BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi informasi telah menciptakan lingkungan di mana data menjadi inti dari banyak proses bisnis dan aktivitas sehari-hari. Data telah menjadi salah satu aset ekonomi yang paling berharga. Perusahaan, pemerintah, dan individu mengumpulkan, menyimpan, dan memproses data untuk mendukung pengambilan keputusan, inovasi, dan efisiensi operasional. Data telah menjadi sangat penting dalam mendukung berbagai keputusan bisnis dan strategi. Perusahaan mengandalkan data untuk menganalisis tren, memahami pelanggan, dan mengidentifikasi peluang baru. Pemerintah menggunakan data untuk menginformasikan kebijakan publik, sedangkan individu memanfaatkan data pribadi mereka untuk pengalaman yang disesuaikan.

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak bertanggung jawab (Fahri Husaini et al., 2022).

Ancaman terhadap keamanan data semakin berkembang dan kompleks. Malware, serangan siber, dan kebocoran data adalah ancaman yang terus berkembang yang dapat merugikan organisasi dan individu. Serangan siber juga dapat membahayakan infrastruktur kritis, seperti listrik, komunikasi, dan keuangan. Karena berharganya suatu data, maka data menjadi target serangan oleh para *hacker*. Karenanya, keamanan suatu informasi menjadi sesuatu informasi yang dijaga dengan baik. Pengamanan informasi pada prinsipnya berfungsi untuk melindungi informasi agar siapapun yang tidak berhak tidak dapat membaca, mengubahnya, atau menghapus informasi tersebut.

Dalam upaya untuk menjaga keamanan data, kriptografi telah menjadi solusi yang luas digunakan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang digunakan untuk mengamankan komunikasi dan data melalui transformasi informasi menjadi bentuk yang tidak dapat dibaca oleh pihak yang

tidak berwenang. Algoritma kriptografi kunci-publik telah menjadi bagian integral dalam membangun sistem keamanan yang kuat untuk mengamankan suatu data (Daffa Ananda, 2022).

Badan Siber dan Sandi Negara (BSSN) mencatat, Indonesia kembali mendapatkan 279,84 juta serangan siber pada 2023. Walaupun demikian, jumlah tersebut menurun 24,4% dari tahun sebelumnya yang sebanyak 370,02 juta serangan dapa dilihat pada gambar 1.1.

Gambar 1. 1 Data serangan siber di Indonesia (BSSN, 2023)

Kejahatan siber di Indonesia tidak hanya menyerang dunia bisnis dan industri, namun juga banyak menyerang data-data tentang riwayat kesehatan seseorang, yang mana hal ini seharusnya menjadi sebuah data penting yang harus diamankan. Rekam medis atau biasa disebut riwayat medis merupakan sekumpulan data yang berisi catatan dan dokumen mengenai identitas pasien, pemeriksaan medis, pengobatan, serta layanan-layanan medis maupun non medis yang telah dilakukan oleh pasien. Setiap pasien yang melakukan pengobatan baik rawat jalan maupun rawat inap dengan segala tindakan yang dilakukan seperti pengecekan laboratorium, radiologi, dan pemeriksaan penunjang Kesehatan lainnya dicatat dan disimpan dengan baik. (Direktorat Jenderal Pelayanan Kesehatan Kemenkes, 2023). Tujuan dari penyimpanan yang baik tersebut adalah bentuk implementasi dari undang-undang yang telah diatur oleh Kemenkes RI pada PERMENKES RI

No. 24 tahun 2022 yang berbunyi, “Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 membebankan kewajiban kepada seluruh fasilitas pelayanan kesehatan (termasuk tempat praktik mandiri yang diselenggarakan oleh tenaga kesehatan dan tenaga medis) untuk menyelenggarakan rekam medis elektronik sesuai dengan peraturan tersebut, paling lambat pada tanggal 31 Desember 2023. Menkes melalui Direktur Jenderal Pelayanan Kesehatan Kementerian Kesehatan dapat mengenakan sanksi administratif (teguran tertulis dan/atau rekomendasi pencabutan atau pencabutan status akreditasi) terhadap fasilitas pelayanan kesehatan yang melakukan pelanggaran. Meskipun data-data medis tersebut telah diatur di beberapa undang-undang kementerian kesehatan, namun kenyataannya masih banyak data-data medis yang bocor atau disalahgunakan oleh oknum-oknum tertentu.

