

ANALISIS DAN IMPLEMENTASI ALGORITMA RSA UNTUK KEAMANAN TRANSAKSI PEMBAYARAN PADA SISTEM E-COMMERCE DI TOKO BANGUN JAYA

Irfan, Mochammad Darip*, Sigit Auliana

Program Studi Ilmu Komputer, Universitas Bina Bangsa
Jl. Raya Serang – Jakarta, KM. 03 No. 1B, Pakupatan, Kota Serang, Banten
Banten Kode Pos 42124
darif.uniba@gmail.com

ABSTRAK

Masalah keamanan data pelanggan menjadi perhatian penting bagi Toko Bangun Jaya, terutama dengan meningkatnya ancaman kebocoran data. Kebocoran data pelanggan tidak hanya mengakibatkan kerugian finansial, tetapi juga menurunkan tingkat kepercayaan pelanggan. Algoritma RSA, sebagai metode enkripsi asimetris yang menggunakan pasangan kunci publik dan privat untuk mengamankan data, menjadi solusi dalam menjaga kerahasiaan informasi pelanggan serta transaksi. Penelitian ini bertujuan menerapkan algoritma RSA dalam sistem e-commerce, dengan metode penelitian menggunakan pendekatan kualitatif untuk analisis risiko keamanan dengan fokus pada implementasi algoritma enkripsi RSA, dan pendekatan kuantitatif untuk mengukur efektivitas penerapan algoritma RSA pada sistem informasi tersebut. Berdasarkan hasil analisis, sistem e-commerce Toko Bangun Jaya yang saat ini berjalan masih memiliki kerentanan terhadap potensi ancaman keamanan, terutama dalam perlindungan data pelanggan dan transaksi pembayaran. Namun, Setelah mengimplementasikan algoritma RSA, hasil evaluasi menunjukkan bahwa penerapan algoritma RSA pada e-commerce Toko Bangun Jaya telah berhasil meningkatkan keamanan transaksi tanpa mengorbankan pengalaman pengguna. Hal ini terlihat dari hasil survey feedback pengguna, 85% merasa lebih aman melakukan transaksi setelah mengetahui bahwa data mereka dienkripsi dengan RSA, 75% pengguna tidak merasakan perbedaan signifikan dalam kecepatan transaksi dan 90% pengguna setuju bahwa implementasi sistem keamanan ini meningkatkan kepercayaan mereka terhadap Toko Bangun Jaya sebagai platform e-commerce.

Kata kunci: Algoritma, Digital, E-Commerce, Keamanan, Pengembangan, RSA

1. PENDAHULUAN

Dalam era transformasi digital, e-commerce telah menjadi salah satu pilar penting dalam perdagangan global, hal seiring dengan perkembangan teknologi dan perubahan perilaku konsumen yang semakin bergantung pada platform digital [1].

Selain itu, kemudahan akses, efisiensi transaksi, serta beragam pilihan produk dan layanan telah mendorong pertumbuhan industri ini secara pesat. Namun, di balik kemajuan tersebut, muncul masalah besar terkait keamanan data, hal ini yang menjadi perhatian utama bagi para penggunanya [2].

Risiko seperti pencurian informasi pribadi, kebocoran data transaksi, serta serangan siber yang semakin canggih dapat menimbulkan dampak serius, salah satunya kepercayaan pelanggan yang akan berakibat pada potensi kerugian finansial [3].

Oleh karena itu, implementasi sistem keamanan yang kuat, seperti enkripsi data, autentikasi berlapis, serta kepatuhan terhadap regulasi perlindungan data, menjadi langkah penting dalam memastikan kelangsungan ekosistem e-commerce yang aman dan terpercaya.

Toko Bangun Jaya, berlokasi di Kabupaten Serang yang merupakan salah satu e-commerce lokal yang bergerak dalam usaha penjualan bahan bangunan. Meski sebagai pendatang baru dalam hal transformasi perdagangan digital, tetapi perusahaan turut perhatian dalam menjaga keamanan data pelanggan demi memastikan kelancaran transaksi digital dan

operasional usahanya. Sebagai platform yang melayani kebutuhan masyarakat, Toko Bangun Jaya terus berupaya mengadopsi teknologi keamanan untuk melindungi informasi pengguna sekaligus meningkatkan kepercayaan pelanggan. Meskipun sudah memiliki website sebagai sarana utama dalam melayani pelanggan secara online, Toko Bangun Jaya terus melakukan pengembangan untuk meningkatkan pengalaman pengguna. Perusahaan berkomitmen untuk menghadirkan sistem yang lebih responsif, ramah pengguna, serta dilengkapi dengan fitur keamanan tambahan seperti enkripsi data.

Untuk mewujudkan komitmen tersebut, maka diperlukan langkah-langkah strategis dalam mengimplementasikannya. Salah satu rekomendasi yang peneliti usulkan adalah dengan menerapkan algoritma RSA sebagai metode enkripsi data pelanggan ke dalam sistem yang saat ini berjalan. Algoritma ini dipilih karena keunggulannya dalam menjaga kerahasiaan dan integritas informasi yang dikirimkan antara pengguna dan server [4].

Langkah-langkah penelitian yang dilakukan mencakup analisis risiko keamanan pada sistem e-commerce Toko Bangun Jaya, perancangan model enkripsi berbasis RSA, implementasi serta pengujian efektivitas sistem terhadap potensi ancaman siber. Tujuan utama dari penelitian ini adalah meningkatkan perlindungan data pelanggan, mengurangi risiko kebocoran informasi, serta memperkuat kepercayaan pengguna terhadap platform e-commerce Toko

Bangun Jaya dalam menjalankan transaksi digital secara aman dan andal.

