BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital yang semakin berkembang pesat, keamanan data menjadi komponen yang sangat penting, khususnya dalam pengelolaan basis data (database). Berdasarkan hasil penelitian yang dipublikasikan dalam jurnal *Database Security Threats and How to Mitigate Them*, tahun 2021 tercatat sebanyak 1.243 insiden pelanggaran keamanan yang menyebabkan lebih dari 5,1 miliar data terekspos. Jumlah tersebut menunjukkan kenaikan sekitar 11% jika dibandingkan dengan tahun sebelumnya [1]. Kondisi ini menunjukkan bahwa penerapan metode pengamanan data, seperti algoritma kriptografi RSA dan AES, sangat dibutuhkan guna menjaga keutuhan serta kerahasiaan informasi yang tersimpan dalam database.

Database digunakan untuk menyimpan dan memproses berbagai jenis data, termasuk informasi sensitif. Namun, dengan meningkatnya penggunaan teknologi informasi juga meningkatkan ancaman terhadap keamanan data seperti, kebocoran dan akses tidak sah. Kasus-kasus kebocoran data yang melibatkan platform besar menunjukkan bahwa ancaman terhadap keamanan data dapat berdampak luas pada kepercayaan pengguna dan stabilitas operasional platform digital. Oleh karena itu, diperlukan solusi keamanan yang efektif untuk melindungi data dari potensi ancaman tersebut [2].

Selain insiden kebocoran data berskala besar seperti yang telah disebutkan, serangan *SQL Injection* menjadi salah satu ancaman utama yang kerap menargetkan sistem basis data. Metode ini memanfaatkan kelemahan pada input yang diberikan pengguna untuk menyisipkan perintah *SQL* berbahaya yang berpotensi merusak, memodifikasi, atau mencuri data penting yang tersimpan dalam database. Berdasarkan penelitian Natanael, Felicia, dan Sakti (2023), teknik *SQL Injection* merupakan salah satu cara eksploitasi yang efektif dalam menguasai kendali database pada situs web, sehingga dapat menimbulkan kerugian signifikan baik dari

sisi data maupun kepercayaan pengguna. Oleh sebab itu, penting untuk menerapkan validasi input yang ketat dan menggunakan *query parameterized* sebagai langkah utama dalam memperkuat keamanan aplikasi web terhadap serangan ini [3].

Kriptografi merupakan salah satu metode yang umum dipakai untuk mengamankan data melalui proses enkripsi dan dekripsi. Dalam penerapannya, kombinasi algoritma RSA dan AES sering digunakan untuk meningkatkan keamanan data. Algoritma RSA yang bersifat asimetris digunakan untuk mengamankan distribusi kunci enkripsi, sementara AES yang bersifat simetris berfungsi untuk mengenkripsi data secara efisien. Dengan menggabungkan kedua algoritma tersebut, sistem dapat memanfaatkan keunggulan masing-masing sehingga menjaga kerahasiaan, integritas, dan keamanan data dalam proses penyimpanan maupun pengiriman [4].

Penelitian sebelumnya menunjukkan bahwa algoritma RSA efektif dalam mengamankan data, namun lambat dalam mengenkripsi file berukuran besar. Di sisi lain, AES jauh lebih cepat dalam proses enkripsi dan dekripsi karena bekerja dengan kunci simetris. Penggabungan kedua algoritma ini, di mana RSA digunakan untuk mengenkripsi kunci AES dan AES digunakan untuk mengenkripsi data itu sendiri, sehingga dapat mengatasi keterbatasan masing-masing algoritma [5].

Aplikasi web lokal yang dikembangkan dalam penelitian ini dirancang untuk melakukan enkripsi dan dekripsi file secara otomatis setelah file diunggah. Aplikasi ini menggunakan kombinasi algoritma RSA dan AES untuk mengamankan data. RSA digunakan untuk mengenkripsi kunci AES, sedangkan AES digunakan untuk mengenkripsi data, sehingga menciptakan sistem yang aman dan efisien. Aplikasi ini mendukung berbagai format file, termasuk PNG, JPG, PDF, DOCX, TXT, dan MP4. Hal ini memungkinkan fleksibilitas dalam mengamankan berbagai jenis dokumen dan media yang sering digunakan dalam aplikasi web [6].

Dalam pengambilan keputusan multikriteria, penggunaan metode AHP atau SAW secara tunggal menghasilkan hasil yang kurang optimal. Metode AHP memiliki keunggulan dalam menetapkan bobot berdasarkan perbandingan antar

kriteria secara sistematis, tetapi belum maksimal dalam memberikan hasil akhir dalam pemilihan alternatif secara langsung. Metode SAW efektif dalam melakukan perangkingan terhadap alternatif berdasarkan bobot yang telah ditentukan, tetapi cenderung rentan terhadap bias apabila bobot kriteria ditetapkan secara subjektif. Oleh karena itu, kombinasi kedua metode menjadi pendekatan yang saling melengkapi: Metode AHP digunakan untuk menentukan bobot kriteria secara konsisten, sementara metode SAW digunakan untuk menghitung nilai akhir dari setiap alternatif berdasarkan bobot tersebut. Pendekatan kombinasi metode telah terbukti efektif melalui penelitian sebelumnya yang menunjukkan bahwa sistem pendukung keputusan menjadi lebih akurat dan mampu membantu pengguna dalam menentukan hasil sesuai kebutuhan [7].

