Teknika 19 (1): 159-168

JURNAL TEKNIKA
ISSN: 0854-3143
e-ISSN: 2622-3481
Journal homepage: http://jurnal.polsri.ac.id/index.php/teknika
Journal Email: teknika@polsri.ac.id

Evaluasi Kuantitatif Penggunaan Algoritma RSA pada Aplikasi *Shopee Pay*: Kecepatan vs Keamanan

Keysa Shifa Adwitia Sitepu[1], Rezkya Nadilla Putri[2], Zulfahmi Indra[3*]

[1,2,3*]Jurusan Matematika, Universitas Negeri Medan, Medan, Indonesia
*Email Penulis Korespondensi: zulfahmi.indra@unimed.ac.id

Abstrak

Penelitian ini mengevaluasi masalah kecepatan dan keamanan transaksi pada aplikasi ShopeePay dengan algoritma RSA, sebuah teknik kriptografi asimetris yang banyak digunakan. Tujuannya adalah menentukan pengaruh ukuran kunci RSA (512-bit, 1024-bit, 2048-bit) terhadap waktu pemrosesan enkripsi dan dekripsi, serta keamanan terhadap serangan brute force. Metode yang digunakan mencakup pengujian pada berbagai volume data (100 KB, 1 MB, 10 MB) untuk mengevaluasi kecepatan dan keamanan. Hasil penelitian menunjukkan bahwa ukuran kunci yang lebih besar meningkatkan keamanan tetapi memperlambat transaksi. Kunci 1024-bit memberikan keseimbangan terbaik antara kecepatan dan keamanan, sementara kunci 2048-bit cocok untuk keamanan lebih tinggi dengan kecepatan lebih lambat. Penelitian ini memberikan panduan penting bagi pengembang aplikasi digital dalam memilih ukuran kunci yang sesuai untuk melindungi data transaksi di Shopee Pay.

Kata kunci*—Algoritma RSA, ShopeePay, Keamanan Data, Kecepatan Transaksi, Kriptografi*

Abstract

This study evaluates the issue of speed and security in transactions on the ShopeePay application using the RSA algorithm, a widely used asymmetric cryptographic technique. The goal is to determine the impact of RSA key sizes (512-bit, 1024-bit, 2048-bit) on encryption and decryption processing time, as well as security against brute force attacks. The method involves testing various data volumes (100 KB, 1 MB, 10 MB) to evaluate speed and security. The results show that larger key sizes enhance security but slow down transactions. The 1024-bit key provides the best balance between speed and security, while the 2048-bit key is suitable for higher security with slower speeds. This research provides important guidance for digital application developers in selecting the appropriate key size to protect transaction data in Shopee Pay.

Keywords*—RSA Algorithm, ShopeePay, Data Security, Transaction Speed, Cryptography*

1. PENDAHULUAN

Transaksi digital di Indonesia mengalami perkembangan pesat dalam beberapa tahun terakhir, seiring dengan meningkatnya penggunaan layanan dompet digital seperti *Shopee Pay*. Setiap perusahaan atau bisnis menggunakan teknologi komputer sebagai cara untuk mendapatkan informasi dengan cepat dan akurat [1]. Aplikasi ini telah menjadi salah satu alat pembayaran yang

populer di Indonesia, digunakan untuk berbagai macam transaksi, mulai dari pembelian barang, pembayaran tagihan, hingga transfer uang antar pengguna [2]. Namun, peningkatan volume transaksi ini membawa tantangan baru dalam hal keamanan, di mana perlindungan data pengguna menjadi prioritas utama bagi pengembang aplikasi. Algoritma RSA, sebagai salah satu algoritma kriptografi yang paling banyak digunakan, menjadi pilihan utama dalam menjamin keamanan transaksi digital [3].

Algoritma RSA dikenal sebagai salah satu metode enkripsi asimetris yang paling aman dan banyak digunakan dalam berbagai aplikasi transaksi online. RSA menggunakan dua kunci: satu kunci publik untuk enkripsi dan satu kunci privat untuk dekripsi. Keamanan algoritma ini sangat bergantung pada ukuran kunci yang digunakan, di mana kunci yang lebih panjang menghasilkan tingkat keamanan yang lebih tinggi, tetapi mempengaruhi kecepatan pemrosesan data. Dalam aplikasi seperti *Shopee Pay*, di mana kecepatan transaksi sangat penting, keseimbangan antara keamanan dan efisiensi harus dicapai. Penelitian ini bertujuan untuk mengevaluasi sejauh mana ukuran kunci RSA mempengaruhi kecepatan dan keamanan transaksi pada *Shopee Pay*.