Dengan diterapkannya algoritma RSA dalam sistem transaksi pembayaran Toko Bangun Jaya, diharapkan tingkat keamanan data pelanggan dapat lebih terjamin, terutama dalam proses enkripsi informasi sensitif seperti detail pembayaran dan identitas pelanggan. Analisis terhadap efektivitas metode ini juga akan memberikan wawasan mengenai sejauh mana RSA dapat mengatasi berbagai ancaman keamanan yang mungkin terjadi di lingkungan e-commerce. Melalui penelitian ini, diharapkan hasil yang diperoleh dapat menjadi dasar bagi pengembangan sistem keamanan yang lebih baik khususnya di Toko Bangun Jaya.

Penerapan algoritma RSA ke dalam sistem keamanan sudah banyak diimplementasikan oleh para peneliti sebelumnya, salah satunya adalah penelitian yang dilakukan oleh Wahdini, dkk pada tahun 2021 dengan judul penelitiannya Pengamanan Data Pelanggan dan Penjualan Menggunakan Algoritma Kriptografi RSA di PT. Sutan Indo Aneka Mobil Pematangsiantar. Dalam penelitian ini, data pelanggan dan penjualan dienkripsi menggunakan kunci RSA sepanjang 1024 bit. Hasil pengujiannya menunjukkan bahwa algoritma RSA efektif digunakan untuk mengamankan data dengan ukuran file yang tidak terlalu besar, seperti data pelanggan dan penjualan. Implementasi ini berhasil meningkatkan keamanan data yang dikirim, sehingga data tersebut terlindungi dari akses oleh pihak ketiga yang tidak berwenang [5].

Selain itu, penelitian lainnya yang telah menerapkan algoritma RSA yaitu penelitian yang berjudul Evaluasi Kuantitatif Penggunaan Algoritma RSA pada Aplikasi Shopee Pay: Kecepatan vs Keamanan, oleh Keysha, dkk pada tahun 2024. Tujuan dari penelitiannya yaitu untuk menilai dampak ukuran kunci RSA terhadap kecepatan dan keamanan transaksi pada aplikasi Shopee Pay. Hasil penelitiannya menunjukkan bahwa pemilihan ukuran kunci RSA harus mempertimbangkan keseimbangan antara kecepatan dan keamanan sesuai dengan kebutuhan spesifik aplikasi. Untuk aplikasi seperti Shopee Pay, kunci 1024-bit dianggap optimal karena menawarkan kombinasi yang baik antara kecepatan transaksi dan tingkat keamanan yang memadai [6].

Namun, untuk transaksi yang memerlukan tingkat keamanan lebih tinggi, penggunaan kunci 2048-bit dapat dipertimbangkan meskipun dengan kompromi pada kecepatan pemrosesan. Dari kedua contoh penelitian di atas, dalam penelitian ini, mencoba mengisi kesenjangan dengan menitikberatkan pada implementasi sistem keamanan data pelanggan dalam e-commerce lokal yang masih dalam tahap pengembangan, berbeda dengan penelitian sebelumnya yang lebih fokus pada efektivitas enkripsi terhadap data pelanggan atau optimasi keseimbangan antara kecepatan dan keamanan dalam transaksi digital. Selain itu, penelitian ini tidak hanya menguji efektivitas

algoritma RSA dalam melindungi informasi sensitif, tetapi juga menganalisis risiko keamanan yang dihadapi oleh e-commerce lokal serta merancang strategi penerapannya secara langsung dalam sistem yang sedang berjalan. Dengan pendekatan ini, penelitian ini berkontribusi pada penguatan sistem keamanan yang lebih kontekstual bagi usaha berbasis digital yang baru bertransformasi ke ranah e-commerce.

2. TINJAUAN PUSTAKA

2.1. E-Commerce

E-commerce merupakan suatu model bisnis yang memanfaatkan teknologi internet untuk melakukan transaksi jual beli barang dan jasa secara elektronik [7].

Menurut Laudon dan Traver (2020), e-commerce telah menjadi bagian integral dari ekonomi digital, memungkinkan perusahaan untuk memperluas pasar dan meningkatkan efisiensi bisnis melalui otomatisasi transaksi [8].

E-commerce telah mengalami perkembangan pesat seiring dengan kemajuan teknologi digital dan perubahan pola konsumsi masyarakat. Platform perdagangan elektronik ini menawarkan berbagai keunggulan, seperti kemudahan akses, efisiensi transaksi, serta beragam pilihan produk dan layanan yang dapat diakses secara luas tanpa batasan geografis. Menurut beberapa penelitian, keberhasilan e-commerce sangat bergantung pada faktor kepercayaan pelanggan, yang dipengaruhi oleh aspek keamanan, kenyamanan, serta keandalan sistem pembayaran.

2.2. Sistem Keamanan Digital

Keamanan digital merupakan aspek penting dalam sistem informasi modern, terutama dalam transaksi berbasis elektronik. Menurut Stallings sistem keamanan digital mencakup prinsip kerahasiaan, integritas, dan autentikasi untuk melindungi data dari ancaman eksternal maupun internal [9].

Salah satu metode yang banyak digunakan untuk menjaga keamanan informasi adalah kriptografi, yang memungkinkan data dienkripsi sehingga hanya pihak yang berwenang dapat mengaksesnya. Pada tahun 1978 Rivest, Shamir, dan Adleman mengembangkan algoritma RSA, yaitu sebuah metode enkripsi asimetris yang mengandalkan konsep faktorisasi bilangan prima untuk menjaga keamanan data [10].

Dan pada tahun 2015, seorang ilmuwan bernama Schneier mengatakan “algoritma RSA efektif dalam mengamankan transaksi digital karena menggunakan dua kunci berbeda, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi, sehingga meningkatkan keamanan dalam proses pengiriman informasi sensitif” [11].

