BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, penggunaan sistem informasi berbasis web telah menjadi bagian integral dari berbagai sektor, baik pemerintahan, pendidikan, layanan publik, maupun bisnis. Digitalisasi yang masif ini mendorong meningkatnya volume data yang dikelola dan disimpan oleh berbagai organisasi. Namun, perkembangan ini diiringi dengan ancaman serius terhadap keamanan data, terutama data yang tersimpan di dalam database berbasis web. Salah satu kasus nyata adalah kebocoran data Tokopedia pada Maret 2020 yang melibatkan lebih dari 91 juta akun pengguna, dimana data nama, email, dan password tersedia di dark web[1]. Sebelumnya, insiden serupa juga terjadi pada platform Bhinneka.com pada Mei 2020, dengan pencurian data sekitar 1,2 juta pengguna yang diperjualbelikan oleh grup peretas ShinyHunter[2]. Permasalahan ini menunjukkan bahwa perlindungan data dalam database berbasis web tidak lagi dapat hanya mengandalkan keamanan jaringan atau aplikasi saja, melainkan harus menerapkan lapisan pengamanan tambahan melalui teknologi kriptografi untuk menjaga kerahasiaan dan integritas data yang tersimpan.

Salah satu bentuk serangan yang paling sering dimanfaatkan oleh peretas untuk mengakses data pada database berbasis web adalah SQL Injection. Serangan ini bekerja dengan cara menyisipkan perintah SQL berbahaya melalui input yang tidak tervalidasi dengan baik pada aplikasi web, sehingga peretas dapat memanipulasi atau membaca informasi yang seharusnya bersifat rahasia. Serangan SQL Injection sering terjadi karena lemahnya penerapan sanitasi input pada formulir atau kolom pencarian yang terhubung langsung dengan database. Dampak dari serangan ini sangat berbahaya, karena selain dapat mencuri data penting, peretas juga dapat menghapus atau mengubah isi database. Dalam skala yang lebih besar, SQL Injection bahkan dapat digunakan untuk mendapatkan akses administratif ke seluruh sistem aplikasi. Banyaknya insiden kebocoran data yang terjadi akibat serangan SQL Injection mempertegas pentingnya pengamanan

berlapis, khususnya dengan menerapkan mekanisme enkripsi pada data yang disimpan dalam database. Dengan menerapkan kriptografi, meskipun data berhasil dicuri melalui SQL Injection, informasi yang didapatkan hanyalah data terenkripsi yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai[3].

Selain SQL Injection, terdapat berbagai jenis ancaman lain yang secara langsung menyasar database berbasis web. Serangan brute force merupakan salah satu teknik yang digunakan untuk membobol kredensial login, terutama jika sistem tidak menerapkan kebijakan password yang kuat. Selain itu, terdapat pula ancaman pencurian data melalui malware atau spyware yang menyusup ke dalam sistem, serta eksploitasi celah keamanan pada perangkat lunak pendukung server database. Tidak jarang pula peretas memanfaatkan teknik social engineering untuk mendapatkan akses ke data sensitif. Ancaman-ancaman tersebut semakin berbahaya apabila data yang tersimpan tidak dilindungi dengan mekanisme pengamanan berbasis kriptografi. Data yang berhasil dicuri dalam bentuk plaintext dapat langsung digunakan oleh pihak yang tidak berwenang untuk berbagai tujuan ilegal, mulai dari penjualan data pribadi hingga penyalahgunaan informasi penting organisasi. Oleh karena itu, implementasi kriptografi menjadi langkah strategis yang tidak hanya memperkuat sistem keamanan, tetapi juga memberikan jaminan perlindungan terhadap kerahasiaan dan integritas data meskipun terjadi upaya akses ilegal terhadap database[4].

Penelitian ini secara khusus berfokus pada implementasi kriptografi simetris menggunakan algoritma Advanced Encryption Standard (AES) untuk meningkatkan keamanan database berbasis web. Algoritma AES dipilih karena telah terbukti kuat, cepat, dan efisien dalam proses enkripsi dan dekripsi data. AES merupakan standar enkripsi yang banyak digunakan dalam berbagai sistem informasi, baik pada skala kecil, menengah, maupun besar. Salah satu keunggulan utama dari algoritma ini adalah kemampuannya dalam menjaga keamanan data dengan tingkat efisiensi komputasi yang tinggi, sehingga tidak membebani sistem secara berlebihan. Sistem yang dirancang dalam penelitian ini akan melakukan proses enkripsi terhadap data yang akan disimpan ke dalam database. Dengan

demikian, apabila database berhasil diakses oleh pihak yang tidak berwenang, informasi yang didapatkan hanya berupa data dalam bentuk sandi atau cipher text, sehingga tidak memiliki arti tanpa kunci enkripsi yang sesuai. Selanjutnya, data yang telah dienkripsi tersebut akan didekripsi kembali ketika diakses oleh pengguna yang memiliki otorisasi dan hak akses.

