Terjemahan dari artikel 10.22146/jnteti.vol13i4.12867

Perbadingan Keamanan Transaksi Seluler Menggunakan NFC dan Kode QR

Lucia Nugraheni Harnaningrum[1], Kristoforus Nanda Mahardhian[1]

[1] Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia, Bantul, D.I. Yogyakarta 55198, Indonesia

[Diserahkan: 12 Mei 2024, Direvisi: 18 Juli 2024, 2024, Diterima: 9 Oktober 2024]
Penulis Korespondensi: Lucia Nugraheni Harnaningrum (email: ningrum@utdi.ac.id)

INTISARI — Transaksi menggunakan perangkat seluler merupakan hal yang lumrah saat ini. Kode *quick-response* (QR) dan *near-field communication* (NFC) adalah metode pembayaran nontunai dan nonkontak yang populer. Kedua metode pembayaran ini memiliki karakteristik masing-masing. Pembayaran NFC menggunakan *secure element* yang mengenkripsi data kredensial untuk memastikan transaksi yang aman. Sebaliknya, sistem pembayaran kode QR mengirimkan data asli tanpa enkripsi. Dengan kata lain, data yang dikirim antarperangkat merupakan data asli. Mengingat luasnya penggunaan metode ini, pengamanan data transaksi sangatlah penting guna mencegah pencurian dan penyalahgunaan. Tingkat keamanan setiap transaksi penting untuk diketahui dan dibandingkan, sehingga diperoleh rekomendasi terbaik. Studi ini melakukan analisis komparatif tentang keamanan dan kinerja model pembayaran seluler berbasis NFC dan kode QR. Studi ini menemukan bahwa transaksi NFC memerlukan waktu untuk enkripsi selama 1.074 ms, sedangkan transaksi kode QR membutuhkan 5,9359 ms. Nilai entropi, yang menunjukkan keacakan data, untuk NFC dan kode QR adalah masing-masing 3,96 dan 3,23. Nilai p, yang menunjukkan signifikansi statistik, untuk NFC dan kode QR adalah masing-masing 0,45 dan 0,069. Kedua metode pembayaran menunjukkan tingkat keamanan yang dapat diterima, dengan waktu pemrosesan dan keacakan data dalam rentang yang memuaskan. Namun, analisis menyimpulkan bahwa transaksi NFC menawarkan kinerja yang lebih unggul dalam hal waktu pemrosesan dan keamanan data dibandingkan dengan transaksi kode QR.

KATA KUNCI — NFC, QR, *Secure Element*, Enkripsi, Keacakan Data.

I. PENDAHULUAN

Transaksi melalui perangkat seluler merupakan hal yang lumrah di kalangan masyarakat saat ini. Perangkat seluler dengan segala fasilitasnya sudah menjadi kebutuhan pokok bagi masyarakat. Menurut survei Statistica, pembayaran seluler di Indonesia, khususnya yang menggunakan kode *quick-response* (QR), mencapai 50% dari seluruh pembayaran seluler yang ada. Di Amerika Serikat, pembayaran dengan kode QR merupakan metode pembayaran yang populer berdasarkan data statistik. Pembayaran dengan perangkat seluler *near-field communication* (NFC) mulai populer saat pandemi COVID-19 melanda dunia. Data statistik menunjukkan bahwa pada tahun 2018 pengiriman *secure element* NFC mencapai 620 juta unit di seluruh dunia.

Kode QR telah banyak digunakan dalam berbagai bidang aktivitas, termasuk pemantauan pasien [1], pemasaran dengan perangkat seluler [2], sistem manajemen inventaris [3], sistem pembayaran seluler [4], dan transportasi [5]. Transaksi menggunakan kode QR juga lebih banyak digunakan karena saat ini ponsel pintar dilengkapi dengan kamera yang dapat digunakan untuk memindai kode QR.

Meskipun memiliki kemiripan dalam hal pembayaran nontunai dan nonkontak, kode QR dan NFC memiliki karakteristiknya masing-masing. Pembayaran dengan NFC menggunakan *secure element*. *Secure element* memastikan bahwa pembayaran dilakukan dengan aman dan data kredensial dienkripsi. Di sisi lain, pembayaran dengan kode QR tidak menggunakan enkripsi. Data yang ada dikirim antarperangkat dalam bentuk data asli. Transaksi saat ini mengakomodasi pembayaran menggunakan banyak metode. Data di atas menunjukkan bahwa kode QR dan NFC merupakan metode pembayaran yang banyak digunakan. Namun, pengguna harus berhati-hati terhadap pencuri yang mengeksploitasi data transaksi untuk merugikan pelanggan dan penjual. Oleh karena itu, sangatlah penting untuk mengamankan data selama transaksi.

Penelitian ini mengulas transaksi menggunakan NFC dan kode QR, khususnya dari perspektif keamanan. Keamanan yang diulas adalah kerahasiaan data dan kecepatan transaksi. Dengan membandingkan dua metode, diharapkan dapat diketahui kelebihan dan kekurangan serta metode yang terbaik, sehingga meminimalkan kemungkinan pencurian data dan penggunaan data oleh orang lain. Penelitian terkait transaksi menggunakan NFC telah dilakukan sebelumnya. Penelitian ini menguji transaksi seluler menggunakan kode QR. Hasil yang diperoleh kemudian dibandingkan dengan penelitian sebelumnya.

Transaksi pembayaran seluler yang aman merupakan hal yang penting. Seiring dengan makin banyaknya transaksi, keamanan juga harus ditingkatkan. Tingkat keamanan tiap transaksi harus diketahui dan dibandingkan untuk dapat memberikan rekomendasi terbaik. Penelitian ini membandingkan model transaksi pembayaran seluler menggunakan NFC dan kode QR.