Dengan mempertimbangkan efektivitas algoritma RSA dalam menjaga keamanan informasi, penelitian ini berfokus pada analisis dan implementasi RSA dalam sistem pembayaran e-commerce Toko Bangun Jaya guna meningkatkan perlindungan

transaksi serta menjaga kepercayaan pelanggan dalam ekosistem digital.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif untuk analisis resiko keamanan dengan fokus pada implementasi algoritma enkripsi RSA dalam sistem e-commerce lokal (Toko Bangun Jaya), dan pendekatan kuantitatif untuk mengukur efektivitas penerapan algoritma RSA pada sistem informasi tersebut. Adapun langkah-langkah penelitiannya adalah sebagai berikut:

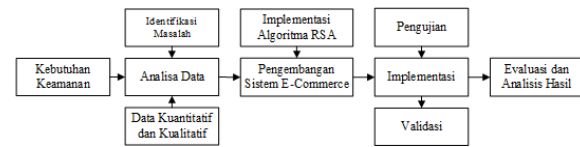
- Analisis Risiko Keamanan pada Sistem E-Commerce Toko Bangun Jaya: Mengidentifikasi potensi ancaman keamanan data pelanggan, melakukan evaluasi terhadap sistem keamanan yang sudah berjalan, serta menganalisis kebutuhan enkripsi pada sistem transaksi dan penyimpanan data pelanggan [12].
- Pengembangan Sistem dan Perancangan Model Enkripsi RSA untuk Keamanan Data: Menentukan skema enkripsi RSA yang digunakan, mendesain arsitektur sistem untuk mengintegrasikan algoritma RSA ke dalam transaksi e-commerce, dan menentukan proses enkripsi dan dekripsi data pelanggan dalam transaksi digital [13].
- Implementasi Algoritma RSA dan Validasi Sistem: Menerapkan algoritma RSA pada sistem pembayaran dan penyimpanan data pelanggan, dan mengintegrasikan sistem enkripsi ke dalam website Toko Bangun Jaya [14].
- Evaluasi dan Analisis Hasil: Melakukan pengujian fungsionalitas sistem dengan metode balckbox testing, Menganalisis performance dampak penerapan RSA terhadap kecepatan transaksi dan keamanan data, serta memberikan rekomendasi terkait peningkatan sistem keamanan di masa depan [15].

Langkah-langkah di atas disusun secara sistematis dan terstruktur dengan harapan dapat:

- Meningkatkan keamanan data pelanggan pada Toko Bangun Jaya.
- Mengurangi risiko kebocoran informasi dan serangan siber.

- Meningkatkan kepercayaan pengguna terhadap platform e-commerce lokal.
- Memberikan wawasan tentang efektivitas algoritma RSA dalam transaksi digital.

Berikut diagram blok mengenai gambaran langkah-langkah penelitian yang dilakukan:



Gambar 1. Langkah-langkah Penelitian

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisis, sistem e-commerce Toko Bangun Jaya yang berjalan masih memiliki kerentanan terhadap potensi ancaman keamanan, terutama dalam perlindungan data pelanggan dan transaksi pembayaran (digital). Evaluasi terhadap sistem yang telah ada menunjukkan bahwa mekanisme keamanan yang diterapkan belum optimal dalam mencegah risiko pencurian informasi serta kebocoran data. Maka untuk meningkatkan perlindungan datanya, peneliti melakukan perancangan model enkripsi RSA yang dirancang agar dapat terintegrasi dengan sistem transaksi yang sudah berjalan. Implementasi algoritma ini diterapkan pada proses pembayaran dan penyimpanan data pelanggan guna meningkatkan kerahasiaan informasi. Setelah diterapkan, dilakukan evaluasi untuk mengukur efektivitas enkripsi terhadap keamanan dan kecepatan transaksi, serta mengidentifikasi aspek yang masih dapat dioptimalkan dalam pengembangan sistem ke depannya.

4.1. Hasil Analisa Risiko Keamanan Pada Sistem Berjalan

Untuk memastikan implementasi dapat berjalan sesuai rencana, maka dilakukan analisis terhadap permasalahan dari sistem yang sedang berjalan. Rincian mengenai identifikasi masalah, rekomendasi solusi, serta kebutuhan sistem dapat dilihat pada Tabel 1 berikut ini.

Tabel 1. Aspek dan Analisis

Aspek	Analisis
Identifikasi Masalah	- Risiko pencurian informasi pribadi dan kebocoran data transaksi di e-commerce. - Keamanan data pelanggan yang belum optimal di Toko Bangun Jaya. - Potensi serangan siber yang dapat mengancam integritas sistem. - Perlunya peningkatan kepercayaan pelanggan terhadap keamanan transaksi digital.
Rekomendasi Solusi	- Mengimplementasikan algoritma RSA untuk enkripsi data pelanggan. - Melakukan analisis risiko terhadap sistem e-commerce yang berjalan. - Mengembangkan fitur keamanan. - Menyesuaikan ukuran kunci RSA untuk keseimbangan antara keamanan dan kecepatan transaksi.
Kebutuhan Fungsional	- Sistem harus dapat mengenkripsi informasi sensitif menggunakan algoritma RSA. - Implementasi mekanisme autentikasi untuk meningkatkan keamanan login. - Sistem harus dapat mendeteksi dan menangani potensi ancaman keamanan secara real-time. - Proses dekripsi harus dilakukan dengan efisien tanpa menghambat pengalaman pengguna.
Kebutuhan Non Fungsional	- Keamanan sistem harus memenuhi standar perlindungan data pelanggan. - Waktu respons dalam proses enkripsi dan dekripsi harus tetap optimal. - Sistem harus memiliki skalabilitas agar dapat menangani peningkatan jumlah pengguna.