Dengan adanya fenomena tersebut diperlukan suatu metode untuk menjaga keamanan data. Salah satu metodenya adalah Enkripsi. Enkripsi adalah proses mengubah informasi atau data menjadi bentuk yang sulit dipahami atau diartikan oleh pihak yang tidak berwenang. Enkripsi merupakan hal yang sangat penting dalam kriptografi supaya data yang dikirimkan bisa terjaga kerahasiaannya. Pesan asli (*plaintext*) diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode (Jenni Hartati et al., 2022).

Perancangan aplikasi pengamanan data Medis menggunakan algoritma *Vigenere Cipher* dan LSB dalam konteks keamanan data masih membutuhkan pemahaman dan analisis yang mendalam. Oleh karena itu, penelitian ini bertujuan untuk menganalisis kinerja algoritma *Vigenere Cipher* dan LSB dalam mengamankan data medis. Dalam penelitian ini, peneliti akan merancang aplikasi pengamanan data medis menggunakan algoritma *Vigenere Cipher* dan LSB dalam sebuah website, melakukan pengujian, dan menganalisis hasil dari pengujian data medis tersebut pada sistem tersebut.

Untuk menambah tingkat keamanan, setelah data medis dienkripsi menggunakan algoritma *Vigenere Cipher*, hasil enkripsi tersebut akan diacak kembali menggunakan algoritma *Fisher-Yates Shuffle*. Algoritma *Fisher-Yates Shuffle* adalah algoritma untuk mengacak elemen-elemen dalam sebuah array atau daftar secara acak dan efisien. Algoritma ini bekerja dengan cara mengunjungi

setiap elemen dari akhir array hingga awal, dan pada setiap langkahnya, menukar elemen saat ini dengan elemen acak dari bagian yang belum diacak. Dengan cara ini, setiap elemen array memiliki peluang yang sama untuk berada di posisi manapun, menghasilkan pengacakan yang benar-benar acak dan merata. Kemudian pada teknik LSB disini peneliti akan memakai gambar *CT Scan* dan *Rontgen* sebagai gambar *cover* untuk menyisipkan data didalam file PDF tersebut

1.2 Rumusan Masalah Penelitian

Beberapa permasalahan yang telah dipaparkan sebelumnya, Peneliti merumuskan beberapa rumusan masalah dalam penelitian ini di antaranya:

1. Bagaimana merancang aplikasi Keamanan Data Medis menggunakan algoritma *Vigenere Cipher* dan teknik *Least Significant Bit* (LSB) berbasis web?
2. Bagaimana mengimplementasikan algoritma *Vigenere Cipher* dan teknik *Least Significant Bit* (LSB) dalam pengamanan Data Medis?
3. Bagaimana kinerja algoritma *Vigenere Cipher* dan *Least Significant Bit* (LSB) dalam hal pengamanan data medis?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dirumuskan sebelumnya, maka penelitian ini bertujuan untuk:

1. Merancang aplikasi yang mampu mengamankan suatu Data dengan mengintegrasikan algoritma *Vigenere Cipher* dan LSB.
2. Mengimplementasikan algoritma *Vigenere Cipher* dan teknik *Least Significant Bit* (LSB) dalam pengamanan Data Medis.
3. Untuk mengetahui kinerja algoritma *Vigenere Cipher* dan LSB dalam hal pengamanan data medis di dalam file, termasuk enkripsi ,dekripsi, *embedded*, ekstraksi, dan pengelolaan sumber daya.

1.4 Batasan Penelitian

Berdasarkan rumusan masalah yang telah dirumuskan sebelumnya, maka penelitian ini bertujuan untuk:

1. File PDF merupakan satu-satunya format yang dapat dimasukkan ke dalam program.
2. Format gambar PNG, JPG dan JPEG merupakan satu-satunya yang dapat digunakan sebagai gambar *cover*.
3. Hanya data berupa teks yang bisa dienkripsi dan dekripsi, jika ada gambar atau tabel didalam file maka tidak akan terbawa.
4. Output yang dihasilkan pada aplikasi ini setelah proses enkripsi dan penyisipan pada *cover image* adalah gambar berupa format PNG.
5. Gambar hasil radiologi yang digunakan sebagai gambar cover.
6. Aplikasi ini hanya bisa diakses oleh dokter dan perawat.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah dipaparkan sebelumnya, diharapkan penelitian ini dapat bermanfaat bagi perkembangan teknologi terutama di bidang *Network and Security*. Berikut beberapa manfaat dari penelitian ini diantaranya:

1.5.1 Manfaat Teoritis

Adapun manfaat teoritis dari penelitian ini yaitu:

1. Melalui rancangan aplikasi yang menggabungkan algoritma *Vigenere Cipher* dan *Least Significant Bit* (LSB), penelitian ini dapat memberikan wawasan tentang pengembangan metodologi keamanan yang dapat diterapkan pada jenis data khusus, seperti data medis.
2. Mengimplementasikan algoritma *Vigenere Cipher* dan teknik *Least Significant Bit* (LSB) dalam konteks keamanan data medis dapat membantu pengembangan teori dan praktik tentang penggunaan teknik kriptografi dan steganografi untuk melindungi data medis.
3. Memberikan kontribusi pada pemahaman teoritis dalam keamanan informasi dengan mengintegrasikan dua teknik kriptografi dan steganografi, yaitu algoritma *Vigenere Cipher* dan teknik *Least Significant Bit* (LSB). Ini membantu memperkuat keamanan data medis yang disimpan dalam file.

1.5.2 Manfaat Praktis

Adapun manfaat praktis dari penelitian ini yaitu:

1. Bagi Petugas Medis, Aplikasi ini dapat memberikan kontrol akses yang cermat, memungkinkan petugas medis untuk mengelola siapa yang memiliki hak akses terhadap data medis tertentu, sesuai dengan kebijakan privasi dan regulasi yang berlaku.
2. Bagi Pasien Layanan Kesehatan, Pasien dapat merasakan manfaat langsung dari tingkat keamanan yang tinggi, menjamin bahwa informasi medis pribadi mereka dijaga dengan ketat dan tidak mudah diakses oleh pihak yang tidak berwenang.
3. Bagi peneliti, Peneliti dapat mengimplementasikan pembelajaran dan pengalaman yang telah didapatkan selama masa perkuliahan berlangsung, Peneliti dapat mengembangkan jiwa kreatif dan inovatif peneliti dengan memadukan beberapa keilmuan secara sekaligus, yaitu Pemrograman Web dan *network security* yang tentunya akan bermanfaat bagi banyak pihak.

1.6 Struktur Organisasi Skripsi

Penelitian ini ditulis dengan pedoman yang sebagian besar mengacu pada Pedoman Penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun 2021. Sistematika penulisan penelitian ini adalah sebagai berikut:

1. PENDAHULUAN

Bagian Bab I ini memberikan penjelasan tentang latar belakang penelitian yang juga mencakup gap penelitian, rumusan masalah penelitian, tujuan penelitian, manfaat teoritis dan praktis, batasan masalah penelitian, hipotesis penelitian, dan struktur organisasi skripsi.

2. KAJIAN PUSTAKA

Kajian Pustaka membahas mengenai studi literatur terkait penelitian. Beberapa bagian dalam bab ini menjelaskan tentang konsep, metode, teori, dan teknologi yang digunakan.

3. METODOLOGI PENELITIAN

Metode Penelitian membahas tentang prosedur penelitian. Ini mencakup jenis dan metode penelitian yang digunakan, perancangan desain web, perancangan sistem, perancangan algoritma, teknik pengujian dan rencana analisis.

4. TEMUAN DAN PEMBAHASAN

Pada Bab IV Hasil dan Pembahasan akan memaparkan hasil yang diperoleh dari penelitian yang telah dilakukan, berupa hasil perancangan aplikasi, hasil pengembangan algoritma pada aplikasi pengamanan data medis dalam mempertahankan dan menjaga data medis.

5. SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Bab terakhir, yaitu Simpulan, Implikasi, dan Rekomendasi, yang merangkum temuan penelitian. Simpulan dari hasil penelitian disajikan, diikuti dengan pembahasan implikasi dari penggunaan enkripsi *Vigenere Cipher* dalam sistem pengamanan data medis berbasis web. Terakhir, penulis menyampaikan rekomendasi untuk pengembangan penelitian selanjutnya, memberikan arah bagi peneliti masa depan untuk mengembangkan konsep dan aplikasi lebih lanjut dalam bidang ini.