II. PROTOKOL PENGGUNAAN NFC DAN KODE QR

Penelitian tentang transaksi seluler menggunakan NFC dan kode QR telah dilakukan sebelumnya. Studi mengenai protokol pembayaran NFC mengungkapkan adanya kerentanan, seperti *random-access memory* (RAM) *scraping*, *denial of service* (DOS), *distributed denial of service* (DDOS), dan serangan *phlashing*. Selain itu, protokol pembayaran ini mengatasi kelemahan aplikasi seluler yang terkenal, seperti Heartbleed dan ROBOT [6]. Penelitian lain mengembangkan protokol keamanan untuk transaksi *automatic teller machine* (ATM) menggunakan NFC pada perangkat seluler [7]. Penelitian ini

menyempurnakan *dynamic array PIN protocol* (DAP), yang rentan terhadap penyadapan video atau perekaman kamera tertentu. Penyempurnaannya difokuskan pada proses autentikasi PIN di ATM untuk memperkuat keamanan transaksi NFC. Efektivitas solusi keamanan yang diusulkan dibuktikan dengan kegagalan penyerang untuk mengenali PIN yang benar melalui serangan *intersection multiple records*.

Penggunaan lain teknologi NFC adalah penggunaannya pada sensor epidermis fleksibel. Sensor ini menggunakan protokol NFC yang dibuat khusus dan diuji untuk melakukan pengawasan terhadap tingkat kortisol di dalam keringat [8]. Prototipe ini memanfaatkan komunikasi frekuensi tinggi (*high frequency*, HF), sehingga memastikan bahwa prototipe tersebut tangguh terhadap variabilitas dan dapat mempertahankan komunikasi pengguna yang konsisten. Prototipe ini mencapai jangkauan deteksi sekitar 3,5 hingga 4 cm untuk setiap pengguna dan titik aplikasi pada tubuh. Pengujian awal sensor mengonfirmasi keandalan data yang dikumpulkan, yang setara dengan perangkat yang jauh lebih mahal.

Teknologi NFC juga telah digunakan pada *battery management system* (BMS) [9]. Studi ini menggunakan teknologi NFC untuk menyajikan sistem baru pada transfer data yang aman antara BMS dan pembaca seluler. Desain ini bekerja dengan baik pada pengaturan BMS aktif dan pasif, baik menggunakan pengontrol standar maupun paket baterai termodulasi. Sistem ini menggabungkan catatan keamanan *secure NFC data exchange format* (SNDEF) dan pendekatan enkripsi simetris ringan untuk memastikan autentikasi, kerahasiaan data, dan integritas selama pembacaan seluler. Tantangan yang dapat diatasi termasuk permasalahan masa pakai baterai, penyimpanan, penggunaan ulang, dan kabel. Penelitian ini menyarankan peningkatan desain BMS tradisional dengan mengintegrasikan NFC untuk memungkinkan pembacaan status paket baterai secara nirkabel. Selain itu, penelitian ini menambahkan lapisan keamanan ringan ke protokol NFC untuk memastikan bahwa paket baterai dikelola hanya oleh perangkat yang diizinkan dan data aman dari intersepsi dan modifikasi eksternal.

Teknologi NFC juga digunakan bersama dengan kode QR. Kode QR membuat token pelanggan atau PIN untuk transaksi [4]. Pelanggan membuatnya saat mengantre pembayaran di penjual. Saat pembayaran dimulai, penjual menunjukkan kode QR. Pelanggan kemudian memindai kode ini dan kunci pribadi satu arah dibuat dengan data pedagang, yang kemudian dikirimkan ke penjual menggunakan komunikasi NFC. Transaksi selanjutnya kemudian disetujui. Data ini kemudian diteruskan ke pihak ketiga, yang seharusnya dapat menyelesaikan transaksi tanpa verifikasi tambahan. Model pembayaran menentukan beberapa kemungkinan, yaitu operator seluler menagih pelanggan, bank pelanggan menangani transfer dana, atau penyedia layanan memfasilitasi transfer dana dari pelanggan ke bank pedagang.

Langkah-langkah keamanan tambahan, seperti memasukkan PIN, dapat diterapkan ketika memindai kode QR pelanggan. Akan tetapi, langkah ini sering kali tidak diperlukan karena ponsel biasanya terkunci. Proses pemindaian mengautentikasi identitas pelanggan dan membatasi jumlah transaksi. Selain itu, tidak adanya jabat tangan untuk mengonfirmasi transaksi antara pihak ketiga dan pelanggan diharapkan dapat mempercepat waktu pemrosesan dibandingkan dengan pembayaran kartu kredit. Penelitian ini bertujuan untuk mengatasi masalah kecepatan pemrosesan dan keamanan. Pendekatan dalam makalah ini dapat diadaptasi di keempat model pembayaran seluler yang dibahas—tidak adanya jabat tangan untuk konfirmasi pembayaran menghasilkan pemrosesan yang lebih cepat daripada transaksi kartu kredit tradisional. Namun, keamanan yang diusulkan dirancang agar sama kuatnya dengan pembayaran kartu kredit.

NFC dan kode QR makin banyak digunakan dalam sistem pembayaran transportasi umum [5]. Dengan perkembangan internet, bersama dengan teknologi NFC dan kode QR, sistem pembayaran baru untuk angkutan umum telah diluncurkan. Sistem ini terintegrasi dengan sistem perbankan dan tiket untuk memfasilitasi perjalanan yang lebih cepat dan efisien. Penelitian ini meningkatkan sistem dengan menggabungkan teknologi NFC dan kode QR dengan kartu *integrated circuit* (IC) untuk mengatasi keterbatasan yang ada. Penelitian ini menciptakan platform yang mendukung interkoneksi pembayaran di ketiga teknologi tersebut. Fungsionalitas sistem diverifikasi melalui simulasi registrasi, proses *login*/*logout*, dan transaksi pembayaran untuk memastikan keamanan dan fungsionalitas. Temuan penelitian menunjukkan bahwa sistem dapat memenuhi beragam kebutuhan pengguna dan menerima berbagai metode pembayaran secara bersamaan, sehingga menawarkan pengalaman yang lebih komprehensif dan memuaskan kepada penumpang.

Penggunaan kode QR sebagai sistem pembayaran telah diuji pada penelitian terdahulu [10]. Studi ini merinci desain dan implementasi sistem pembayaran yang aman menggunakan kode QR, yang makin popular karena kemampuannya memperlancar proses pembayaran dan meningkatkan kenyamanan pengguna. Terlepas dari kelebihannya, sistem pembayaran berbasis kode QR rentan terhadap ancaman keamanan. Proses transaksi harus cukup tangguh untuk menjaga integritas dan kerahasiaan setiap pembayaran. Sistem pembayaran *online* juga harus memverifikasi keaslian pengirim dan penerima di setiap transaksi. Makalah ini memperkenalkan solusi keamanan untuk sistem berbasis QR yang diusulkan menggunakan kriptografi. Sistem ini meliputi aplikasi seluler dan server gerbang pembayaran yang menggunakan kriptografi visual untuk menyediakan antarmuka pengguna yang mudah dan aman guna melakukan transaksi pembayaran.