Algoritma RSA adalah metode kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. RSA terkenal karena tingkat keamanannya yang tinggi, yang bergantung pada panjang kunci yang digunakan. Semakin panjang kunci, semakin sulit untuk memecahkan algoritma ini melalui serangan *brute force*. Namun, penggunaan kunci yang lebih panjang juga memiliki dampak negatif pada kecepatan transaksi. Hal ini menjadi penting untuk diteliti lebih lanjut, khususnya dalam konteks aplikasi seperti *Shopee Pay*, di mana kecepatan dan keamanan harus seimbang [4].

Ancaman keamanan dalam transaksi *online* tidak bisa dianggap remeh. Berdasarkan laporan keamanan siber, terdapat banyak kasus di mana pengguna dompet digital menjadi korban peretasan akibat enkripsi yang lemah atau tidak efektif. *Shopee Pay* sebagai aplikasi pembayaran digital harus menerapkan sistem keamanan yang kuat untuk melindungi data pengguna dari serangan pihak ketiga. Algoritma RSA merupakan salah satu solusi yang telah terbukti efektif dalam mengamankan data pengguna, namun dengan kompromi tertentu dalam kecepatan pemrosesan. Oleh karena itu, penting untuk mengevaluasi performa algoritma ini dalam lingkungan yang membutuhkan kecepatan tinggi seperti *Shopee Pay*.

Dengan meningkatnya ancaman keamanan, *Shopee Pay* dan aplikasi dompet digital lainnya semakin sering menjadi target serangan siber. Penerapan algoritma RSA bertujuan untuk melindungi data pengguna dari serangan seperti peretasan dan pencurian identitas. Akan tetapi, penggunaan kunci RSA dengan ukuran yang lebih besar dapat memperlambat kecepatan transaksi, yang dapat memengaruhi pengalaman pengguna secara keseluruhan. Oleh karena itu, penting untuk menemukan keseimbangan optimal antara kecepatan dan keamanan dalam penerapan algoritma RSA di aplikasi *Shopee Pay* [5].

Penelitian sebelumnya menunjukkan bahwa ada *trade-off* antara kecepatan dan keamanan dalam penerapan RSA. Sebagai contoh, penggunaan kunci RSA yang lebih besar memberikan keamanan yang lebih baik tetapi memperlambat proses transaksi. Dalam konteks aplikasi *Shopee Pay* yang melibatkan jutaan pengguna, ini menjadi dilema bagi pengembang aplikasi: apakah harus lebih memprioritaskan keamanan atau kecepatan transaksi? Penelitian ini akan memberikan wawasan lebih lanjut mengenai bagaimana penggunaan ukuran kunci yang berbeda pada RSA mempengaruhi pengalaman pengguna dalam transaksi *online*. Hasil penelitian diharapkan dapat menjadi referensi bagi pengembang dalam memilih ukuran kunci yang optimal untuk aplikasi dompet digital seperti *Shopee Pay* [6].

Pada aplikasi dompet digital seperti *Shopee Pay*, kecepatan transaksi adalah salah satu faktor penting yang memengaruhi kepuasan pengguna. Namun, perlindungan data pribadi pengguna juga tidak boleh diabaikan. Keseimbangan antara kecepatan dan keamanan menjadi tantangan yang perlu diatasi oleh pengembang aplikasi [7]. Penelitian ini berfokus pada evaluasi penggunaan algoritma RSA dengan berbagai ukuran kunci (512-bit, 1024-bit, dan 2048-bit) dalam konteks aplikasi ShopeePay untuk menemukan keseimbangan optimal antara kedua aspek tersebut.

Shopee Pay sebagai salah satu aplikasi dompet digital terkemuka di Indonesia memerlukan sistem keamanan yang kuat untuk melindungi data penggunanya [8]. Serangan siber yang semakin canggih memaksa pengembang untuk selalu mengevaluasi dan memperbarui metode enkripsi yang digunakan. RSA, meskipun sudah teruji sebagai salah satu metode kriptografi terbaik, tetap membutuhkan kajian lebih lanjut dalam hal pengaturan ukuran kunci yang optimal sesuai dengan kebutuhan transaksi digital moderen [9].

