BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan ilmu pengetahuan dan teknologi telah membawa dampak besar pada kehidupan masyarakat di Indonesia, terutama dalam bidang keamanan siber [1]. Keamanan siber memiliki peran krusial dalam konteks perlindungan sistem komputer, jaringan, perangkat, dan data dari berbagai ancaman dan upaya akses ilegal [2,3]. Hal ini penting untuk melindungi data pribadi, menjaga keamanan bisnis, serta menjaga kestabilan infrastruktur kritis seperti transportasi data. Selain itu, keamanan siber juga menjadi landasan bagi pengembangan teknologi yang lebih canggih dan berkontribusi pada kesadaran masyarakat akan pentingnya menjaga keamanan data pribadi [2,4,5].

Situasi saat ini menunjukkan adanya permasalahan yang penting terkait dengan kebocoran data. Indonesia sering kali mengalami kasus kebocoran data. Menurut data dari perusahaan keamanan siber Surfshark, Indonesia bahkan menempati peringkat ketiga dalam jumlah kasus kebocoran data terbanyak di dunia pada tahun 2022, dengan lebih dari 12 juta akun yang terkena dampak [6]. Bahkan pada tahun 2023, telah terjadi 94 insiden kebocoran data di Indonesia, dimana 35 diantaranya terjadi pada tahun tersebut. Salah satu insiden yang mencolok adalah aksi peretasan oleh kelompok LockBit yang berhasil mengeksploitasi data internal Bank Syariah Indonesia (BSI) hingga sekitar 1,5 terabyte. Data yang berhasil diakses oleh peretas mencakup informasi sensitif dari sekitar 15 juta nasabah BSI, termasuk data seperti nama, nomor telepon, alamat, saldo rekening, riwayat transaksi, tanggal pembukaan rekening, detail pekerjaan, dan beberapa data lainnya. Kemudian data nasabah BSI disebarkan di pasar gelap internet atau *dark web* [7]. Tidak hanya kasus peretasan terhadap BSI, tetapi juga banyak kasus kebocoran data lainnya yang telah mencuat, seperti kebocoran data BPJS Ketenagakerjaan, data paspor, data dari Dukcapil, dan bahkan data kartu SIM [8]. Semua peristiwa ini menunjukan kerentanan yang serius terhadap privasi dan keamanan data individu serta lembaga-lembaga yang terkena dampak. Kerentanan akan terjadi jika keamanan data

yang digunakan masih sangat lemah dan mudah untuk diretas oleh pihak yang tidak berwenang.

Untuk mengatasi masalah kebocoran data yang telah dijelaskan sebelumnya, salah satu langkah yang diambil adalah mengimplementasikan enkripsi pada tingkat database, termasuk proses pengenkripsian seluruh tabel yang ada dalam database tersebut. Dengan menerapkan enkripsi di level database, tujuan utamanya adalah memastikan bahwa keamanan data tetap terjaga dengan baik, terlepas dari upaya akses ilegal yang terjadi di berbagai lembaga, termasuk layanan kesehatan seperti Arif Merbabu Care Ponorogo. Dalam konteks penelitian ini, digunakan algoritma enkripsi yang sudah mempunyai lisensi berstandar internasional dan telah diadopsi secara luas oleh perusahaan maupun lembaga keuangan di seluruh dunia yaitu *Advanced Encryption Standard* (AES-128) [9].

Proses enkripsi dilakukan pada data pasien sebelum data tersebut disimpan ke dalam database. Selama proses enkripsi, informasi sensitif seperti NIK, nama, alamat, data kelahiran, jenis kelamin, umur, nomor telepon, dan riwayat penyakit, keluhan, password, email diubah menjadi format yang hanya dapat dibaca dengan menggunakan kunci enkripsi yang benar. Dengan menerapkan pendekatan ini, penelitian ini bertujuan untuk mengurangi risiko terhadap kemungkinan bocornya data pasien. Kebocoran data termasuk dalam masalah serius yang dapat mengancam privasi pasien, dan dengan memasukkan lapisan keamanan ini dalam sistem database, upaya dilakukan untuk memberikan solusi praktis guna menjaga keamanan data pasien, memastikan privasi tetap terjaga, dan mengurangi potensi akses yang tidak sah. Berdasarkan latar belakang yang telah diuraikan diatas, maka pada penelitian ini dipilih judul "Implementasi *Advanced Encryption Standard* (AES-128) pada Keamanan Database Pasien (Studi Kasus : Merbabu Care Ponorogo)".

1.2 RUMUSAN MASALAH

Berdasarkan permasalahan dari latar belakang yang telah diuraikan diatas, maka rumusan masalah dari penelitian ini adalah bagaimana pengamanan data

pasien menggunakan Algoritma *Advanced Encryption Standard* (AES-128) pada Database Sistem Registrasi Pasien ?

1.3 TUJUAN PENELITIAN

Tujuan dalam penelitian ini adalah pengamanan data pasien menggunakan Algoritma *Advanced Encryption Standard* (AES-128) pada Database Sistem Registrasi Pasien.

1.4 BATASAN MASALAH

Batasan masalah yang terdapat pada penelitian ini yaitu :

1. Penelitian ini tidak mencakup evaluasi pengguna.
2. Penelitian ini tidak melakukan perbandingan dengan metode enkripsi lainnya.
3. Penelitian ini hanya membahas tentang keamanan database pasien pada Sistem Registrasi Pasien**.**
4. Penelitian ini menggunakan bahasa pemrograman PHP untuk penerapan kode Algoritma *Advanced Encryption Standard* (AES-128)**.**
5. Penelitian ini menggunakan mode operasi *Electronic Code Book* (ECB).
6. Penelitian ini menggunakan data pasien di Arif Merbabu Care dengan jumlah 150 data.

1.5 MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah melindungi database pasien dan mengurangi potensi risiko kebocoran pada Database Sistem Registrasi Pasien, khususnya pada layanan kesehatan Merbabu Care di Ponorogo.