Aspek	Analisis
	- Antarmuka pengguna harus tetap intuitif dan ramah pengguna meskipun memiliki fitur keamanan tambahan.

Sumber: Pengolahan Data Penelitian

4.2. Pengembangan dan Perancangan Model Enkripsi Algoritma RSA

Berikut adalah rancangan Use Case Diagram dan Activity Diagram yang menggambarkan sistem:

4.2.1. Use Case Diagram

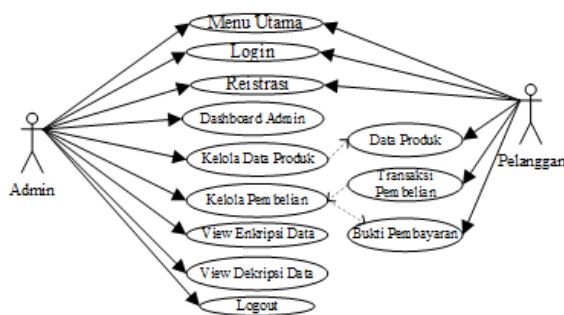
Use Case Diagram merupakan gambaran interaksi antara user dalam sistem. Terdapat dua aktor utama, yaitu:

a. Pelanggan:

- Melakukan pendaftaran akun
- Melakukan login untuk mengakses sistem
- Memilih produk dan melakukan transaksi pembelian.
- Melakukan pembayaran melalui sistem yang terenkripsi.
- Menerima notifikasi transaksi yang telah diproses.

b. Admin:

- Mengelola data produk.
- Mengelola data transaksi
- Mengelola akun pelanggan.
- Melihat dan mengelola laporan penjualan.
- Melakukan enkripsi dan dekripsi data menggunakan algoritma RSA.



Gambar 2. Use Case Diagram

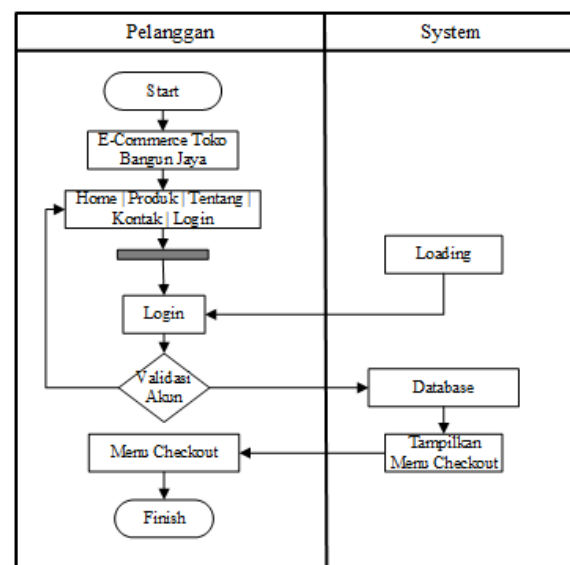
Use Case utama yang terdapat dalam sistem keamanan dalam pengembangan e-commerce ini adalah:

- Enkripsi data pelanggan saat pendaftaran. Data yang dimasukkan pelanggan dienkripsi menggunakan kunci publik RSA sebelum disimpan di database.
- Autentikasi login menggunakan enkripsi RSA. Saat pelanggan login, sistem akan memverifikasi data yang sudah dienkripsi untuk memastikan keamanan akses.
- Pengamanan transaksi pembayaran. Informasi transaksi dienkripsi sebelum dikirim ke server untuk mencegah pencurian data.

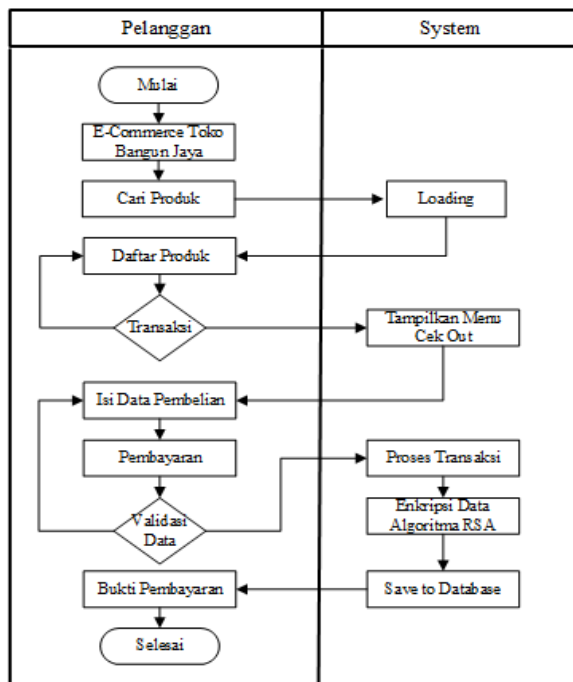
- Penyimpanan data transaksi yang terenkripsi. Data pelanggan dan transaksi tersimpan dalam bentuk terenkripsi di database e-commerce.
- Dekripsi data untuk keperluan administrasi. Admin memiliki akses untuk mendekripsi data tertentu dengan menggunakan kunci privat RSA.