1.2 Rumusan Masalah

Bagaimana mengimplementasikan kriptografi pada database berbasis web menggunakan algoritma Advanced Encryption Standard (AES) ?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan fokus, batasan masalah dalam penelitian ini adalah:

1. Sistem yang dibangun berupa aplikasi web sederhana untuk mendemonstrasikan proses enkripsi dan dekripsi data menggunakan algoritma AES.
2. Data yang diamankan merupakan data teks biasa (plaintext), tidak mencakup file atau data multimedia.
3. Pengujian dilakukan hanya pada algoritma AES tanpa membandingkan dengan algoritma kriptografi lainnya.
4. Sistem tidak mencakup manajemen kunci secara kompleks seperti key exchange atau key distribution berbasis PKI.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah :

1. Membangun sistem database berbasis web yang menerapkan algoritma AES untuk proses enkripsi dan dekripsi data.
2. Menunjukkan bagaimana penerapan algoritma AES dapat meningkatkan keamanan data dalam penyimpanan database.
3. Menyediakan referensi implementatif bagi pengembang sistem yang ingin mengamankan data menggunakan kriptografi simetris.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah:

1. Manfaat Teoritis:

   Secara teoritis, hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang keamanan informasi, khususnya terkait penerapan algoritma kriptografi simetris pada sistem basis data berbasis web. Penelitian ini juga dapat menambah literatur dan referensi bagi mahasiswa, peneliti, maupun akademisi yang tertarik mempelajari lebih dalam mengenai penerapan algoritma Advanced Encryption Standard (AES) dalam konteks pengamanan data. Dengan adanya penelitian ini, diharapkan dapat memperkaya kajian ilmiah terkait konsep, implementasi, dan penerapan kriptografi pada sistem informasi.

2. Manfaat Praktis:

   Secara praktis, penelitian ini diharapkan dapat memberikan solusi teknis bagi pengembang aplikasi dan sistem informasi dalam meningkatkan keamanan data pada sistem database berbasis web. Dengan menerapkan algoritma AES, pengembang dapat memiliki acuan atau contoh implementasi enkripsi data yang efektif untuk mencegah akses tidak sah terhadap data yang tersimpan. Selain itu, penelitian ini juga dapat menjadi bahan pertimbangan bagi instansi atau organisasi dalam menerapkan langkah-langkah pengamanan data, khususnya pada aspek perlindungan data sensitif yang tersimpan dalam database.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi gambaran umum mengenai latar belakang permasalahan yang mendasari dilakukannya penelitian, rumusan masalah, tujuan penelitian, batasan penelitian, metode penelitian, manfaat penelitian, serta sistematika penulisan. Latar belakang penelitian menjelaskan urgensi pengamanan data dalam sistem database

berbasis web, khususnya melalui penerapan algoritma kriptografi AES. Bagian ini juga menegaskan relevansi topik penelitian dengan kondisi terkini terkait keamanan data digital.

BAB II TINJAUAN PUSTAKA

Bab ini membahas landasan teori yang mendukung penelitian, meliputi konsep dasar kriptografi, algoritma Advanced Encryption Standard (AES), database berbasis web, serta kajian dari penelitian-penelitian terdahulu yang relevan. Teori dan literatur yang disajikan menjadi dasar untuk membangun pemahaman tentang bagaimana penerapan kriptografi dapat meningkatkan keamanan data dalam database.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan tentang tahapan perancangan sistem yang meliputi desain proses enkripsi dan dekripsi data dengan algoritma AES, alur sistem, serta spesifikasi kebutuhan perangkat keras dan perangkat lunak. Perancangan ini bertujuan untuk memastikan bahwa integrasi algoritma kriptografi dengan sistem database berbasis web dapat dilakukan secara optimal dan efektif.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan proses implementasi algoritma AES dalam sistem database berbasis web. Selain itu, disajikan pula hasil pengujian terhadap proses enkripsi dan dekripsi data untuk mengukur efektivitas penerapan algoritma tersebut.

BAB V PENUTUP

Bab terakhir berisi kesimpulan dari hasil penelitian yang telah dilakukan, serta saran untuk pengembangan lebih lanjut. Kesimpulan disusun berdasarkan hasil implementasi dan pengujian yang telah dilakukan, sedangkan saran ditujukan untuk penelitian mendatang agar dapat mengembangkan metode pengamanan data yang lebih baik.