III. TRANSAKSI MENGGUNAKAN NFC DAN KODE QR

A. PERBANDINGAN TRANSAKSI MENGGUNAKAN NFC DAN KODE QR

Tabel I membandingkan pengodean NFC dan kode QR. NFC memiliki sistem keamanan yang relatif baik dan sistem protokol transaksi yang sudah lama ada dibandingkan dengan perangkat NFC. NFC juga memiliki standar protokol berdasarkan International Organization for Standardization (ISO). Hal ini membuat NFC cukup dikenal dan dipercaya. Sementara itu, pengodean menggunakan kode QR masih dalam tahap pengembangan dan banyak celah keamanan yang dapat mengancam transaksinya.

B. POTENSI ANCAMAN KEAMANAN KODE QR

Contoh terjadinya eksploitasi dan penyalahgunaan kode QR sudah banyak. Peretas dan pihak-pihak yang tidak bertanggung jawab sering menggunakan kode QR sebagai metode untuk meluncurkan serangan. Bentuk eksploitasi yang umum terjadi melibatkan penyematan URL berbahaya ke dalam kode QR. Ancaman keamanan yang paling umum terkait kode QR meliputi serangan *malware*, percobaan *phising*, *bug* kode QR, dan pencurian finansial. Pengguna kode QR harus memastikan

TABEL I
PERBANDINGAN PENGODEAN MENGGUNAKAN NFC DAN KODE QR

NFC	Kode QR
Secara *default* NFC melakukan enkripsi yang meningkatkan keamanan transaksi pembayaran secara singnifikan. NFC juga beroperasi pada jarak yang pendek yang membatasi kemampuan peretas untuk memotong data selama transfer menggunakan NFC.	Kode QR dapat dienkripsi, tidak ada cara untuk mengetahui apakah ada atau tidak, artinya terserah pengguna untuk menilai apakah kode tertentu mungkin aman.
Tag NFC harus berisi chip yang disandikan agar dapat dibaca oleh perangkat.	Kode QR bebas dibuat melalui situs web atau aplikasi.

bahwa generator kode QR aman. Generator kode QR aman jika platform yang digunakan untuk membuatnya menyediakan fitur yang tepat dan memiliki reputasi yang baik. Langkah terbaik adalah memastikan keamanan dan privasi dengan tetap waspada. Pemindaian kode QR dilakukan menggunakan kamera dan kode QR yang dipindai harus berada dalam bidang pandang kamera.

C. MODEL ENKRIPSI DAN ENKAPSULASI DATA

Data yang dikirimkan dari ponsel ke *point of sale* (POS) pertama-tama dienkripsi dan dienkapsulasi. Setelah data mencapai POS, data tersebut didekodekan untuk mengambil data asli. Model yang diusulkan ini menggunakan data pengguna ponsel dan data kartu. Data disimpan, dienkripsi, dikirim, dan diterima dalam bentuk terenkripsi. Data didekripsi hanya saat transaksi dilakukan. Data tersebut dihapus setelah transaksi selesai karena data dekripsi hanya disimpan dalam variabel.

Enkripsi dilakukan dengan menggunakan algoritma kriptografi *advanced encryption standard* (AES) dan Rivest-Shamir-Adleman (RSA) yang diuji menggunakan protokol transaksi. AES digunakan karena algoritma kriptografi simetris bersifat ringan. Sementara itu, RSA digunakan dalam proses transaksi karena algoritma kriptografi asimetris lebih cocok untuk pertukaran data jarak dekat [11]. Algoritma yang dipilih bersifat lugas, ringan, dan memiliki parameter yang dapat disesuaikan. Algoritma tersebut dipilih karena sederhana dan kebutuhan sumber dayanya minimal. Selain itu, keamanan dapat ditingkatkan dengan mengubah parameter untuk setiap transaksi baru.

D. ANALISIS DESAIN DARI HASIL UJI MODEL

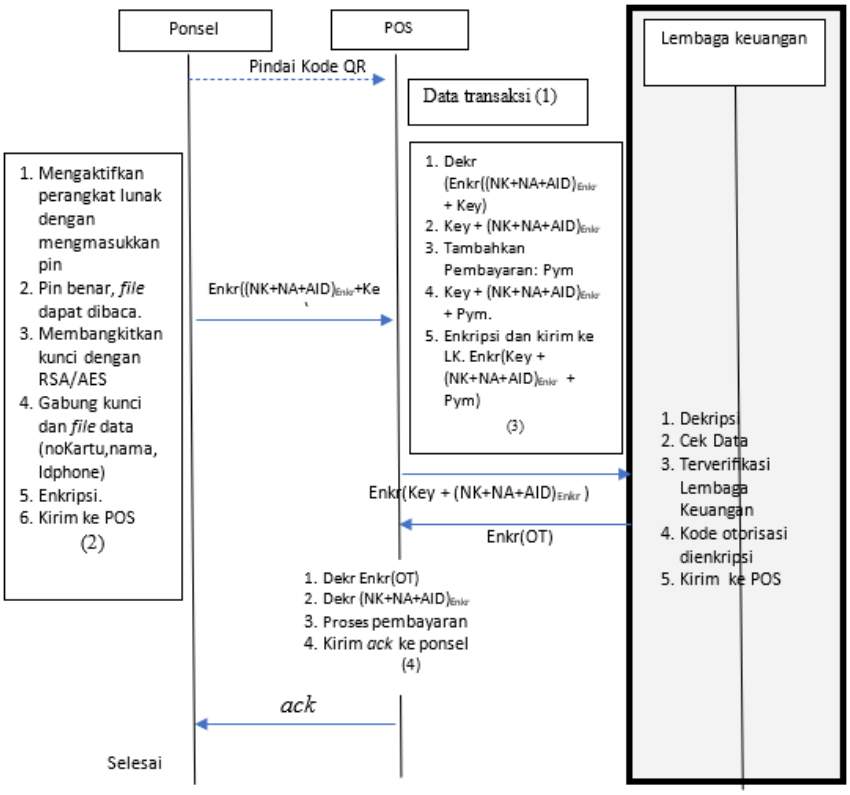
Model transaksi yang dibangun menggunakan kode QR didasarkan pada keamanan dan kecepatan. Keamanan diuji dengan menganalisis keacakan data. Kecepatan diuji karena proses yang lebih cepat mengurangi peluang serangan. Model ini diuji pada ponsel Android dengan berbagai merek, ukuran memori, dan versi. Hasil pengujian dianalisis menggunakan metode yang akan dijelaskan kemudian. Model ini mengacu pada model transaksi menggunakan NFC yang telah diuji dan diperoleh hasilnya [12]. Kemudian, hasil yang diperoleh dalam penelitian ini dibandingkan dengan hasil pengujian pada [12].