Penelitian ini difokuskan pada penilaian efektivitas penggunaan kombinasi algoritma RSA dan AES terhadap tiga jenis data, yaitu terenkripsi, terdekripsi, dan tidak terenkripsi. Penilaian dilakukan menggunakan metode AHP dan SAW dengan mengukur beberapa parameter kinerja sistem, seperti waktu pemrosesan (meliputi waktu enkripsi dan waktu tanpa enkripsi), penggunaan CPU, konsumsi memori atau RAM, serta throughput. Evaluasi ini bertujuan untuk menilai sejauh mana penerapan kombinasi kedua algoritma tersebut memengaruhi efisiensi sistem dalam pengolahan data melalui aplikasi web [4].

Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem keamanan data yang lebih efektif dalam aplikasi berbasis web, terutama dalam konteks pengolahan file berukuran besar secara lokal. Efektivitas sistem tidak hanya dilihat dari sisi perlindungan data, tetapi juga dari performa teknisnya dalam memproses file secara efisien, baik dari segi kecepatan pemrosesan maupun penggunaan sumber daya sistem. Pendekatan ini juga memberikan gambaran yang lebih menyeluruh terhadap dampak integrasi algoritma kriptografi terhadap kinerja aplikasi secara real-time, sehingga dapat dijadikan acuan dalam perancangan sistem serupa di masa mendatang.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mengimplementasikan algoritma RSA dan AES pada transaksi data di database ?
2. Bagaimana mengevaluasi kinerja terenkripsi, terdekripsi dan tidak terenkripsi dengan menggunakan metode AHP dan SAW ?

1.3 Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan yang ditetapkan untuk memperjelas ruang lingkup penelitian:

1. Aplikasi web yang dikembangkan hanya dijalankan secara lokal dan tidak diimplementasikan dalam lingkungan berbasis cloud atau jaringan publik.
2. Algoritma enkripsi yang digunakan terbatas pada kombinasi RSA dan AES, tanpa membandingkan dengan algoritma enkripsi lainnya.
3. Pengujian dilakukan dengan beberapa format file, yaitu PNG, JPG, PDF, DOCX, TXT, dan MP4, dengan ukuran file yang bervariasi.
4. Analisis hanya difokuskan pada menentukan nilai efektivitas antara data yang terenkripsi, data yang terdekripsi dan data yang tidak terenkripsi menggunakan metode AHP dan SAW tanpa mempertimbangkan faktor keamanan dari masing-masing algoritma secara mendalam.
5. Sistem yang dikembangkan tidak melibatkan mekanisme otentikasi pengguna atau sistem manajemen akses, melainkan hanya berfokus pada proses enkripsi dan dekripsi file.
6. Belum berhasil dalam mengembalikan data pribadi dalam proses dekripsi.
7. Batas ukuran file pengujian hanya berkisar kurang dari 50 MB.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Mengimplementasikan algoritma RSA dan AES untuk mengenkripsi dan mendekripsi serta transaksi data dalam database.
2. Menentukan nilai efektifitas dari penggunaan kombinasi algoritma RSA dan AES pada data terenkripsi, terdekripsi dan tidak terenkripsi dengan mengukur parameter seperti waktu (waktu enkripsi dan waktu tidak enkripsi), cpu, memory/ram, dan throughput dengan menggunakan metode AHP dan SAW.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini dapat dilihat dari dua sisi, yaitu manfaat teknis dan manfaat praktis:

1. Secara teknis, penelitian ini memberikan wawasan mengenai implementasi kombinasi algoritma RSA dan AES dalam proses enkripsi dan dekripsi file pada aplikasi web. Penelitian ini juga efisien dalam evaluasi performa sistem berdasarkan beberapa parameter, seperti waktu pemrosesan, penggunaan CPU, memori/RAM, dan throughput dengan menggunakan metode AHP dan SAW.
2. Secara praktis, aplikasi web yang dikembangkan dapat dimanfaatkan oleh berbagai pihak seperti institusi pendidikan, perusahaan, maupun individu yang memerlukan sistem perlindungan data. Selain itu, penelitian ini memberikan pemahaman yang lebih mendalam mengenai perbandingan efektivitas antara data terenkripsi, tidak terenkripsi, dan terdekripsi, sehingga hasil pengembangan aplikasi dapat dioptimalkan untuk mencapai keseimbangan antara aspek keamanan dan efisiensi kinerja sistem.
3. Manfaat Pengembangan Ilmu Pengetahuan: Penelitian ini turut memberikan kontribusi terhadap pengembangan sistem keamanan data berbasis web, khususnya yang menggabungkan kriptografi RSA dan AES. Hasil dari penelitian ini diharapkan dapat menjadi acuan bagi penelitian lebih lanjut

untuk mengembangkan sistem enkripsi yang lebih efektif dan efisien dalam pengolahan data yang aman.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut:

- BAB I PENDAHULUAN: Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
- BAB II TINJAUAN PUSTAKA: Membahas teori-teori yang relevan dengan penelitian ini, seperti teori dasar algoritma RSA dan AES, enkripsi dan dekripsi file, serta aplikasi web.
- BAB III METODE PENELITIAN: Menguraikan metode penelitian yang digunakan, termasuk identifikasi masalah, studi literatur, perancangan sistem, implementasi algoritma RSA dan AES, pengembangan aplikasi web, pengujian.
- BAB IV HASIL DAN PEMBAHASAN: Membahas hasil penelitian yang meliputi pengembangan aplikasi web, integrasi algoritma RSA dan AES, serta pengujian yang telah dilakukan.
- BAB V PENUTUP: Berisi kesimpulan dan saran yang diperoleh dari penelitian ini.