4.2.2. Activity Diagram Transaksi Pembelian

Proses transaksi dimulai ketika pengguna memutuskan untuk melakukan pembelian. Pengguna kemudian memilih barang yang diinginkan dan melanjutkan ke proses pembayaran. Setelah itu, data transaksi yang mencakup detail barang dan jumlah pembelian dikirim dari perangkat pengguna ke server database. Server database menerima data transaksi tersebut dan melakukan pemeriksaan untuk memastikan validitasnya, termasuk mengecek ketersediaan stok dan keabsahan pembayaran. Jika data transaksi valid, sistem melanjutkan proses dengan mengenkripsi data menggunakan kunci publik server guna memastikan keamanannya. Data terenkripsi kemudian disimpan dalam database server. Selanjutnya, server database mengirimkan konfirmasi pembayaran kepada pengguna sebagai tanda bahwa transaksi sedang diproses. Setelah itu, server memproses data transaksi untuk menyelesaikan pesanan. Jika semua langkah berhasil dilalui, transaksi dinyatakan selesai. Namun, jika data transaksi tidak valid, sistem akan membatalkan transaksi. Proses berakhir setelah transaksi berhasil diselesaikan atau dibatalkan.



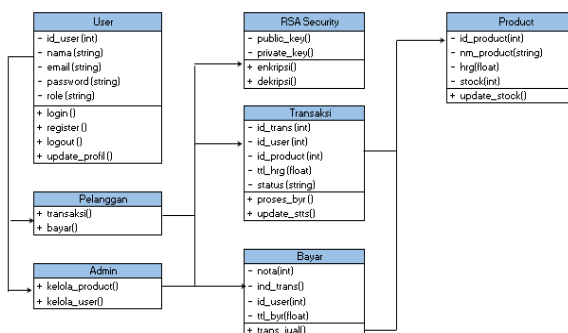
Gambar 3. Activity Diagram Login



Gambar 4. Activity Diagram Transaksi Pembelian

4.2.3. Class Diagram Keamanan Transaksi

Class Diagram digunakan untuk memodelkan struktur statis dari sebuah sistem perangkat lunak. Diagram ini menggambarkan kelas-kelas dalam sistem, atribut yang dimilikinya, metode (fungsi) yang dapat dilakukan, serta hubungan antara kelas-kelas tersebut. Algoritma enkripsi RSA merupakan modul keamanan utama dalam mengenkripsi dan mendekripsi data yang masuk dan keluar dari siste. Seperti aat pelanggan melakukan registrasi atau login, data kredensial mereka dienkripsi menggunakan kunci publik RSA sebelum disimpan dalam database, sehingga pihak yang tidak berwenang tidak dapat mengaksesnya. Gambar 5 di bawah ini merupakan model class diagram dalam sistem yang digunakan.



Gambar 5. Class Diagram Kemananan Transaksi

4.3. Implementasi Algoritma RSA dan Validasi pada Sistem E-Commerce

Gambar fitur-fitur di bawah ini merupakan hasil pengembangan dari fitur yang menerapkan sistem keamanan algoritma RSA yang mencakup:

4.3.1. Menu Utama

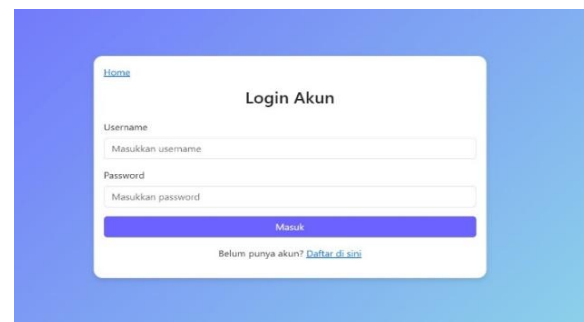
Gambar 6 merupakan tampilan utama yang mengarahkan pengguna untuk melakukan transaksi.



Gambar 6. Menu Utama E-Commerce

4.3.2. Menu Login

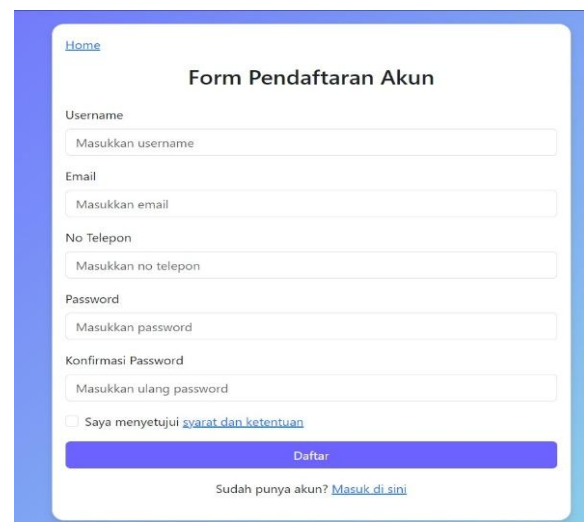
Gambar 7 di bawah ini adalah tampilan ketika pengguna melakukan login pada aplikasi e-commerce Toko Bangun Jaya.



Gambar 7. Menu Login

4.3.3. Halaman Registrasi

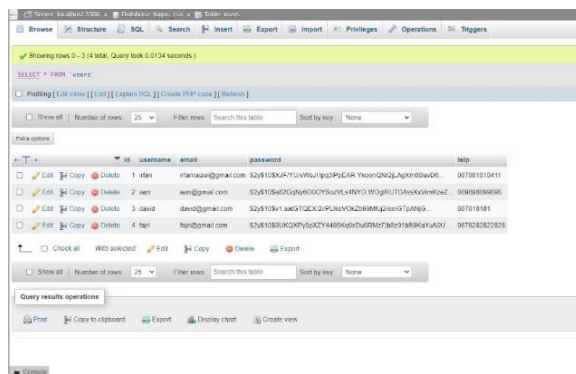
Gambar 8 merupakan fitur pendaftaran pengguna baru dengan enkripsi RSA untuk menjaga kerahasiaan data.



