

Analisis Keamanan Sistem Pembayaran Digital Quick Response Code Indonesian Standard (QRIS)

Abdul Azzam Ajhari¹⁾

(1) Deputi Bidang Perekonomian, Badan Siber dan Sandi Negara, abdul.azzam@bssn.go.id

Abstrak

Penggunaan sistem pembayaran digital melalui Quick Response Code (QR Code) telah membawa kemajuan signifikan dalam efisiensi transaksi, khususnya di era digital saat ini. Teknologi ini menawarkan kecepatan dan kemudahan dalam proses pembayaran, mengurangi ketergantungan pada uang tunai dan memfasilitasi transaksi yang aman dan nyaman. Pemanfaatan QR Code diterapkan pada Quick Response Code Indonesian Standard (QRIS) yang telah menopang perekonomian di sektor perdagangan. Namun, semakin berkembangnya teknologi akan selalu memunculkan kerentanan seperti masalah keamanan pada QRIS, yaitu risiko keamanan QR Code dan Phishing (Quishing). Dalam serangan ini, pelaku kejahatan membuat QRIS yang tampaknya sah seolah-olah QRIS milik pedagang, tetapi ketika dipindai QRIS tersebut mengarahkan korban melakukan transaksi ke rekening QRIS pelaku kejahatan. Studi ini memberikan solusi untuk mengatasi Quishing pada QRIS dengan analisis keamanan sistem pembayaran digital QRIS dengan merekomendasikan implementasi keamanan tambahan pada sistem QRIS yang sudah ada. Selain itu, kampanye edukasi yang berkelanjutan tentang keamanan digital serta peningkatan infrastruktur pendukung sangat diperlukan untuk meningkatkan adopsi dan keefektifan sistem pembayaran digital berbasis QRIS di masyarakat. Studi ini menunjukkan bahwa penerapan autentikasi ganda, verifikasi lokasi, dan edukasi keamanan digital adalah langkah yang efektif untuk melindungi dan mencegah pengguna dari serangan Quishing.

Kata kunci: QR Code, Quick Response Code Indonesian Standard (QRIS), Keamanan QRIS, Quishing, Pembayaran digital.

Abstract

Digital payment systems through Quick Response Codes (QR Codes) have brought significant progress in transaction efficiency, especially in today's digital era. This technology offers speed and convenience in the payment process, reduces dependence on cash and facilitates safe and convenient transactions. QR Codes are applied to the Quick Response Code Indonesian Standard (QRIS), which has helped the economy in the trade sector. However, the increasing development of technology will always cause vulnerabilities such as security issues in QRIS, namely the risk of QR Code security and Phishing (Quishing). In this attack, criminals create QRIS that appear legitimate as if the QRIS belong to the merchant, but when sending, the QRIS directs the victim to make a transaction to the perpetrator's QRIS account. This study provides a solution to overcome Quishing in QRIS with a security analysis of the QRIS digital payment system by recommending the implementation of additional security in the existing QRIS system. In addition, ongoing education campaigns on digital security and improvements to supporting infrastructure are needed to increase the adoption and effectiveness of QRIS-based digital payment systems in the community. This study shows that the implementation of dual authentication, location verification, and digital security education are effective steps to protect and prevent users from Quishing attacks.

Keywords: QR Code, Quick Response Code Indonesian Standard (QRIS), Secure QRIS, Quishing, Digital payment.

1. PENDAHULUAN

Quick Response Code (QR Code) sebagai sarana pembayaran telah menjadi umum diterapkan di dunia [1], [2], [3], [4], [5]. Penelitian Eren [6] mengungkapkan keterkaitan kualitas sistem dan kecepatan memberi dampak signifikan terhadap QR Code Payment. Menurut penelitian Shasanti [7] dan Djanir [8], Quick Response Code Indonesian Standard (QRIS) erat hubungannya diterima sebagai *lifestyle* dan telah membawa manfaat besar dalam efisiensi transaksi [9], [10], [11], [12], [13]. QRIS juga telah menopang sektor perdagangan dengan mayoritas Usaha Mikro Kecil Menengah (UMKM) sekitar 91,4% dari total 26,7 juta *merchant* berdasarkan data Bank Indonesia per Juni 2023 [14].