Penelitian ini penting untuk dilakukan karena perkembangan transaksi digital yang pesat memunculkan kebutuhan mendesak akan sistem keamanan yang handal untuk melindungi data sensitif. Dompet digital seperti *Shopee Pay* digunakan oleh jutaan pengguna untuk berbagai transaksi keuangan, sehingga ancaman keamanan, seperti peretasan dan pencurian data, menjadi isu kritis. Algoritma RSA merupakan salah satu solusi yang terbukti efektif dalam melindungi data melalui kriptografi asimetris yang kuat. Evaluasi algoritma RSA, terutama terkait keseimbangan antara kecepatan pemrosesan dan tingkat keamanan, memberikan wawasan penting bagi pengembang aplikasi dalam memilih strategi enkripsi yang optimal [10].

Fokus pada algoritma RSA dibanding algoritma lain yang sepadan, seperti AES atau ECC, didasari oleh keunggulan RSA dalam hal keamanan kunci publik dan privasi data. RSA memiliki ketahanan yang tinggi terhadap serangan *brute force*, terutama ketika ukuran kunci diperbesar, meskipun ada kompromi dalam hal kecepatan. Algoritma RSA sangat relevan untuk aplikasi yang memerlukan otentikasi dan pertukaran kunci secara aman, di mana kunci publik dapat didistribusikan secara luas tanpa mengurangi keamanan. Algoritma simetris seperti AES mungkin lebih cepat, namun RSA lebih unggul dalam aspek keamanan otentikasi dan pertukaran kunci [11].

Penelitian ini tidak hanya menganalisis tingkat keamanan RSA tetapi juga mempertimbangkan pengaruhnya terhadap kecepatan transaksi, terutama dalam aplikasi yang memproses banyak transaksi setiap saat. Ini sangat relevan karena pengembang aplikasi seperti *Shopee Pay* perlu mempertimbangkan keseimbangan antara pengalaman pengguna yang cepat dan perlindungan data yang optimal [12].

Hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam dunia pengembangan aplikasi dompet digital di Indonesia. Dengan menemukan ukuran kunci RSA yang tepat, pengembang dapat meningkatkan keamanan aplikasi tanpa mengorbankan kecepatan transaksi, sehingga pengguna dapat merasakan pengalaman yang lebih aman dan efisien saat bertransaksi menggunakan *Shopee Pay*.

2. METODE PENELITIAN

Berikut adalah tahapan atau rancangan penelitan yang dilakukan, dengan mengacu pada tahapan penelitian pada Gambar 1.

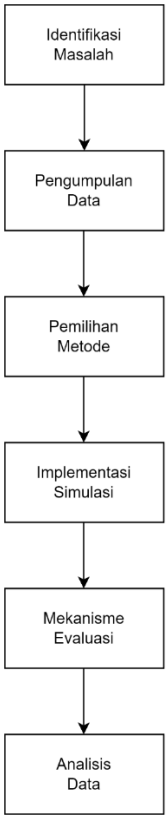
2.1 Identifikasi Masalah

Tahapan ini merupakan langkah awal yang sangat penting dalam penelitian, karena menentukan arah dan fokus keseluruhan proses penelitian. Di sini peneliti perlu merumuskan masalah penelitian secara jelas dan spesifik. Dalam konteks penelitian ini, fokusnya adalah mengevaluasi kinerja algoritma RSA yang digunakan pada aplikasi *Shopee Pay*. *Shopee Pay* merupakan platform transaksi digital yang banyak digunakan di Indonesia. Dengan mengidentifikasi masalah, peneliti dapat menetapkan tujuan penelitian yang jelas dan fokus pada aspek yang relevan untuk penelitian selanjutnya.

2.2 Pengumpulan Data

Pada tahap ini, peneliti melakukan simulasi transaksi untuk mengumpulkan data yang diperlukan untuk penelitian ini. Simulasi akan menggunakan kunci RSA dengan panjang 512-bit, 1024-bit, dan 2048-bit, serta berbagai ukuran data, yaitu 100 KB, 1 MB, dan 10 MB. Tujuan pendekatan ini adalah memberikan gambaran menyeluruh tentang bagaimana ukuran kunci mempengaruhi kinerja algoritma RSA dalam aplikasi *Shopee Pay*. Pengumpulan data akan dilakukan di lingkungan terkendali di mana perubahan dapat dikelola dan dipantau dengan cermat. Sasarannya adalah untuk memastikan keputusan yang tepat dan dapat diandalkan, agar

analisis selanjutnya menghasilkan temuan yang valid. Selain waktu pemrosesan, peneliti juga mempertimbangkan untuk mengumpulkan data tambahan seperti penggunaan memori dan sumber daya sistem lainnya, guna memberikan pemahaman yang lebih komprehensif tentang kinerja algoritma.