Gambar 8. Menu Registrasi

4.3.4. Tabel Database Pengguna

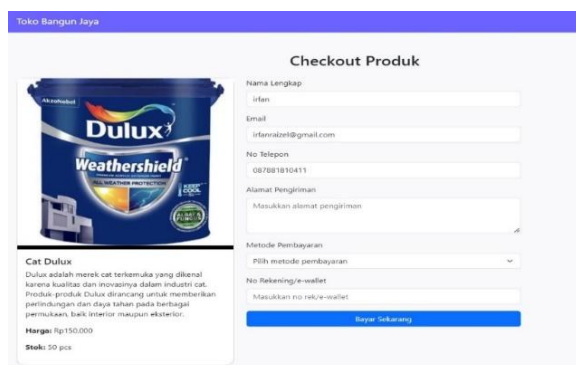
Gambar 9 di bawah adalah bentuk tabel dari database yang disimpan menggunakan algoritma RSA.



Gambar 9. Tampilan Tabel Pengguna

4.3.5. Fitur Pengamanan Transaksi Pembelian

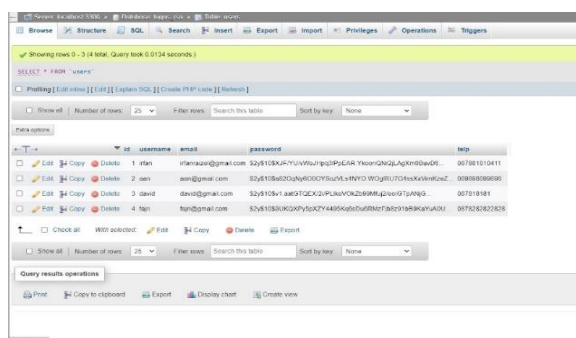
Gambar 10 di bawah ini merupakan fitur pengembangan sistem keamanan. Dan untuk melakukan transaksi pembelian pelanggan, kemudian pelanggan melakukan checkout dengan mengisi formulir yang terdiri dari Nama, Email, No. Telepon, Alamat, Metode Pembayaran, dan No. Rekening atau E-wallet.



Gambar 10. Implementasi Algoritma RSA

4.3.6. Tabel Database

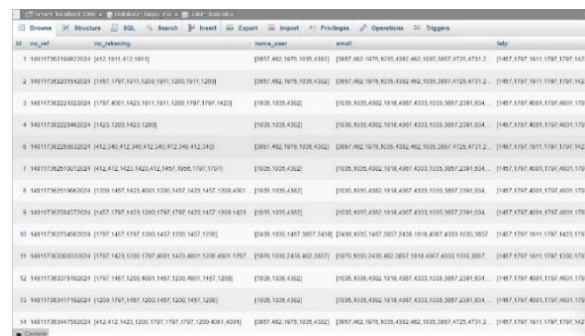
Gambar 11 di bawah ini merupakan informasi transaksi yang tersimpan dalam bentuk terenkripsi di database.



Gambar 11. Tampilan Database Terenkripsi RSA

4.3.7. Tampilan Tabel Transaksi Pembelian yang Terenkripsi

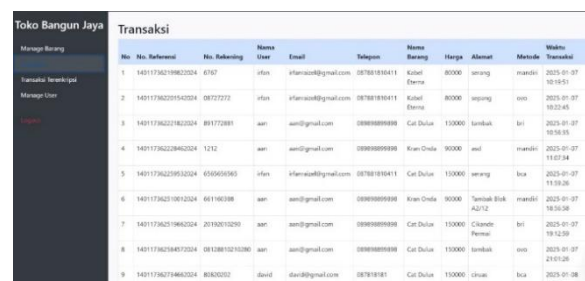
Gambar 12 di bawah ini adalah merupakan bentuk tabel dari database pembelian barang yang sudah di enkrip sehingga data privasi pelanggan tidak dapat dilihat oleh orang lain selain pemilik usaha.



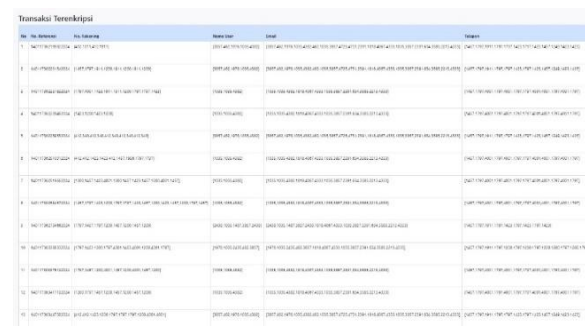
Gambar 12. Tampilan Database dari Tabel Transaksi Pembelian Terenkripsi Algoritma RSA

4.3.8. Menu Tampilan Data dari Sisi Server

Gambar 13 dan 14 di bawah ini menampilkan data transaksi dalam bentuk terenkripsi dan dekripsi hanya dapat dilakukan oleh admin yang berwenang.



Gambar 13. Tampilan Menu dari Sisi Server (Transaksi Pembelian Dekripsi)



Gambar 14. Tampilan Menu dari Sisi Server (Transaksi Pembelian Enkripsi)

Kedua menu tampilan diatas di dapatkan setelah melakukan pengujian pada sistem untuk melihat dan memastikan apakah sistem dapat beroperasi sesuai dengan spesifikasi atau seharusnya. Dari kedua gambar di atas hasil menunjukkan bahwasannya sistem dapat mengenkripsi data pribadi user dengan benar.

4.4. Evaluasi dan Analisis Hasil

Setelah implementasi algoritma RSA pada sistem e-commerce Toko Bangun Jaya, dilakukan serangkaian pengujian untuk mengevaluasi efektivitas enkripsi dalam meningkatkan keamanan data pelanggan dan transaksi. Evaluasi ini mencakup pengujian fungsionalitas sistem, analisis performa

enkripsi, serta pengukuran dampaknya terhadap pengalaman pengguna.

