

BAB II

TINJAUAN LITERATUR

2.1 Penelitian Terkait

Dibawah ini adalah beberapa penelitian yang memiliki kesamaan dan perbedaan dengan penelitian sekarang.

Dalam penelitian Rizki Tahun (2021) yang berjudul “Penerapan Kriptografi Dengan Menggunakan Algoritma RSA Untuk Pengamanan Data Berbasis Desktop Pada PT Trias Mitra Jaya Manunggal”. PT Trias Mitra Jaya Manunggal memberi Anda layanan mesin hitung uang, mesin sortir, dan perawatan dan perawatan. Perusahaan ini mempunyai data sensitif mengenai jumlah mesin, lokasi bank yang menggunakan mesin, dan harga sewa mesin. Untuk menjaga kerahasiaan data ini dari pesaing, diperlukan perlindungan data yang kuat. Oleh karena itu, diperlukan penggunaan kriptografi dengan algoritma RSA untuk mengamankan pertukaran informasi. Kriptografi adalah teknik untuk mengamankan data dengan mengubahnya menggunakan kunci, sehingga sulit dibaca tanpa dekripsi. Sebuah aplikasi telah dikembangkan menggunakan Java untuk mengamankan data, yang telah berhasil mengubah teks asli menjadi teks terenkripsi (*chipertext*). Kecepatan aplikasi tergantung pada ukuran file yang diolah (Rizki, Muhamad & Teknik, 2021).

Dalam penelitian anwar tahun (2022) yang berjudul “Analisis Performa Kriptografi *Hybrid* Algoritma *Blowfish* Dan Algoritma RSA”.

Perlindungan data komputer terfokus pada mencegah akses ilegal ke informasi, dan salah satu metode yang umum digunakan adalah kriptografi. Penelitian ini bertujuan untuk mengevaluasi kecepatan kriptografi gabungan yang menggabungkan algoritma simetris seperti *Blowfish* dan algoritma asimetris seperti RSA. Penelitian ini mencakup berbagai jenis file seperti video, foto, audio, dan dokumen. Pembuktian penelitian menunjukkan bahwa kinerja dari algoritma kriptografi gabungan ini serupa dengan algoritma Blowfish, dengan keamanan tambahan yang disediakan oleh RSA. (Anwar et al., 2019).

Dalam penelitian Christian (2023) yang berjudul “Implementasi Algoritma RSA Dan *One Time Password* (OTP) Untuk Pengamanan Data Pengguna Dan Proses Transaksi Pada Website *E-Commerce*”. Teknologi yang maju dan luasnya penyebaran informasi telah mempermudah banyak hal, namun disayangkan bahwa kecanggihan tersebut sering disalahgunakan untuk kejahatan, terutama dalam hal keamanan data. Pada serangkaian kejadian yang melibatkan kebocoran, pencurian, dan penjualan data pengguna dalam jumlah besar dari situs *e-commerce*. Kejadian ini terjadi karena kurangnya langkah-langkah untuk melindungi data tersebut. Sebagai respon, penelitian dilakukan untuk membangun sistem keamanan pada situs *e-commerce* menggunakan Algoritma RSA dan *One Time Password* (OTP). RSA digunakan untuk mengamankan basis data dengan melakukan proses enkripsi dan dekripsi data, sementara OTP digunakan untuk melindungi proses registrasi, login, dan transaksi

dengan memverifikasi kode OTP. Pengujian sistem tersebut berhasil melindungi data 30 pengguna dengan menyimpannya dalam bentuk *ciphertext* yang dapat diubah kembali menjadi *plaintext*. Namun, beberapa *ciphertext* memiliki kombinasi angka yang sama karena rentang nilai bilangan prima yang digunakan untuk pembangkitan kunci masih terbatas. Penggunaan OTP juga berhasil dalam melindungi transaksi dengan syarat bahwa verifikasi akan berhasil hanya jika kode OTP yang dimasukkan benar dan masa berlaku kode tersebut belum berakhir (Christian et al., 2023).

Dalam penelitian Gunawan (2020) yang berjudul “Kombinasi Algoritma Caesar Cipher Dan Algoritma RSA Untuk Pengamanan File Dokumen Dan Pesan Teks”. Saat ini, perkembangan pesat dalam bidang ilmu komputer dan telekomunikasi telah menyoroti pentingnya keamanan data. Menjaga kerahasiaan informasi penting dari ancaman potensial merupakan prioritas utama. Dengan menambahkan tingkat keamanan melalui penggunaan gabungan algoritma, memastikan bahwa informasi yang disimpan aman dari upaya merusak oleh pihak yang tidak bertanggung jawab. Khususnya, perlindungan data dalam format dokumen dan pesan teks telah ditingkatkan menggunakan gabungan algoritma *Caesar Cipher* dan RSA. Dengan menerapkan kedua algoritma ini, keaslian dan integritas data dalam file dokumen dan pesan teks dapat dijaga dengan lebih baik (Gunawan, n.d.).

Dalam penelitian Ernanda tahun (2020) yang berjudul “Penerapan

Algoritma *Rice Codes* dan Algoritma Rivest Shamir Adleman (RSA) Untuk Kompresi dan Pengamanan Teks Pada Aplikasi *Chatting*". keamanan juga menjadi hal yang penting dalam pengiriman pesan teks melalui aplikasi *chatting*. Pesan yang dikirimkan harus terjamin keasliannya dan tidak boleh berubah selama proses pengiriman. Untuk mengatasi hal ini, diperlukan penggunaan algoritma pengamanan seperti *Rice Codes* dan RSA dalam aplikasi *chatting*. Hal ini memastikan bahwa pesan yang dikirimkan tetap terjaga keasliannya dan tidak dapat dimanipulasi oleh pihak yang tidak bertanggung jawab. Dengan menerapkan teknologi ini, aplikasi *chatting* dapat memberikan solusi atas berbagai kendala dalam berkomunikasi, terutama yang terkait dengan jarak dan waktu. Dengan menggunakan algoritma kompresi dan pengamanan, aplikasi *chatting* dapat memfasilitasi komunikasi efektif antara individu yang berjarak jauh, menjadikan proses berkomunikasi menjadi lebih mudah dan efisien (Ernanda et al., 2020).

Dari penelitian di atas algoritma RSA dapat mengamankan data dengan mengubahnya menggunakan kunci agar sulit dibaca mengubah teks asli menjadi teks terenkripsi (ciphertext), kriptografi menggunakan kombinasi angka yang sama karena rentang nilai bilangan prima terbatas. RSA meningkatkan perlindungan data, menjaga keaslian dan integritas data. Nah maka dari itu penelitian ini menggunakan algoritma RSA dalam mengamankan data penjualan sehingga data penjualan menjadi lebih aman dan memudahkan perusahaan untuk mengamankan data penjualan.