Gambar 1 Rancangan Penelitian

2.3 Pemilihan Metode

Penelitian ini menerapkan pendekatan kuantitatif dengan metode eksperimental. Selama simulasi transaksi, protokol RSA akan digunakan untuk proses enkripsi dan dekripsi. Memilih metode yang tepat sangat penting untuk mengukur dan menganalisis hasil penelitian dengan objektif [13].

2.4 Implementasi Simulasi

Pada tahap ini akan dijalankan simulasi untuk menguji kinerja algoritma RSA menggunakan berbagai ukuran kunci (512-bit, 1024-bit, dan 2048-bit) dan volume data (100 KB, 1 MB, 10 MB). Untuk mengukur waktu yang dibutuhkan pada proses enkripsi dan dekripsi digunakan rumus seperti pada Formula (1) dan Formula (2).

Rumus Waktu Enkripsi ($T_{enkripsi}$):

$$(T_{enkripsi})(k, v) = a.k + b.v + c \qquad (1)$$

Keterangan:

$T_{enkripsi}(k, v)$: Waktu enkripsi dalam detik.
k : Ukuran kunci (dalam bit) yang dapat bernilai 512,1024, atau 2048.
v : Volume data (dalam KB atau MB).
$a, b, dan\ c$: Konstanta yang ditentukan berdasarkan hasil pengujian empiris.

Rumus Waktu Deskripsi ($T_{deskripsi}$):

$$(T_{deskripsi})(k, v) = d.k + e.v + f \qquad (2)$$

Keterangan:

$T_{deskripsi}(k, v)$: Waktu deskripsi dalam detik.
k : Ukuran kunci (dalam bit).
v : Volume data (dalam KB atau MB).
$d, e, dan\ f$: Konstanta yang ditentukan berdasarkan pengujian.

Tingkat Keamanan

$$Tingkat\ Keamanan\ (k) = \begin{cases} Rendah\ jika\ k = 512 - bit \\ Sedang\ jika\ k = 1024 - bit \\ Tinggi\ jika\ k = 2048 - bit \end{cases}$$

2.5 Mekanisme Evaluasi

Penulis melakukan pengujian terhadap kinerja algoritma RSA dengan memperhatikan variasi ukuran kunci serta volume data yang digunakan. Simulasi ini bertujuan untuk mengukur seberapa lama waktu yang diperlukan oleh algoritma dalam memproses data dengan berbagai ukuran kunci yang ditentukan.

2.6 Analisis Data

Untuk menganalisis data, protokol RSA akan diterapkan dalam proses enkripsi dan dekripsi selama simulasi transaksi [14]. Pemilihan metode yang tepat sangat penting agar hasil simulasi dapat diukur dan dianalisis secara objektif, sehingga menghasilkan evaluasi kinerja yang akurat [15].

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Masalah

Masalah utama pada penelitian ini adalah bagaimana kinerja algoritma RSA dalam menjaga keseimbangan antara pemrosesan dan tingkat keamanan pada aplikasi *Shopee Pay*.

3.2 Pengumpulan Data

Sumber utama data berasal dari simulasi transaksi menggunakan algoritma RSA yang diimplementasikan di lingkungan yang menyerupai aplikasi *Shoppe Pay*. Simulasi ini melibatkan berbagai ukuran kunci RSA (512 bit, 1024 bit, 2048 bit) dan volume data yang bervariasi (100 KB, 1 MB, 10 MB). Tabel 1 adalah tabel hasil pengukuran waktu enkripsi dan dekripsi berdasarkan berbagai ukuran kunci RSA dan volume data yang digunakan.