Berikut ini adalah analisis keamanan yang menggabungkan pengujian keacakan data. Tingkat keamanan data terenkripsi dapat dianalisis untuk mengetahui keacakannya. Data acak menyulitkan penyerang untuk menginterpretasikan data meskipun penyerang berhasil menangkapnya. Penyerang hanya dapat memperoleh data asli jika mengetahui metode dan parameter enkripsi, termasuk kunci enkripsi. Data diuji untuk mengetahui keacakannya menggunakan uji monobit untuk memperoleh nilai p dan entropi analisis ini. Analisis keacakan data dilakukan dengan menggunakan metode uji frekuensi (monobit) [13]. Parameter uji keamanan ditunjukkan pada Tabel II.

TABEL II
PARAMETER UJI KEAMANAN

Parameter Uji	Artikel Pendukung	Penjelasan	Tujuan
Nilai p	[11] [13]	Jika nilai p < 0,01 tidak acak dan sebaliknya	Untuk mengetahui data hasil enkripsi sudah masuk kategori *unpredictable*
Entropi Shannon	[11] [14]	Nilai entropi mendekati 2^n dengan n adalah banyaknya probabilitas bit	Untuk mengetahui data hasil enkripsi sudah masuk kategori *unpredictable*
Waktu pemrosesan	[14]	Waktu tercepat untuk faktorisasi saat ini adalah 17,5 ms dengan n = 500	Untuk memastikan bahwa waktu proses di bawah waktu yang diperlukan penyerang untuk mengartikan data, seandainya penyerang berhasil mengambil data.
Ketahanan terhadap serangan faktorisasi dan perhitungan statistik	[15] [13]	Proses faktorisasi dan perhitungan statistik masih perlu waktu yang lama.	Untuk mengetahui nilai keacakan dapat bertahan terhadap serangan.
Mutual autentikasi	[16] [17] [18] [19] [20]	Pihak-pihak yang terlibat dipastikan dapat dipercaya.	Memastikan pengiriman data berasal dan ditujukan kepada pihak yang benar atau tepat.
Tingkat keamanan dan autentikasi	[16] [17]	Data yang aman membuat pengguna percaya.	Memastikan data yang dikirimkan antarpihak mempunyai lapisan keamanan yang baik.

Parameter uji entropi Shannon menjelaskan bahwa nilai entropi mendekati 2^n, dengan n adalah jumlah bit probabilitas [11], [14]. Parameter ini menentukan data yang dienkripsi masuk ke dalam kategori tidak terduga atau tidak. Mengenai parameter waktu pemrosesan [14], waktu tercepat untuk faktorisasi adalah 17,5 ms dengan n = 500. Parameter tersebut



Gambar 1. Model transaksi tanpa koneksi internet antara ponsel dan POS (dimodifikasi dari [12]).

memastikan bahwa waktu pemrosesan lebih cepat daripada waktu yang dibutuhkan penyerang untuk menafsirkan data. Mengenai ketahanan terhadap serangan faktorisasi dan perhitungan statistik [15], [13], proses faktorisasi dan perhitungan statistik masih membutuhkan waktu yang lama. Parameter ini menentukan nilai keacakan yang dapat bertahan terhadap serangan. Parameter autentikasi mutual pihak-pihak yang terlibat harus dijamin dapat dipercaya [16]–[20] karena parameter tersebut digunakan untuk memastikan pengiriman data berasal dari dan ditujukan kepada pihak yang benar atau tepat. Parameter keamanan dan tingkat autentikasi serta data yang aman membuat pengguna percaya [16], [17]. Parameter ini memastikan bahwa data yang dikirim antarpihak memiliki lapisan keamanan yang baik.

Kecepatan dibandingkan dengan waktu yang dibutuhkan penyerang untuk mencari kunci enkripsi. Jika waktu pemrosesan data lebih singkat daripada waktu pencarian kunci enkripsi, data tersebut dianggap aman. Serangan yang dilakukan oleh penyerang dapat terjadi dengan melihat waktu yang dibutuhkan untuk memperoleh informasi tentang kunci atau teks biasa. Jika waktu pemrosesan cepat, serangan dapat dihindari.

IV. HASIL DAN DISKUSI

A. ARSITEKTUR MODEL TRANSAKSI

Model keamanan transaksi seluler diterapkan pada transaksi dengan NFC. Model yang sama juga diterapkan pada kode QR. Kode QR digunakan karena semua ponsel memiliki kamera yang memungkinkannya memindai kode QR. Keunggulan ini, ditambah dengan manfaat transaksi NFC yang menggunakan enkripsi dan tidak memerlukan koneksi internet, menjadikan transaksi lebih aman.

Sistem pembayaran seluler yang menggunakan kode QR menjalani pengujian selama fase transaksi. Kartu pembayaran yang disimpan di ponsel dengan aman siap digunakan untuk transaksi. Model transaksi memastikan pertukaran yang aman dan akurat antara ponsel dan POS. Arsitektur model transaksi ditunjukkan pada Gambar 1.

Model transaksi ini menggabungkan sistem keamanan di dalam ponsel. Sistem keamanan, sebuah aplikasi yang didesain untuk melindungi data dan komunikasi antara ponsel dan POS, dibuat menggunakan komponen yang dipasang dalam ponsel. Komponen-komponen yang ada di kedua perangkat diuji dan dimodifikasi untuk diintegrasikan dengan aplikasi sistem keamanan.