Pada Gen-Z yang sangat umum dengan teknologi khususnya dinyatakan oleh penelitian Febriyanti [15] dan Rafferty [16] bahwa meskipun diterimanya manfaat penggunaan QRIS yang baik, namun

pengetahuan tentang risiko finansial dari QRIS masih rendah, sehingga diperlukan perhatian lebih terhadap kemungkinan yang akan terjadi dari layanan QRIS. Penelitian [17], [18], [19], [20], [21] menunjukkan perubahan teknologi dapat memberikan perubahan perilaku terhadap penggunaan QRIS. Hal ini menunjukkan bahwa peningkatan kemampuan baik dari keandalan teknologi maupun keamanannya dapat memberikan dampak baik dari QRIS sekaligus pada *brand* instansi terkait yang mengeluarkannya [22], [23].

Namun, seiring dengan adopsi QRIS sebagai pembayaran digital yang semakin meluas, kasus kejahatan siber seperti Quishing meningkat. Quishing adalah teknik serangan di mana pelaku mengganti kode QRIS yang sah dengan kode palsu untuk mengalihkan pembayaran ke rekening penyerang. Salah satu contoh kasus adalah penggantian QRIS pada kotak amal di beberapa masjid di Jakarta, di mana kode QRIS asli diganti dengan milik pelaku

sehingga donasi diarahkan ke akun pelaku [24], [25], [26], [27], [28]. Solusi yang diperlukan untuk mengatasi ancaman ini meliputi edukasi tentang praktik kesadaran keamanan digital (*cybersecurity awareness*), penerapan autentikasi dan deteksi lokasi pada QRIS, serta penguatan infrastruktur keamanan pada sistem pembayaran digital.

Beberapa penelitian sebelumnya menunjukkan bahwa pemahaman dan kesadaran keamanan digital di kalangan pengguna QRIS di Indonesia masih rendah. Penelitian ini berkontribusi dalam meningkatkan kesadaran tentang ancaman Quishing, sekaligus menawarkan panduan mitigasi untuk memperkuat keamanan QRIS di Indonesia.

2. LANDASAN TEORI

2.1 QRIS

Kemudahan penggunaan QRIS memainkan peran penting dalam meningkatkan minat pengguna untuk mengadopsi sistem pembayaran digital. Beberapa penelitian yang mendukung temuan ini antara lain.

Pontoh dkk. [29] menemukan bahwa kemudahan penggunaan secara signifikan mempengaruhi niat pedagang untuk menggunakan QRIS sebagai metode pembayaran digital, meskipun risiko yang dirasakan tidak terlalu berpengaruh. Preferensi konsumen terhadap QRIS sebagai metode pembayaran dipengaruhi oleh kemudahan penggunaan, kepercayaan, serta risiko yang dirasakan [30], [31].

Persepsi manfaat yang dirasakan oleh pengguna dalam menggunakan QRIS berperan penting dalam mendorong niat mereka untuk terus menggunakan sistem ini. Pada penelitian [32] dan [33] ditemukan bahwa persepsi manfaat berperan besar dalam mempengaruhi niat pedagang UMKM untuk menggunakan QRIS sebagai sistem pembayaran.

Selain digunakan sebagai pembayaran digital UMKM, Wulansari dkk. [34] mengungkapkan QRIS juga dapat digunakan untuk pembayaran pajak bumi dan bangunan. Manfaat ini juga meningkatkan tingkat kepercayaan terhadap QRIS.

