

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemilihan algoritma yang tepat merupakan faktor fundamental dalam memastikan efisiensi dan efektivitas berbagai proses komputasi di era digital saat ini. Beragam algoritma telah dikembangkan untuk berbagai keperluan, termasuk enkripsi data, yang masing-masing memiliki karakteristik spesifik dalam hal tingkat keamanan, kecepatan pemrosesan, dan penggunaan sumber daya. Namun, dalam praktiknya, pemilihan algoritma enkripsi masih menghadapi hambatan besar, terutama bagi pengguna maupun organisasi yang tidak memiliki latar belakang teknis yang kuat. Keterbatasan pemahaman mengenai parameter teknis, kelebihan, dan kekurangan masing-masing algoritma sering kali berujung pada pengambilan keputusan yang tidak optimal.

Permasalahan utama terletak pada banyaknya literatur ilmiah yang membahas enkripsi yang terus berkembang pesat, sehingga individu maupun organisasi memiliki keterbatasan waktu untuk mempelajari setiap perkembangan tersebut secara manual. Akibatnya, pemilihan algoritma sering kali hanya didasarkan pada popularitas atau rekomendasi umum tanpa mempertimbangkan kebutuhan spesifik data yang akan dilindungi. Kondisi ini sangat berisiko menimbulkan celah keamanan, inefisiensi pemrosesan data, hingga pemborosan sumber daya komputasi. Oleh karena itu, diperlukan sebuah pendekatan sistematis yang mampu memberikan rekomendasi berbasis analisis literatur ilmiah agar pengguna dapat mengambil keputusan secara cepat, tepat, dan didukung oleh data yang valid.

Salah satu solusi yang diusulkan dalam penelitian ini adalah pengembangan sistem rekomendasi berbasis *content-based filtering* yang terintegrasi dengan teknik *text mining*. Pendekatan ini memungkinkan sistem untuk menganalisis karakteristik teknis berbagai algoritma enkripsi yang tersedia dalam basis data literatur ilmiah, mengekstrak informasi yang relevan, dan mencocokkannya dengan kebutuhan pengguna secara akurat sesuai dengan studi dari Fahriani & Rosyid (2019). Berbeda dengan metode *collaborative filtering* yang bergantung pada opini

atau preferensi pengguna lain, *content-based filtering* jauh lebih cocok untuk domain keamanan informasi karena sistem menilai item berdasarkan parameter teknis fitur algoritma itu sendiri. Selain itu, metode ini mampu mengatasi masalah *cold-start*, di mana pengguna baru yang belum memiliki riwayat interaksi tetap bisa mendapatkan rekomendasi yang relevan berdasarkan masukan kriteria mereka.

Urgensi penggunaan *text mining* dalam penelitian ini didasarkan pada kemampuannya untuk mengolah teks dalam jumlah besar dan mengidentifikasi tren serta pola teknis yang sulit dideteksi melalui analisis manual. Melalui teknik ekstraksi kata kunci, sistem dapat mengintegrasikan data dari berbagai sumber seperti jurnal, artikel penelitian, dan laporan teknis untuk meningkatkan akurasi rekomendasi. Studi oleh Sholihuda et al (2022) membuktikan bahwa penerapan *text mining* dalam klasifikasi data mampu meningkatkan relevansi hasil rekomendasi secara signifikan. Selain itu, kombinasi *text mining* dengan kecerdasan buatan dapat mengoptimalkan proses pengambilan keputusan dalam pemilihan opsi terbaik, sebagaimana ditunjukkan dalam penelitian Kurniawan. R & Ikhsan (2023).

Dalam konteks enkripsi, tantangan pemilihan menjadi semakin kompleks karena setiap algoritma memiliki kekuatan yang bervariasi tergantung pada jenis data dan konteks penggunaannya. Sebagai contoh, algoritma simetris seperti AES (*Advanced Encryption Standard*) menonjol dalam hal kecepatan, namun algoritma asimetris seperti RSA (*Rivest-Shamir-Adleman*) mungkin lebih unggul dalam aspek keamanan kunci pada konteks tertentu. Melalui sistem rekomendasi yang mengintegrasikan *text mining* dan *content-based filtering*, pengguna dapat mengidentifikasi pilihan terbaik berdasarkan analisis kebutuhan spesifik individu secara personal.

Pengembangan sistem ini juga sangat relevan dengan tren global dalam meningkatkan kesadaran akan keamanan data di tengah meningkatnya intensitas serangan siber. Penelitian ini tidak hanya bertujuan untuk mengembangkan inovasi teknologi, tetapi juga memberikan edukasi bagi masyarakat luas, pengembang perangkat lunak, hingga organisasi sektor publik mengenai pentingnya pemilihan algoritma enkripsi yang tepat untuk melindungi informasi sensitif (Bhaskara et al., 2024).