4.4.1. Pengujian Fungsionalitas dengan Blackbox Testing

Metode Blackbox Testing digunakan untuk memastikan bahwa sistem berfungsi sesuai dengan spesifikasi yang telah dirancang. Hasil pengujian menunjukkan bahwa:

- Proses pendaftaran dan login pelanggan berhasil terenkripsi dengan RSA, sehingga data kredensial pelanggan tersimpan dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang.
- Transaksi pembayaran berjalan dengan aman, di mana informasi pelanggan dan detail pembayaran hanya dapat diakses oleh sistem setelah melalui proses dekripsi dengan kunci privat RSA.
- Sistem menolak akses yang tidak sah terhadap data transaksi, mencegah potensi serangan dari pihak eksternal yang mencoba mengakses informasi pelanggan tanpa izin.

Dengan hasil tersebut, dapat disimpulkan bahwa sistem yang dibangun mampu mengimplementasikan enkripsi RSA dengan baik, sehingga data pelanggan dapat terlindungi dari risiko pencurian atau manipulasi.

4.4.2. Analisis Performa Enkripsi RSA terhadap Kecepatan Transaksi

Selain aspek keamanan, kecepatan eksekusi sistem juga menjadi faktor penting dalam implementasi enkripsi. Evaluasi dilakukan dengan membandingkan waktu pemrosesan transaksi dengan dan tanpa enkripsi RSA. Hasil analisis menunjukkan bahwa:

- Proses enkripsi dan dekripsi dengan kunci 1024-bit membutuhkan tambahan waktu rata-rata 0,75 detik per transaksi.
- Penggunaan kunci 2048-bit meningkatkan keamanan, tetapi memperlambat transaksi hingga 1,2 detik, yang dapat berdampak pada pengalaman pengguna.
- Sistem tetap mampu menangani transaksi dengan baik, meskipun ada sedikit peningkatan waktu pemrosesan akibat proses enkripsi.

Berdasarkan hasil tersebut antara keamanan dan efisiensi sistem perlu dipertimbangkan. Untuk menjaga keseimbangan, sistem ini menggunakan kunci 1024-bit sebagai standar, karena masih memberikan tingkat keamanan yang baik dengan dampak minimal terhadap kecepatan transaksi.

4.4.3. Dampak Implementasi RSA terhadap Keamanan Data

Evaluasi selanjutnya dilakukan dengan melakukan simulasi serangan siber, seperti man-in-the-middle attack dan brute-force attack, guna menilai

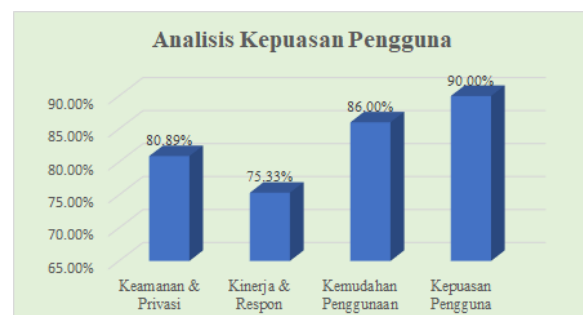
seberapa efektif enkripsi RSA dalam melindungi data pelanggan. Hasil analisis menunjukkan bahwa:

- Data pelanggan yang telah dienkripsi tidak dapat dibaca oleh pihak eksternal tanpa kunci privat, sehingga risiko pencurian informasi dapat diminimalisir.
- Serangan brute-force terhadap data yang dienkripsi dengan RSA membutuhkan waktu yang sangat lama, sehingga tidak memungkinkan untuk dipecahkan dalam waktu yang wajar.
- Sistem mampu menangkal percobaan akses ilegal, membuktikan bahwa algoritma RSA dapat secara efektif meningkatkan perlindungan terhadap transaksi digital.

4.4.4. Analisis Kepuasan Pengguna

Selain aspek teknis, feedback dari pengguna juga dikumpulkan untuk mengevaluasi pengalaman mereka setelah sistem keamanan baru diterapkan. Hasil survei menunjukkan bahwa:

- 85% pengguna merasa lebih aman melakukan transaksi setelah mengetahui bahwa data mereka dienkripsi dengan RSA.
- 75% pengguna tidak merasakan perbedaan signifikan dalam kecepatan transaksi, meskipun ada proses enkripsi tambahan.
- 90% pengguna setuju bahwa implementasi sistem keamanan ini meningkatkan kepercayaan mereka terhadap Toko Bangun Jaya sebagai platform e-commerce yang aman.



Gambar 15. Grafik Kepuasan Pengguna

Hasil evaluasi ini menunjukkan bahwa penerapan algoritma RSA pada e-commerce Toko Bangun Jaya telah berhasil meningkatkan keamanan transaksi tanpa mengorbankan pengalaman pengguna.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi algoritma RSA pada sistem keamanan e-commerce, dapat disimpulkan bahwa RSA sangat efektif dalam meningkatkan perlindungan data sensitif selama transaksi. Algoritma ini berhasil mengenkripsi informasi penting seperti data kartu kredit, identitas pelanggan, dan riwayat transaksi sehingga mengurangi risiko pencurian data. Meskipun demikian, RSA memiliki kelemahan dalam hal efisiensi, karena proses enkripsi dan dekripsi membutuhkan daya komputasi yang cukup besar, terutama untuk kunci dengan

panjang lebih dari 2048 bit. Hal ini dapat memperpanjang waktu pemrosesan, sehingga perlu dipertimbangkan penggunaan metode pendukung, seperti enkripsi hybrid, untuk meningkatkan efisiensi.