Tabel 1 Ukuran Kunci RSA dan Waktu Pemrosesan

Ukuran Kunci	Volume Data	Waktu Enkripsi (detik)	Waktu Deskripsi (detik)	Tingkat Keamanan
512-bit	100 KB	0.005	0.004	Rendah
512-bit	1 MB	0.045	0.038	Rendah
512-bit	10 MB	0.400	0.350	Rendah
1024-bit	100 KB	0.015	0.012	Sedang
1024-bit	1 MB	0.130	0.110	Sedang
1024-bit	10 MB	1.250	1.100	Sedang
2048-bit	100 KB	0.030	0.025	Tinggi

2048-bit	1 MB	0.260	0.210	Tinggi
2048-bit	10 MB	2.400	2.100	Tinggi

3.3 Pemilihan Metode

Simulasi transaksi menggunakan protokol RSA dengan ukuran kunci dan volume data yang berbeda. Rumus waktu enkripsi dan dekripsi digunakan untuk memperkirakan waktu pemrosesan.

3.4 Implementasi Simulasi

Untuk menghitung waktu enkripsi dan dekripsi berdasarkan rumus umum yang tentukan, peneliti akan mengalikan koefisien dengan ukuran kunci dan volume data. Pendekatan ini memungkinkan peneliti memperkirakan waktu enkripsi dan dekripsi dengan lebih fleksibel. Berikut cara penghitungannya:

Ukuran kunci 512-bit, volume data 1 MB:

$T_{enkripsi}(512{,}1) = a.512 + b.1 + c$

$T_{enkripsi}(512{,}1) = 0.045\ detik$

Ukuran kunci 2048-bit, volume data 10 MB:

$T_{deskripsi}(2048{,}10) = d.2048 + e.10 + f$

$T_{deskripsi}(2048{,}10) = 2.100\ detik$

3.5 Mekanisme Evaluasi

Evaluasi dilakukan untuk mengukur waktu pemrosesan dan keamanan algoritma RSA. Setiap ukuran kunci diuji terhadap serangan brute force untuk menilai tingkat keamanannya seperti dapat dilihat pada Tabel 2.

Tabel 2 Perbandingan Keamanan dan Kecepatan Berdasarkan Ukuran Kunci

Ukuran Kunci	Volume Data	Waktu Emkripsi (detik)	Waktu Deskripsi (detik)	Tingkat Keamanan	Tingkat Kerentanan Terhadap Brute Force
512-bit	100 KB	0.005	0.004	Rendah	Tinggi
1024-bit	100 KB	0.015	0.012	Sedang	Sedang
2048-bit	100 KB	0.030	0.025	Tinggi	Rendah
512-bit	1 MB	0.045	0.038	Rendah	Tinggi
1024-bit	1 MB	0.130	0.110	Sedang	Sedang
2048-bit	1 MB	0.260	0.210	Ttinggi	Rendah

Dari Tabel 2 tersebut, dapat dilihat bahwa ukuran kunci RSA mempengaruhi kecepatan pemrosesan data, baik untuk enkripsi maupun dekripsi. Ukuran kunci yang lebih besar menghasilkan tingkat keamanan yang lebih baik, namun mengorbankan efisiensi pemrosesan data, terutama pada volume data yang lebih besar. Dengan demikian, pengembang aplikasi harus mempertimbangkan keseimbangan antara kecepatan dan keamanan berdasarkan kebutuhan transaksi.

Berdasarkan hasil penelitian, terlihat bahwa ukuran kunci RSA memengaruhi secara signifikan terhadap kecepatan enkripsi dan dekripsi di aplikasi ShopeePay. Kunci 512-bit menunjukkan waktu pemrosesan tercepat untuk volume data kecil, tetapi tingkat keamanannya

rendah, sehingga tidak cocok untuk melindungi data sensitif. Penggunaan kunci 1024-bit menunjukkan keseimbangan terbaik antara keamanan dan kecepatan, terutama untuk transaksi dengan volume data sedang. Sementara itu, kunci 2048-bit memberikan tingkat keamanan tertinggi, namun dengan waktu pemrosesan yang lebih lambat, terutama pada volume data besar. Hal ini membuktikan bahwa semakin besar ukuran kunci RSA, semakin tinggi tingkat keamanannya, namun mengorbankan efisiensi waktu.

Tabel 3 Tingkat Keamanan Kunci RSA terhadap Serangan *Brute Force*

Ukuran Kunci	Perkiraan Waktu untuk Memecahlan (*Brute Force*)	Tingkat Keamanan
512-bit	1 Hari	Rendah
1024-bit	1 Tahun	Sedang
2048-bit	1 Miliar Tahun	Tinggi

Berdasarkan Tabel 3, kunci RSA 512-bit sangat rentan terhadap serangan *brute force*, hanya membutuhkan waktu sehari untuk dipecahkan. Sebaliknya, kunci 2048-bit hampir tidak dapat ditembus, dengan waktu yang dibutuhkan mencapai miliaran tahun. Ini menunjukkan bahwa kunci dengan ukuran yang lebih besar menawarkan keamanan yang jauh lebih kuat, namun sekali lagi perlu mempertimbangkan dampaknya pada efisiensi aplikasi.

