan

1. Menerapkan algoritma kriptografi AES-128 untuk mengamankan data pelanggan layanan wifi.
2. Mengimplementasikan proses enkripsi dan dekripsi data menggunakan algoritma AES-128.

1.4 Batasan Masalah

1. Penelitian hanya berfokus pada implementasi algoritma AES-128 sebagai metode pengamanan data.
2. Data yang digunakan adalah data pelanggan berupa Nama, NIK, Nomor Telepon, dan Alamat.
3. Implementasi penelitian dilakukan dalam bentuk sistem web sederhana untuk mengelola data pelanggan, yang dilengkapi dengan proses enkripsi dan dekripsi menggunakan algoritma AES-128, tanpa mencakup seluruh operasional sistem provider secara penuh.

1.5 Manfaat

Penelitian ini diharapkan memberikan kontribusi dalam penerapan algoritma AES-128 sebagai metode enkripsi untuk menjaga kerahasiaan data pelanggan layanan WiFi, sehingga informasi yang bersifat sensitif dapat terlindungi dari akses yang tidak sah. Selain itu, hasil penelitian ini dapat dijadikan acuan dalam pengembangan sistem keamanan data pada berbagai layanan berbasis informasi yang mengolah identitas pengguna.

Penelitian ini juga diharapkan dapat meningkatkan pemahaman mengenai pentingnya perlindungan data pribadi melalui proses enkripsi serta membuktikan efektivitas algoritma AES-128 dalam memperkuat keamanan penyimpanan data.