2.2 Quishing

Musyaffi dkk. [35] menyoroti bahwa salah satu risiko utama dalam penggunaan QRIS adalah terkait keamanan dan masalah data. Salah satu masalah tersebut terjadi ketika saldo yang tidak terpotong atau kesalahan aplikasi saat melakukan transaksi dengan QR Code.

Penelitian [36] menunjukkan bahwa risiko siber seperti serangan manipulasi QR Code oleh aktor jahat yang mengubah kode penerima dana adalah ancaman nyata. Autentikasi terhadap QR Code menjadi penting untuk mencegah kejahatan siber dalam transaksi pembayaran digital dengan QRIS.

Dengan demikian risiko keamanan siber menjadi salah satu hambatan utama dalam adopsi QRIS. Konsumen menjadi terpengaruh negatif untuk mengadopsi QRIS [37] dalam pembayaran digital.

Hal itulah yang menunjukkan pentingnya mitigasi risiko untuk meningkatkan adopsi QRIS [38]. Dengan peningkatan keamanan dan mitigasi risiko menjadi langkah penting untuk mempercepat penerimaan QRIS di masyarakat.

3. METODE PENELITIAN

Berdasarkan data pengukuran keamanan informasi dalam penelitian [39] ditemukan bahwa tingkat literasi di UMKM selama 3 tahun (2020-2022) adalah buruk dan kurang. Sehingga dibutuhkan suatu sistem deteksi dini sebagai langkah mitigatif dan preventif untuk melindungi konsumen sekaligus UMKM Indonesia pada sistem QRIS.

Penelitian ini menggunakan pendekatan studi literatur dengan tujuan mengidentifikasi risiko dan solusi terkait Quishing dalam penggunaan QRIS. Proses ini melibatkan pengumpulan dan analisis literatur dari jurnal, laporan penelitian, dan berita terkait kasus Quishing pada QRIS. Data sekunder yang diambil dari literatur ini digunakan untuk menyusun rekomendasi mitigasi keamanan yang efektif, termasuk pendekatan edukasi pengguna dan teknologi autentikasi.

3.1 Autentikasi dan Verifikasi Lokasi

Pada tahap ini, bertujuan untuk melakukan autentikasi dan verifikasi lokasi dengan Python. Langkah-langkah yang dilakukan adalah.

- Mengumpulkan data transaksi QRIS Quishing yang teridentifikasi. Data yang dikumpulkan mencakup data QRIS yang digunakan sebagai Quishing berasal dari [24], [25], [26], [27], [28].



Gambar 1. Quishing QRIS

Data QRIS pada Gambar 1 yang ditemukan berlokasi di area masjid Jakarta Selatan, Indonesia.

- Melakukan eksplorasi awal terhadap data untuk memahami karakteristik data, identifikasi anomali, serta pola-pola yang dapat menunjukkan serangan Quishing.

Tabel 1. Data Quishing QRIS

QR Code Data	Location
00020101021126660014ID.LINKAJA.WWW011893600911...	None

- Memastikan kualitas data yang dikumpulkan dengan memeriksa adanya missing values, outliers, atau kesalahan dalam data. Data yang ditemukan pada Tabel 1 menunjukkan belum ditemukannya Quishing.
- Menghapus atau memperbaiki data yang hilang, duplikasi, atau tidak valid.
- Mengubah atribut-atribut yang relevan ke dalam format yang dapat digunakan oleh algoritma deteksi. Misalnya, mengubah atribut waktu transaksi menjadi variabel yang menunjukkan jam transaksi, atau menghitung selisih waktu antara transaksi yang mencurigakan.
- Membangun fitur-fitur baru yang dapat membantu dalam mendeteksi serangan Quishing, seperti pola frekuensi pemindaian QRIS oleh *merchant* tertentu.