Tabel 3 ini menunjukkan bagaimana performa algoritma RSA pada aplikasi *Shopee Pay* dipengaruhi oleh volume transaksi harian dan bagaimana ukuran kunci RSA memengaruhi efisiensi sistem, termasuk penggunaan sumber daya CPU.

3.6 Analisis Data

Berdasarkan hasil simulasi dan evaluasi, berikut adalah analisis statistik menggunakan ANOVA untuk mengukur pengaruh ukuran kunci RSA dan volume data terhadap waktu pemrosesan.

Tabel 4 Tabel ANOVA

Sumber Variasi	JK (Jumlah Kuadrat)	DF (Derajat Bebas)	RJK (Rata-Rata Jumlah Kuadrat)	F	Sig.
Ukuran Kunci	8.21	2	4.105	19.48	0.000
Volume Data	15.60	2	7.800	37.04	0.000
Interaksi	2.44	4	0.610	2.90	0.038
Kesalahan	3.15	12	0.263		
Total	29.40	20			

Dari hasil analisis ANOVA pada Tabel 4, dapat disimpulkan bahwa ukuran kunci RSA dan volume data secara signifikan mempengaruhi waktu pemrosesan enkripsi dan dekripsi pada aplikasi *Shopee Pay* (nilai F untuk kedua variabel lebih besar dari F kritis, dengan $p < 0.05$). Selain itu, interaksi antara ukuran kunci dan volume data juga memberikan pengaruh signifikan terhadap kecepatan pemrosesan.

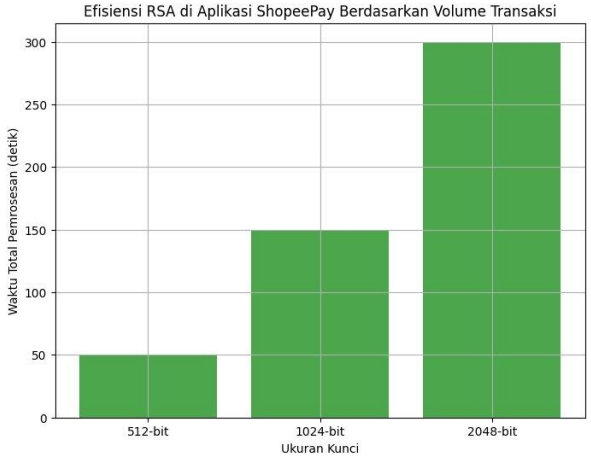
Tabel 4 ini memberikan perbandingan antara ukuran kunci RSA, volume data yang dienkripsi, serta waktu pemrosesan (enkripsi dan dekripsi) dan tingkat keamanan yang dihasilkan. Hasil menunjukkan bahwa ukuran kunci yang lebih besar memberikan keamanan yang lebih tinggi, tetapi juga meningkatkan waktu yang dibutuhkan untuk memproses data.

3.7 Evaluasi

Tabel 5 Efisiensi RSA di Aplikasi ShopeePay Berdasarkan Volume Transaksi

Ukuran Kunci	Volume Transaksi Harian	Waktu Total Pemrosesan (detik)	Tingkat Penggunaan CPU (%)	Efisiensi Sistem
512-bit	10.000	50	30%	Tinggi
1024-bit	10.000	150	45%	Sedang
2048-bit	10.000	300	60%	Rendah

Berdasarkan Tabel 5, volume transaksi yang tinggi memperbesar dampak ukuran kunci RSA terhadap efisiensi sistem. Kunci 512-bit memproses transaksi lebih cepat dengan penggunaan CPU rendah, namun keamanannya kurang memadai. Kunci 2048-bit menawarkan keamanan tinggi tetapi memerlukan waktu dan sumber daya lebih besar, yang menurunkan efisiensi. Kunci 1024-bit menunjukkan keseimbangan terbaik antara kecepatan dan keamanan, cocok untuk volume data harian di ShopeePay (100 KB hingga 1 MB). Untuk transaksi sensitif, kunci 2048-bit lebih disarankan meski memperlambat pemrosesan.