Selain itu, implementasi RSA pada prototipe e-commerce menunjukkan bahwa algoritma ini dapat diintegrasikan tanpa mengganggu fungsi utama aplikasi. Sistem tetap berjalan dengan baik, dan proses transaksi tetap responsif meskipun terdapat tambahan lapisan keamanan. Dengan demikian, RSA merupakan solusi yang dapat diandalkan untuk menciptakan sistem e-commerce yang aman, selama tantangan efisiensi dapat dikelola dengan baik. Untuk optimalisasi lebih lanjut, dapat dipertimbangkan penggunaan enkripsi secara hybrid, seperti kombinasi RSA dengan AES, agar proses enkripsi menjadi lebih efisien tanpa mengurangi tingkat keamanan. Secara keseluruhan, penelitian ini menunjukkan bahwa RSA merupakan metode enkripsi yang efektif untuk e-commerce, memberikan perlindungan maksimal terhadap data pelanggan sekaligus menjaga kepercayaan pengguna terhadap sistem.

DAFTAR PUSTAKA

- [1] S. Auliana, G. Untirtha Pratama, B. Rakhim Setya Permana, and O. Firmansyah, "Design of a Mobile Phone Sales System Website at Vivo Store," *ARRUS Journal of Engineering and Technology*, vol. 4, no. 1, pp. 126–140, 2024, doi: 10.35877/jetech2710.
- [2] A. Poeja Kehista *et al.*, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Keamanan (Literature Review)," *JIMT*, vol. 4, no. 5, 2023, doi: 10.31933/jimt.v4i5.
- [3] S. T. Zahwani¹, M. Irwan, and P. Nasution², "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital," *JoSES: Journal of Sharia Economics Scholar*, vol. 2, no. 2, pp. 105–109, 2023, doi: 10.5281/zenodo.12608751.
- [4] N. Berliano Novanka Putra, F. Amalia Raihana, W. Michael Albert Mondong, and A. Rosadi Kardian, "Analisis Enkripsi Kriptografi Asimetris Algoritma RSA Berbasis Pemrograman Batch pada Media Flashdisk," *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, vol. 8, pp. 142–154, Feb. 2023, [Online]. Available: <https://tunasbangsa.ac.id/ejurnal/index.php/jurasik>
- [5] S. Vivi Wahdini, D. Hartama, and I. Okta Kirana, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *Journal of Informatics Management and Information Technology*, vol. 1, no. 3, pp. 101–107, 2021, [Online]. Available: <https://hostjournals.com/>
- [6] K. Shifa Adwitia Sitepu, R. Nadilla Putri, and Z. Indra, "Evaluasi Kuantitatif Penggunaan Algoritma RSA pada Aplikasi Shopee Pay: Kecepatan vs Keamanan," *TEKNIKA*, vol. 19, no. 1, pp. 159–168, Oct. 2024.
- [7] B. Rakhim, S. Permana, F. Fatullah, K. Maharani, Darip Mochammad, and G. Untirtha Pratama, "Pendampingan UMKM Melalui Strategi Pemasaran Berbasis Media Sosial Untuk Pelaku UMKM Desa Kebuyutan Kecamatan Tirtayasa," *Batara Wisnu Journal: Indonesian Journal of Community Services*, vol. 3, no. 2, pp. 512–519, 2023, doi: 10.53363/bw.v3i2.207.
- [8] I. Pagala, T. Abdulghani, A. Budi Pratomo, and H. Syofya, *Bisnis Digital 5.0*. CV Rey Media Grafika, 2024. Accessed: Feb. 11, 2025. [Online]. Available: <https://books.google.co.id/books?id>
- [9] A. M. Pratama, Syaiful, and M. F. Rahman, *Keamanan Data dan Informasi*. Kaizen Media Publishing, 2024. Accessed: Feb. 11, 2025. [Online]. Available: <https://books.google.co.id/books?id>
- [10] M. F. Rafli, Z. Panjaitan, and W. Riansah, "Aplikasi Keamanan Sistem Pengiriman Tagihan Pembayaran Online (Invoice) Berbasis Website dengan algoritma RSA-CRT," *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 23, no. 1, pp. 138–146, Feb. 2024, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jis/index>
- [11] R. Rachman Judhieputra and I. Nur Anisa, *Kriptografi Penerapan dalam Keamanan Transaksi Komersial*. Indonesia Emas Group, 2024.
- [12] N. Supiana and M. Darip, "Optimalisasi Pengelolaan Proyek Menggunakan Algoritma HRN Dalam Sistem Informasi Manajemen Proyek Di Perusahaan Properti," *INFOTECH journal*, vol. 11, no. 1, pp. 20–27, Jan. 2025, doi: 10.31949/infotech.v11i1.12842.
- [13] Rudianto, A. Sapaatullah, B. Rakhim Setya Permana, and D. Mochammad, "Implementasi Struktur Data Array dalam Sistem Perpustakaan Berbasis Web dengan Python Flask," *Buletin Ilmiah Informatika Teknologi*, no. 2, Jan. 2025.
- [14] M. Darip, "Desain Integrasi Sistem Payroll Karyawan Outsourcing Antara Perusahaan Alih Daya Dengan Perusahaan Mitra (Studi Kasus PT. BCA dan PT. KIP)," *Jurnal Simasi: Jurnal Ilmiah Sistem Informasi*, vol. 3, no. 2, p. 241, Dec. 2023.
- [15] A. Sapaatullah, Rudianto, B. R. S. Permana, and D. Mochammad, "Simulasi Model Antrean FIFO Untuk Mengoptimalkan Penanganan Permintaan Layanan Di KUD CV. Rama Investama," *Buletin Ilmiah Informatika Teknologi*, vol. 2, no. 2, Jan. 2025, Accessed: Jan. 25, 2025. [Online]. Available: <https://ejurnal.amikstiekomu.ac.id/index.php/B-IIT/article/view/92>