Model transaksi ini menggunakan data yang disimpan di dalam ponsel dan memastikan keamanannya, khususnya ketika menggunakan komunikasi kode QR. Dua langkah diterapkan untuk mencegah serangan, yaitu melindungi data dari akses yang tidak diizinkan dan memastikan perutean permintaan data sudah benar. Sistem keamanan transaksi meliputi tiga entitas, yaitu ponsel, POS, dan lembaga keuangan. Studi ini fokus pada pengamanan transaksi antara ponsel dan POS.

Pada langkah pertama, POS mengubah data jumlah pembelian ke dalam bentuk kode QR dan menampilkannya ke layar POS. Ketika POS menampilkan data kode QR, ponsel memindai kode QR menggunakan aplikasi transaksi. Pada langkah kedua, ponsel memproses data kartu, mengenkripsinya, dan mengubah data terenkripsi ke bentuk kode QR. Pada langkah ketiga, POS memindai kode QR ponsel. Selanjutnya, POS mengautentikasi dan meneruskan data kartu ke server lembaga keuangan. POS menerima pemberitahuan persetujuan dari lembaga keuangan, mendekripsinya, dan data pembayaran ditambahkan, sebagaimana ditunjukkan pada (1).

$$D_{trans} = D_{user} + D_{pay} \quad (1)$$

dengan D_{trans} adalah data yang digunakan untuk transaksi, D_{user} adalah data pengguna, dan D_{pay} adalah data pembayaran. POS mengenkripsi data dan mengirimkannya ke lembaga keuangan, seperti yang ditunjukkan (2).

$$E_{trans} = (RV, D_{trans}). \quad (2)$$

E_{trans} adalah data transaksi terenkripsi dan $E(RV, D_{trans})$ adalah data angka acak yang diperoleh selama transaksi.

Pada lembaga keuangan, data didekripsikan dan diperiksa berdasarkan catatan nasabah. Jika lembaga keuangan mengonfirmasi kecocokannya, kode otorisasi terenkripsi diperoleh. Jika tidak diverifikasi, pesan yang menginformasikan kurangnya verifikasi dikirim. Lembaga keuangan kemudian mengomunikasikan data atau pemberitahuan yang relevan ke POS.

Pada langkah keempat, POS memproses pembayaran dan memberi tahu ponsel jika transaksi berhasil. Data autentikasi, data dari ponsel, dan pengguna didekripsi. Selanjutnya, transaksi pembayaran dijalankan. Proses ini diakhiri dengan pemberitahuan yang dikirim ke ponsel, dengan POS sebagai pengirim dan ponsel sebagai penerima.

Data yang dikirim dari ponsel ke POS awalnya dienkripsi dan dienkapsulasi. Setelah mencapai POS, data ini didekode untuk mendapatkan konten asli. Enkripsi dilakukan menggunakan algoritma kriptografi RSA. Algoritma yang dipilih tidak rumit dan ringan serta memiliki parameter yang dapat dimodifikasi, sehingga ideal untuk perangkat seperti ponsel yang kapasitas memorinya terbatas.

Sementara itu, opsi parameter dapat dimodifikasi untuk meningkatkan keamanan dengan mengubah nilai parameter untuk setiap transaksi baru. Model ini juga diuji menggunakan algoritma enkripsi AES. AES dipilih karena transaksi bersifat tertutup dan kunci enkripsi dapat dibagikan antara dua perangkat yang berdekatan. Aplikasi seluler juga mendukung algoritma AES karena ringan.

Sampai tahap ini, model transaksi telah selesai. Model ini dirancang untuk transaksi rutin. Untuk mencegah serangan, data dienkripsi saat disimpan dan dikirim antarperangkat.

B. PENGEMBANGAN SISTEM UNTUK MODEL TRANSAKSI

Pengembangan model transaksi diterapkan ke dua perangkat, yaitu ponsel yang digunakan pengguna, yang telah memiliki data kartu yang aman; dan POS, yang menerima pembayaran dari proses transaksi. Langkah awal proses transaksi untuk POS adalah menentukan jumlah nominal yang ditransaksikan. Jumlah ini diubah ke bentuk kode QR pada POS, sehingga dapat dipindai oleh ponsel milik pengguna.

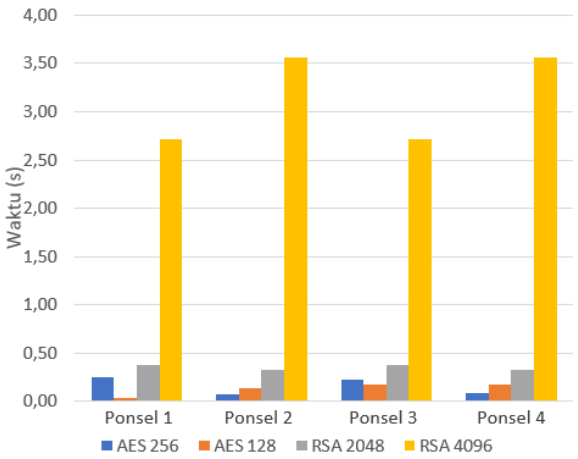
POS siap mengirimkan data transaksi; pengguna berada di laman transaksi setelah memasukkan PIN. Jika PIN diautentikasi, pengguna berada di laman transaksi. Saat masuk laman transaksi, kamera diaktifkan untuk membaca kode QR.

Transaksi dijalankan oleh pengguna dengan memindai kode QR dan menerjemahkan konten data. Ponsel pengguna menyiapkan data kartu, mengenkripsinya, dan mengubahnya ke dalam bentuk kode QR. POS menerima data kartu, menambahkan dengan data pembayaran, dan mengirimkannya ke server lembaga keuangan. Jika data terverifikasi, proses transaksi dilanjutkan dan lembaga keuangan mengirimkan pemberitahuan keberhasilan transaksi ke POS. POS menerima dan memproses transaksi yang sudah selesai.