Tabel 2. Data Detil Quishing QRIS

QR Code Data
array([['00020101021126660014ID.LINKAJA.WWW011893600911002162700102151802110116270010303UME51440014ID.CO.QRIS.WWW02151802110116270010303UME5204111153033605802ID5916RESTORASI MASJID6005MEDAN61052015362400716377B6EAF-F97B-41981602126281165802586304A749', None, '00020101021126660014ID.LINKAJA.WWW011893600911002162700102151802110116270010303UME51440014ID.CO.QRIS.WWW02151802110116270010303UME5204111153033605802ID5916RESTORASI MASJID6005MEDAN61052015362400716377B6EAF-F97B-41981602126281165802586304A749']], dtype=object)

Diketahui pada Tabel 2 terdapat data detil Quishing QRIS yang dimana data QR Code menunjukkan lokasi pembayaran digitalnya ada di “MEDAN”, sedangkan QRIS berada di area masjid Jakarta Selatan.

- Inisialisasi data seperti *merchant ID* dan *location*. Berdasarkan data nama lokasi kota, dilakukan konversi ke bentuk *latitude* dan *longitude*.
- Definisikan aturannya

Tabel 3. Rule Verifikasi Lokasi User

Rule 1
IF distance(current_location, merchant_location) > allowed_radius THEN flag_transaction = "Quishing suspected"

Jika lokasi tidak sesuai dengan lokasi *merchant* yang tercatat di sistem (misalnya lokasi berada di luar radius yang ditentukan dari lokasi sah *merchant*), maka flag sebagai **potensi Quishing**.

Tabel 4. Rule Verifikasi Lokasi Merchant

Rule 2
IF count(transactions_outside_merchant_location) > threshold AND time_between_transactions < threshold_time THEN flag_transaction = "Quishing highly suspected"

Jika **merchant ID** berulang kali terdeteksi di lokasi yang jauh dari lokasi sah *merchant* dalam jangka waktu singkat, maka flag sebagai **potensi Quishing**.

Tabel 5. Rule Verifikasi Blacklist Lokasi

Rule 3
IF current_location IN blacklist_locations THEN flag_transaction = "Confirmed Quishing"

Jika **transaksi QRIS** terjadi di lokasi yang sudah pernah diidentifikasi sebagai lokasi serangan Quishing (lokasi "blacklist"), maka flag sebagai **Quishing**.

- Hitung jarak lokasinya dengan lokasi resmi *merchant* menggunakan rumus *Haversine formula* untuk menghitung jarak antara dua titik geografis (*Latitude*, *Longitude*) dalam pseudocode Tabel 6 sebagai berikut.

Tabel 6. Perhitungan Jarak Lokasi

Pseudocode Haversine (1)
def haversine(lat1, lon1, lat2, lon2): import math R = 6371 # Radius bumi dalam kilometer dLat = math.radians(lat2 - lat1) dLon = math.radians(lon2 - lon1) a = math.sin(dLat/2) * math.sin(dLat/2) + math.cos(math.radians(lat1)) * math.cos(math.radians(lat2)) * math.sin(dLon/2) * math.sin(dLon/2) c = 2 * math.atan2(math.sqrt(a), math.sqrt(1-a)) distance = R * c return distance # dalam kilometer

Lalu, dilakukan perbandingan jarak yang dihitung dengan radius yang diizinkan untuk *merchant*.

Tabel 7. Perhitungan Perbandingan Jarak Lokasi

Pseudocode Haversine (2)
distance = haversine(current_lat, current_lon, merchant_lat, merchant_lon) if distance > allowed_radius: flag_transaction = "Quishing suspected"

- Eksekusi aturan deteksi untuk setiap transaksi dengan menghitung jarak antara lokasi transaksi dan lokasi *merchant*. Kemudian terapkan aturan jarak yang lebih besar dari radius yang diizinkan, maka flag sebagai **potensi Quishing**. Selanjutnya, jika lokasi tersebut ada dalam daftar lokasi yang terindikasi sebagai serangan Quishing, tandai sebagai **konfirmasi Quishing**.