Dengan adanya sistem yang memanfaatkan pendekatan berbasis data ini, diharapkan organisasi di berbagai sektor dapat meminimalisir risiko keamanan melalui keputusan yang didasarkan pada analisis konten ilmiah yang tervalidasi. Berdasarkan latar belakang tersebut, penulis tertarik untuk mengangkat penelitian tugas akhir dengan judul “Pemanfaatan *Text Mining* Pada Sistem Rekomendasi Pemilihan Algoritma Enkripsi Terbaik Untuk Keamanan Data Menggunakan *Content Based Filtering*”. Penelitian ini diharapkan mampu menghasilkan rekomendasi yang akurat serta memperluas pemahaman mengenai implementasi *text mining* dalam domain keamanan informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang diangkat dalam penelitian ini yaitu:

1. Bagaimana model implementasi *Text Mining* dalam menganalisis literatur ilmiah untuk mendukung ekstraksi fitur pada sistem rekomendasi enkripsi?
2. Bagaimana metode *Content-Based Filtering* dapat digunakan untuk memetakan kebutuhan pengguna terhadap algoritma enkripsi yang tersedia di dalam basis data literatur?
3. Bagaimana performa dan tingkat akurasi sistem dalam memberikan rekomendasi algoritma enkripsi berdasarkan hasil evaluasi metrik *Information Retrieval*?

1.3 Tujuan Penelitian

Berdasarkan latar belakang diatas, tujuan penelitian ini yaitu sebagai berikut:

1. Mengembangkan model implementasi *Text Mining* untuk mengekstrak informasi teknis dari literatur ilmiah secara otomatis guna mendukung basis data sistem rekomendasi.
2. Membangun sistem rekomendasi berbasis *Content-Based Filtering* yang mampu memberikan saran algoritma enkripsi yang relevan sesuai masukan pengguna.

3. Menganalisis akurasi sistem dalam memberikan rekomendasi melalui pengujian *Cosine Similarity* dan validasi terhadap literatur ilmiah.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini meliputi:

1. Mempermudah pemilihan algoritma enkripsi dengan menghadirkan sistem rekomendasi yang dapat mencocokkan kebutuhan pengguna dengan algoritma yang paling sesuai.
2. Meningkatkan efisiensi dalam pemilihan algoritma enkripsi, sehingga pengguna tidak perlu melakukan pencarian manual atau memiliki pemahaman teknis yang mendalam.
3. Mengurangi kesalahan dalam pemilihan algoritma karena sistem berbasis *Text Mining* dan *Content Based Filtering* akan memberikan rekomendasi yang berbasis data ilmiah.
4. Dapat dikembangkan lebih lanjut untuk mendukung rekomendasi algoritma dalam skenario yang lebih luas, seperti kemanan, jaringan, atau sistem penyimpanan data.
5. Bagi mahasiswa/i mempercepat literatur *review* untuk tugas akhir/mata kuliah kriptografi.
6. Bagi pengembang aplikasi membantu memilih algoritma enkripsi yang tepat untuk produk mereka tanpa perlu menjadi ahli kriptografi terlebih dahulu.
7. Bagi masyarakat sebagai solusi sederhana untuk meningkatkan kesadaran dan implementasi keamanan data dasar.

1.5 Ruang Lingkup dan Batasan Penelitian

Agar penelitian ini lebih terarah, terdapat beberapa ruang lingkup dan batasan yang diterapkan, yaitu:

1. Dataset yang digunakan dalam penelitian ini terdiri dari 300 jurnal penelitian dan literatur ilmiah yang membahas berbagai algoritma enkripsi.
2. Sistem yang dibuat berbasis web dan berfungsi sebagai sistem rekomendasi algoritma enkripsi data berdasarkan kebutuhan pengguna. Sistem ini

dirancang agar mudah digunakan dan dapat memberikan rekomendasi yang relevan sesuai dengan input pengguna.

3. Sistem merekomendasikan algoritma enkripsi berdasarkan data yang diperoleh dari jurnal penelitian dan literatur ilmiah yang membahas berbagai jenis algoritma enkripsi. Dengan demikian, rekomendasi yang diberikan bergantung pada informasi yang tersedia dalam sumber literatur yang dianalisis.
4. Analisis teks dilakukan dengan menggunakan teknik *Term Frequency-Inverse Document Frequency* (TF-IDF) untuk mengukur relevansi kata kunci dalam dokumen, serta *Cosine Similarity* untuk menentukan tingkat kesamaan antara kebutuhan pengguna dengan algoritma enkripsi yang tersedia.
5. Format dokumen yang didukung untuk analisis teks terbatas pada PDF dan TXT, memastikan kompatibilitas dengan jurnal penelitian dan literatur ilmiah yang digunakan dalam *dataset*.
6. Sistem ini dibuat menggunakan bahasa pemrograman *Python* dan *framework Flask* sebagai *backend* dan didukung oleh teknologi web *modern* untuk tampilan antarmuka yang interaktif dan *user-friendly*.
7. Evaluasi performa sistem dilakukan dengan mengukur akurasi rekomendasi berdasarkan relevansi hasil terhadap dataset literatur yang dianalisis.