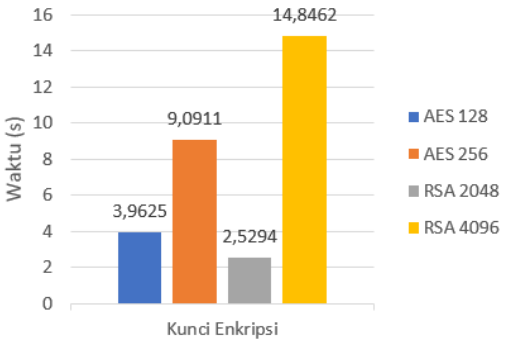
C. PENGUJIAN RUNTIME

Model transaksi yang diusulkan diuji pada ponsel dengan sistem operasi Android versi 8 dan 10. Parameter-parameter yang diuji meliputi waktu eksekusi dan analisis keacakan data menggunakan uji monobit.

Gambar 2 menunjukkan bahwa waktu enkripsi dipengaruhi oleh panjang kunci, memori, dan versi ponsel tanpa pola yang



Gambar 2. Waktu untuk membangkitkan kode QR.



Gambar 3. Waktu untuk memindai kode QR.

jelas. Waktu untuk memindai kode QR dengan AES dan RSA ditunjukkan pada Gambar 3. Kunci enkripsi RSA-4096 memerlukan waktu enkripsi terlama, sedangkan panjang kunci AES adalah 128. Waktu yang dibutuhkan untuk enkripsi dan pembuatan kode QR dengan RSA-4096 relatif lebih lama dibandingkan dengan panjang kunci dan metode enkripsi lainnya.

D. UJI MONOBIT DAN ENTROPI

Data yang digunakan untuk pengujian dibuat dengan ketentuan sebagai berikut. Data *ID* (*ID* kartu, *ID* perangkat, dan *ID* pengguna) dirancang dengan selisih antara data pertama dan kedua hanya satu karakter. Pemilihan ini dilakukan agar analisis dapat dilakukan dengan hanya mempertimbangkan perubahan yang mendekati satu bit.

Tabel III menyajikan nilai p dan Tabel IV menyajikan nilai entropi, yang menunjukkan bahwa hasil enkripsi data dinyatakan acak [11]. Nilai entropi berada di bawah 3, kecuali RSA-4096, sehingga data untuk analisis entropi tidak mendekati nilai acak. Dibandingkan dengan penelitian sebelumnya yang memiliki model transaksi serupa [19], waktu yang dibutuhkan untuk model transaksi dalam penelitian ini adalah 5,9359 ms, lebih cepat dibandingkan dengan model transaksi pada penelitian sebelumnya yang membutuhkan waktu 50 ms [19].

E. ANALISIS RESISTANSI TERHADAP SERANGAN FAKTORISASI

Resistansi terhadap serangan faktorisasi dapat dianalisis dengan menghitung kemungkinan proses yang terjadi untuk memperoleh kunci algoritma RSA. Total waktu pemrosesan transaksi dalam penelitian ini adalah 1,074 ms. Waktu untuk memfaktorkan adalah 4 jam untuk faktorisasi Fermat dan 1,98 jam untuk Pollards' rho.

TABEL III
NILAI P UNTUK BERBAGAI KONDISI PONSEL

Enkripsi	Ponsel 1	Ponsel 2	Ponsel 3	Ponsel 4	Kesimpulan
AES-128	0,0449	0,1228	0,0212	0,0884	Acak
AES-256	0,0398	0,0697	0,1129	0,0310	Acak
RSA-2048	0,0641	0,0683	0,0768	0,0768	Acak
RSA-4096	0,0641	0,0641	0,0777	0,0777	Acak

TABEL IV
NILAI ENTROPI UNTUK BERBAGAI KONDISI PONSEL

Enkripsi	Ponsel 1	Ponsel 2	Ponsel 3	Ponsel 4	Kesimpulan
AES-128	3,2617	3,2487	3,2971	3,2971	Acak
AES-256	3,2388	3,2838	3,2469	3,2686	Acak
RSA-2048	3,2468	3,2710	3,2468	3,2710	Acak
RSA-4096	3,2468	2,9894	3,2468	2,9894	Acak

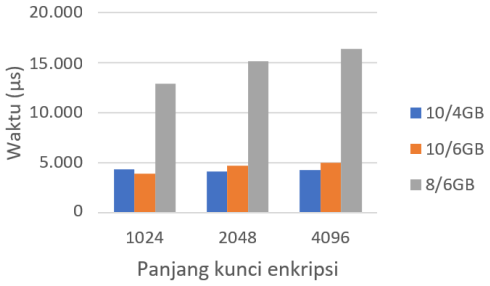
Ketika data dikirim ke server lembaga keuangan, pada ponsel dibuat kunci AES atau RSA. Kunci terenkripsi ini kemudian dicari nilai entropi dan nilai p-nya. Nilai entropi dan nilai p juga menunjukkan bahwa data dinyatakan acak. Data dinyatakan acak jika nilai p adalah 0,01 [11], [13]. Data yang telah dinyatakan acak dapat dikatakan aman karena untuk menginterpretasikan data acak, seseorang memerlukan kunci enkripsi. Kunci tersebut dapat diperoleh apabila seseorang dapat menebak kunci tersebut. Faktorisasi digunakan untuk melakukan hal tersebut.

Ketahanan terhadap serangan faktorisasi dapat diketahui dengan menganalisis ketahanan algoritma AES terhadap serangan *brute-force* [21]. Algoritma AES dengan kunci 128 bit memiliki kemungkinan kombinasi 3.403 × 1.038, sedangkan kunci 192 memiliki potensi kombinasi 6.278 × 1.057. Kunci 254 memiliki kemungkinan kombinasi 1.158 × 1.077. Superkomputer saat ini memiliki kapasitas *floating point operations per second* (PFLOPS) sebesar 33,86 [21], 415,5 [22], dan 488 [23]. Superkomputer tercepat saat ini adalah 415,5 PFLOPS, setara dengan 415,5 × 1.015 FLOPS. Oleh karena itu, algoritma AES dengan kunci 256 yang dipecahkan dengan kecepatan superkomputer membutuhkan waktu 7,525 × 1.052, dengan perhitungan 1 tahun = 31.536.000 s. Maka, dalam satu tahun dapat dihasilkan kombinasi kunci sebanyak 31.536.000 × 488 × 1.015 = 15.389.568 × 1.018 dan waktu yang dibutuhkan adalah 1.158 × 1.077 / 1,539 × 1.024 = 7,525 × 1.052. Algoritma AES dinyatakan aman terhadap serangan yang berupaya menguraikan data terenkripsi dengan cara menemukan kuncinya, bahkan jika upaya tersebut dilakukan oleh superkomputer tercepat saat ini.