Gambar 2 Grafik Efiesiensi RSA di Aplikasi *Shoppe Pay* Berdasarkan Volume Transaksi

Dari hasil penelitian, kunci RSA 1024-bit optimal karena menyeimbangkan kecepatan dan keamanan. Kunci 512-bit terlalu cepat tetapi tidak aman, sementara 2048-bit memperlambat proses secara signifikan. Untuk transaksi yang lebih sensitif, kunci 2048-bit tetap diperlukan karena tingkat keamanan yang jauh lebih tinggi. Penelitian ini menunjukkan bahwa ukuran kunci RSA dan volume data berpengaruh signifikan pada kecepatan pemrosesan, dengan kunci 1024-bit sebagai solusi ideal untuk keseimbangan kecepatan dan keamanan di aplikasi *Shopee Pay*.

4. KESIMPULAN

Dari hasil pengujian, algoritma RSA dengan berbagai ukuran kunci menunjukkan variasi yang signifikan dalam hal kecepatan dan keamanan. Kunci RSA 512-bit, misalnya, mampu mengenkripsi data sebesar 100 KB dalam waktu 0,005 detik dan mendekripsinya dalam 0,004 detik, sedangkan untuk data 1 MB, enkripsi memerlukan 0,045 detik dan dekripsi 0,038 detik. Meski prosesnya cepat, kunci ini memiliki tingkat keamanan yang rendah dan rentan terhadap serangan *brute force*, yang dapat memecahkannya dalam satu hari. Di sisi lain, RSA 1024-bit menunjukkan keseimbangan yang lebih baik antara kecepatan dan keamanan. Untuk data 100 KB, proses enkripsi berlangsung selama 0,015 detik dan dekripsi 0,012 detik, sementara untuk data 1 MB, waktu enkripsinya mencapai 0,130 detik dan dekripsinya 0,110 detik. Keamanan RSA 1024-

bit berada pada tingkat menengah, dengan estimasi waktu pemecahan sekitar satu tahun menggunakan brute force. RSA 2048-bit, meskipun memiliki keamanan yang sangat tinggi dengan waktu pemecahan lebih dari satu miliar tahun, memerlukan waktu enkripsi dan dekripsi yang lebih lama. Pada data 100 KB, waktu enkripsi dan dekripsi masing-masing adalah 0,030 detik dan 0,025 detik, dan untuk data 1 MB, waktu enkripsi menjadi 0,260 detik dan dekripsi 0,210 detik. Dengan demikian, kunci RSA 1024-bit direkomendasikan karena dapat memberikan keseimbangan yang ideal antara kecepatan pemrosesan dan tingkat keamanan yang memadai, terutama untuk penggunaan pada aplikasi seperti *Shopee Pay*.

5. SARAN

Berdasarkan hasil analisa penelitian, beberapa saran yang bisa dijadikan peluang bagi penelitian selanjutnya adalah penelitian mendatang sebaiknya mempertimbangkan penerapan kombinasi algoritma RSA dengan metode enkripsi lain, seperti AES, untuk mengoptimalkan kinerja dan keamanan. Selain itu, pengujian penerapan algoritma pada berbagai platform dompet digital juga disarankan guna memberikan wawasan yang lebih luas dan mendalam terkait efektivitas RSA dalam berbagai skenario transaksi. Penelitian juga perlu mengevaluasi ukuran kunci RSA yang lebih bervariasi untuk menemukan keseimbangan yang ideal antara kecepatan dan keamanan. Lebih lanjut, fokus penelitian pada pengujian RSA terhadap serangan siber terbaru sangat penting untuk memastikan sistem tetap aman.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tim Redaksi Jurnal Teknika Politeknik Negeri Sriwijaya yang telah memberi memberi kesempatan, sehingga artikel ilmiah ini dapat diterbitkan.

DAFTAR PUSTAKA

[1] Rafli, M. F., Panjaitan, Z., & Riansah, W., 2024. Aplikasi Keamanan Sistem Pengiriman Tagihan Pembayaran Online (Invoice) Berbasis Website dengan algoritma RSA-CRT. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, No.1,Vol.*23*,138-146 https://ojs.trigunadharma.ac.id/index.php/jis/article/view/9604.

[2] Brahmanta, G. P., & Wardhani, N. I. K. (2021). Pengaruh persepsi kebermanfaatan, kemudahan, risiko terhadap minat menggunakan ulang shopeepay di Surabaya. Sains Manajemen: Jurnal Manajemen Unsera, 7(2), 97-108, https://e-jurnal.lppmunsera.org/index.php/SM/article/view/3580.