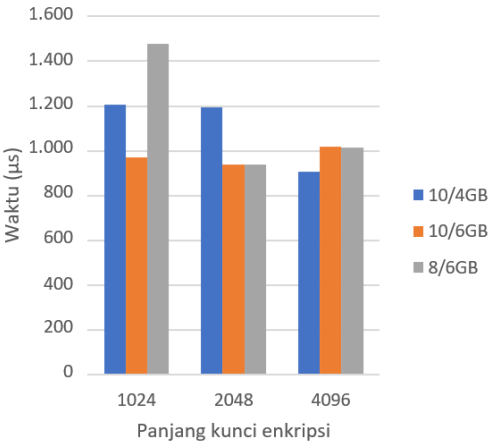
F. PERBANDINGAN TRANSAKSI MENGGUNAKAN NFC DAN KODE QR

Hasil uji coba transaksi menggunakan kode QR dibandingkan dengan transaksi menggunakan NFC. Penelitian sebelumnya telah melakukan uji coba transaksi dengan NFC, dengan hasil seperti yang ditunjukkan pada Gambar 4, Gambar 5, Tabel V, dan Tabel VI.

Waktu yang dibutuhkan jauh kurang dari 1 s, dengan rata-rata menurut pengujian sebesar 1,074 ms (Gambar 4 dan Gambar 5). Waktu untuk membuat enkripsi dan kode QR adalah 5,9359 ms. Meskipun terdapat perbedaan yang signifikan dalam durasi transaksi NFC dan kode QR, keduanya masih dalam batas keamanan yang dapat diterima. Durasi ini jauh lebih singkat dibandingkan dengan waktu yang diperlukan penyerang untuk mengakses dan mendekode data terenkripsi,



Gambar 4. Waktu enkripsi data pada ponsel dengan NFC.



Gambar 5. Waktu untuk mengirimkan data pelanggan ke POS menggunakan NFC-*host card emulation* (HCE).

TABEL V
NILAI P UNTUK BERBAGAI KONDISI PONSEL DENGAN NFC

N	Nilai p			Kesimpulan
	10/4 GB	*10/6 GB*	*8/6 GB*	
1024	0,456868	0,429522	0,454812	Acak
2048	0,456868	0,426614	0,454812	Acak
4096	0,472147	0,447746	0,454812	Acak

TABEL VI
NILAI ENTROPI UNTUK BERBAGAI KONDISI PONSEL DENGAN NFC

N	Entropi			Kesimpulan
	10/4 GB	*10/6 GB*	*8/6 GB*	
1024	3,955636	3,959980	3,955243	Acak
2048	3,955636	3,960128	3,955243	Acak
4096	3,956296	3,960702	3,955243	Acak

yang melebihi 1 s. Interval ini jauh lebih singkat daripada waktu minimum penyerang untuk menyelesaikan proses faktorisasi menggunakan berbagai metode. Algoritma Fermat membutuhkan waktu 7,2 ms, sedangkan waktu untuk algoritma lain melebihi hasil ini.

Nilai entropi dan nilai p untuk transaksi menggunakan NFC dan kode QR pada Tabel V dan Tabel VI juga menunjukkan bahwa data terenkripsi dinyatakan acak. Berdasarkan nilai ini, nilai entropi dan nilai p transaksi dengan NFC lebih tinggi daripada kode QR.

Waktu yang dibutuhkan untuk enkripsi transaksi dengan NFC adalah 1.074 ms, sementara kode QR adalah 5,9359 ms. Nilai entropi transaksi menggunakan NFC adalah 3,96, sementara pada kode QR, nilai entropinya adalah 3,23. Nilai p pada transaksi menggunakan NFC adalah 0,45, sementara pada kode QR adalah 0,069. Perbedaan pada kecepatan disebabkan oleh pembacaan kode QR yang memerlukan pengenalan pola, sementara NFC langsung membaca data yang dikirimkan.

Perbandingan NFC dan kode QR menunjukkan bahwa transaksi NFC lebih baik daripada kode QR. Namun, keduanya masih dalam batas waktu dan keacakan data yang aman. Berdasarkan hasil dan analisis hasil uji coba, protokol transaksi dengan NFC dan kode QR dapat digunakan untuk mencegah serangan yang akan mengambil dan mengeksploitasi data.

V. KESIMPULAN

Protokol transaksi seluler dapat dilakukan menggunakan NFC dan kode QR. Penelitian ini membandingkan kinerja keduanya, yang meliputi waktu pemrosesan dan keacakan data. Durasi enkripsi untuk transaksi NFC adalah 1.074 ms, sedangkan untuk kode QR adalah 5,9359 ms. Nilai entropi untuk transaksi NFC adalah 3,96, sedangkan untuk kode QR adalah 3,23. Nilai p untuk transaksi NFC adalah 0,45, sedangkan untuk kode QR adalah 0,069. Hasil penelitian menunjukkan bahwa kedua transaksi tersebut menjaga waktu pemrosesan dalam batas aman dan data dinyatakan acak. Meskipun demikian, saat membandingkan nilai-nilai tersebut, transaksi seluler dengan NFC menunjukkan keunggulan dalam hal waktu dan keacakan. Penelitian ini dapat dikembangkan dengan melakukan uji coba pada transaksi aktual menggunakan protokol yang ada. Penelitian ini juga dapat dikembangkan dengan cara membandingkannya dengan transaksi seluler lainnya.

KONFLIK KEPENTINGAN

Penulis menyatakan bahwa penelitian ini dilakukan tanpa adanya konflik kepentingan.

KONTRIBUSI PENULIS

Konseptualisasi, Lucia Nugraheni Harnaningrum; metodologi, Lucia Nugraheni Harnaningrum; perangkat lunak, Kristoforus Nanda Mahardhian; validation, Lucia Nugraheni Harnaningrum; analisis formal, Lucia Nugraheni Harnaningrum; investigasi, Lucia Nugraheni Harnaningrum; sumber daya, Kristoforus Nanda Mahardhian; kurasi data, Kristoforus Nanda Mahardhian; penulisan—penyusunan draf asli, Kristoforus Nanda Mahardhian; penulisan—peninjauan dan penyuntingan, Lucia Nugraheni Harnaningrum; visualisasi, Kristoforus Nanda Mahardhian; supervisi, Lucia Nugraheni Harnaningrum; administrasi proyek, Kristoforus Nanda Mahardhian.