[3] Christian, C., Sitorus, S. H., & Nirmala, I., 2023. Implementasi Algoritma RSA Dan One Time Password (OTP) Untuk Pengamanan Data Pengguna dan Proses Transaksi pada Website E- Commerce. *Coding Jurnal Komputer dan Aplikasi*,No.1,Vol.11,62-72, https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/58684.

[4] Syifauddin, M.R., Kusomodestoni, R.H., Sarwindo., 2024. Penerapan Algoritma Rivest Shamir Aldeman (RSA) untuk Pengamanan Data Gambar Nasabah BMT Al-Hikmah Permata, *Jurnal Minfo Polgan*, No.1, Vol.13, 726-741, https://jurnal.polgan.ac.id/index.php/jmp/article/view/13805.

[5] Andriani, K., & Hayadi, B. H., 2022. Pengamanan Data Penjualan Dengan Kriptografi Algoritma Rivest Shamir Adleman (RSA) Pada Toko Baju Family. *Journal of Science and Social Research*, No. 3, Vol. 5, 664-670, https://jurnal.goretanpena.com/index.php/JSSR/article/view/1018.

[6] Alzaidan, M. S. Evaluasi dan Analisis Penggunaan Algoritma RSA pada Penyimpanan Password di MongoDB.

[7] Rivai, M,R., 2022. Penerapan Algoritma Rivest Shamir Adleman Pada IPSEC (Internet Protocol Security) Untuk Router Dalam Perluasan Jaringan, *Skripsi*, Program Sarjana Teknik Informatika, Univ. Binaniaga Indonesia, Bogor.

[8] Fajrin, A. M., Kelvin, C., Owen, B., & Aji, B., 2024. Perbandingan Performa dari Algoritma AES dan RSA dalam Keamanan Transaksi. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*,No.2, Vol.5, 696-705, https://tunasbangsa.ac.id/pkm/index.php/kesatria/article/view/379.

[9] Widiyasari, E,K., 2022, Perbandingan Algoritma RSA dan Merkle Hellman Dalam Rancang Bangun Aplikasi Penyandian Pesan Teks, *Skripsi*, Program Sarjana Sistem Komputer, Univ. Pembangunan Panca Budi, Medan.

[10] Ghazanfar, G. F. Evaluasi Kinerja dan Keamanan Penggunaan Algoritma Kriptografi HMAC SHA-3 dan RSA dalam Implementasi JSON Web Token (JWT).

[11] Christian, C., Sitorus, S. H., & Nirmala, I. 2023. Implementasi Algoritma RSA Dan One Time Password (OTP) Untuk Pengamanan Data Pengguna dan Proses Transaksi pada Website E-Commerce. Coding Jurnal Komputer dan Aplikasi, 11(1), 62-72, https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/58684

[12] Mahardika, B.T., & Alfian, M.R., 2024. Penerapan Algoritma Kriptografi Untuk Pengamanan Dokumen Transaksi Dengan Metode Rivest Shamir Adleman, *Jurnal Sains & Teknologi*, No.1, Vol.12, 212-220, https://unsada.e-journal.id/jst/article/view/339.

[13] Dairi, M. S., & Asih, M. S., 2023. Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan. *Jurnal Ilmu Komputer dan Sistem Informasi*, Vol. 2, No.1, 214-223 https://jurnal.unity-academy.sch.id/index.php/jirsi/article/view/44.

[14] Wahyudi, R., & Ristian, U. 2024. Pengamanan Tanda Tangan Digital Dalam QR Code Berbasis Website Menggunakan Metode RSA (Studi Kasus: Kantor Desa Parit Baru). JUPITER: Jurnal Penelitian Ilmu dan Teknologi Komputer, 16(1), 181-193 https://jurnal.polsri.ac.id/index.php/jupiter/article/view/8402.

[15] Raya, Y. C., & Arfida, S. 2024. Penerapan Algoritma Decision Tree C4. 5 Untuk Penerimaan Beasiswa Kip Bagi Mahasiswa Baru Berbasis Website: Penerapan Algoritma Decision Tree C4. 5. TEKNIKA: Jurnal Ilmiah Bidang Ilmu Rekayasa, 18(2), 377-388, https://jurnal.polsri.ac.id/index.php/teknika/article/view/8658.