REFERENSI

[1] M. Raikar, P.N. Naik, C. Bhavikatti, dan S. Shetty, "QR code based patient monitoring system," *Int. Res. J. Eng. Technol.*, vol. 7, no. 5, hal. 7635–7638, Mei 2020.

[2] T. Cata, P.S. Patel, dan T. Sakaguchi, "QR code: A new opportunity for effective mobile marketing," *J. Mob. Technol. Knowl. Soc.*, vol. 2013, hal. 1–7, Agu. 2013, doi: 10.5171/2013.748267.

[3] S. Kamble, "A QR code technology for centralized inventory management system," *Int. Res. J. Eng. Technol.*, vol.8, no. 4, hal. 1537–1540, Apr. 2021.

[4] S. Nseir, N. Hirzallah, dan M. Aqel, "A secure mobile payment system using QR code," dalam *2013 5th Int. Conf. Comput. Sci. Inf. Technol.*, 2013, hal. 111–114, doi: 10.1109/CSIT.2013.6588767.

[5] C. Shuran dan Y. Xiaoling, "A new public transport payment method based on NFC and QR code," dalam *2020 IEEE 5th Int. Conf. Intell. Transp. Eng. (ICITE)*, 2020, hal. 240–244, doi: 10.1109/ICITE50838.2020.9231356.

[6] S.S. Ahamad, "A novel NFC-based secure protocol for merchant transactions," *IEEE Access*, vol. 10, hal. 1905–1920, Des. 2022, doi: 10.1109/ACCESS.2021.3139065.

[7] S. Chabbi dan N.E. Madhoun, "A new security solution enhancing the dynamic array PIN protocol," dalam *2022 Int. Wirel. Commun. Mob. Comput. (IWCMC)*, 2022, hal. 991–996, doi: 10.1109/IWCMC55113.2022.9825252.

[8] A.B. Barba dkk., "Design and manufacture of flexible epidermal NFC device for electrochemical sensing of sweat," dalam *2022 IEEE Int. Conf. Flex. Printable Sens. Syst. (FLEPS)*, 2022, hal. 1–4, doi: 10.1109/FLEPS53764.2022.9781563.

[9] F. Basic, C.R. Laube, C. Steger, dan R. Kofler, "A novel secure NFC-based approach for BMS monitoring and diagnostic readout," dalam *2022 IEEE Int. Conf. RFID (RFID)*, 2022, hal. 23–28, doi: 10.1109/RFID54732.2022.9795979.

[10] L. Ahmad, R. Al-Sabha, dan A. Al-Haj, "Design and implementation of a secure QR payment system based on visual cryptography," dalam *2021 7th Int. Conf. Inf. Manag. (ICIM)*, 2021, hal. 40–44, doi: 10.1109/ICIM52229.2021.9417129.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Harlow, Inggris: Pearson, 2013.

[12] L.N. Harnaningrum, A. Ashari, dan A.E. Putra, "Mobile payment transaction model with robust security in the NFC-HCE ecosystem with secure elements on smartphones," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, hal. 160–168, Agu. 2022, doi: 10.14569/IJACSA.2022.0130819.

[13] A. Rukhin dkk., "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Natl. Inst. Stand. Technol. Spec. Publ., Gaithersburg, MD, AS, Tech. Rep. NIST SP 800-22rev1a, 2010.

[14] K. Oad, "Reduce the complexity of big number factoring for RSA breaking," Thesis M.S., Southeast Missouri State University, Cape Girardeau, MO, AS, 2021.

[15] H.M. Bahig dkk., "Performance analysis of Fermat factorization algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, hal. 340–352, Des. 2020, doi: 10.14569/IJACSA.2020.0111242.

[16] K. Fan, P. Song, dan Y. Yang, "ULMAP : Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mob. Inf. Syst.*, vol. 2017, hal. 1-7, Apr. 2017, doi: 10.1155/2017/2349149.

[17] N.E. Madhoun, E. Bertin, dan G. Pujolle, "For small merchants: A secure smartphone-based architecture to process and accept NFC payments," dalam *2018 17th IEEE Int. Conf. Trust Secur. Priv. Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (Trust./BigDataSE)*, 2018, hal. 403–411, doi: 10.1109/TrustCom/BigDataSE.2018.00067.

[18] A. Al-Haj dan M.A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," dalam *2018 4th Int. Conf. Inf. Manag. (ICIM)*, 2018, hal. 184–187, doi: 10.1109/INFOMAN.2018.8392832.

[19] N.E. Madhoun, E. Bertin, dan G. Pujolle, "An overview of the EMV protocol and its security vulnerabilities," dalam *2018 Fourth Int. Conf. Mob. Secure Serv. (MobiSecv)*, 2018, hal. 1–5, doi: 10.1109/MOBISECSERV.2018.8311444.

[20] S.S. Ahamad dan A.-S.K. Pathan, "Trusted service manager (TSM) based privacy-preserving and secure mobile commerce framework with formal verification," *Complex Adapt. Syst. Model.*, vol. 7, no. 1, hal. 1–18, Des. 2019, doi 10.1186/s40294-019-0064-z.

[21] A. Al-Mamun, S.S.M. Rahman, T.A. Shaon, dan M.A. Hossain, "Security analysis of AES and enhancing its security by modifying s-box with an additional byte," *Int. J. Comput. Netw. Commun.*, vol. 9, no. 2, hal. 69–88, Mar. 2017, doi: 10.5121/ijcnc.2017.9206.

[22] R. Skibba, "Japan's Fugaku supercomputer crushes competition, but likely not for long," *Engineering*, vol. 7, no. 1, hal. 6–7, Jan. 2021, doi: 10.1016/j.eng.2020.12.003.

[23] Y. Kodama, T. Odajima, E. Arima, dan M. Sato, "Evaluation of power management control on the supercomputer Fugaku," dalam *2020 IEEE Int. Conf. Clust. Comput. (CLUST.)*, 2020, hal. 484–493, doi: 10.1109/CLUSTER49012.2020.00069.