Tabel 8. Perhitungan Anomali Jarak Lokasi
Pseudocode Rule-Based Detection

```
def detect_quishing(transaction):
    merchant_location =
    get_merchant_location(transaction['merchant_id'])
    current_location = transaction['location']

    # Step 1: Calculate distance between transaction
    location and merchant location
    distance = haversine(current_location['lat'],
    current_location['lon'],
    merchant_location['lat'],
    merchant_location['lon'])

    # Step 2: Apply rules
    if distance > allowed_radius:
        return "Quishing suspected"

    # Step 3: Check for multiple anomalies in a short
    time
    if
    recent_transactions_outside_merchant(transaction['
    merchant_id'], current_location):
        return "Quishing highly suspected"

    # Step 4: Check if the location is in the blacklist
    if current_location in blacklist_locations:
        return "Confirmed Quishing"

    return "Transaction normal"

# Function to check if there are multiple anomalous
transactions
def
recent_transactions_outside_merchant(merchant_id,
current_location):
    recent_transactions =
    get_recent_transactions(merchant_id)
    anomaly_count = sum(1 for t in
    recent_transactions if haversine(t['location']['lat'],
    t['location']['lon'],
    current_location['lat'],
    current_location['lon']) > allowed_radius)
    if anomaly_count > threshold and
    time_between_transactions(recent_transactions) <
    threshold_time:
        return True
    return False
```

Dengan algoritma ini, sistem dapat mendeteksi serangan Quishing berbasis QRIS berdasarkan pola lokasi yang mencurigakan.

3.2 Edukasi Pengguna

Edukasi pengguna tentang ancaman Quishing menjadi bagian penting dari mitigasi risiko. Kampanye edukasi ini perlu mencakup informasi tentang mengenali QR Code yang aman, serta pentingnya memverifikasi lokasi dan sumber QRIS sebelum melakukan transaksi. Edukasi ini dapat dilakukan melalui sosialisasi digital, pelatihan [40], serta informasi di dalam aplikasi QRIS itu sendiri.

3.3 Sistem Peringatan Dini

Sistem peringatan dini berfungsi untuk mengidentifikasi aktivitas mencurigakan [39] dan [41] berdasarkan pola transaksi. Sistem ini akan mengirimkan notifikasi kepada pengguna jika terdeteksi aktivitas tidak wajar, seperti transaksi yang terjadi di lokasi yang berbeda dari lokasi *merchant*.

4. HASIL DAN PEMBAHASAN

Hasil analisis penelitian menunjukkan bahwa Quishing pada QRIS dapat dicegah dengan mengombinasikan solusi teknologi dan edukasi pengguna. Beberapa langkah mitigasi yang diusulkan adalah sebagai berikut.

4.1 Konversi Latitude dan Longitude ke Radian

$$radian = degree \times \frac{\pi}{180} \quad (1)$$

Diketahui bahwa *merchant* QRIS yang sah berada di lokasi Jakarta dan *merchant* Quishing berada di lokasi Medan. Kemudian kita hitung konversi derajat ke radian dengan rumus 2.

$$\phi_1(Jakarta) = -6.2088 \times \frac{\pi}{180} = -0.1083 \text{ radian} \quad (2)$$

$$\phi_2(Medan) = 3.5952 \times \frac{\pi}{180} = 0.0627 \text{ radian} \quad (3)$$

$$\lambda_1(Jakarta) = 106.8456 \times \frac{\pi}{180} = 1.8644 \text{ radian} \quad (4)$$

$$\lambda_2(Medan) = 98.6722 \times \frac{\pi}{180} = 1.7225 \text{ radian} \quad (5)$$

4.2 Hitung Perbedaan Latitude dan Longitude

Setelah diketahui radian antara latitude dan longitude dari kota Jakarta dan Medan, kemudian kita hitung perbedaannya.

4.3 Hitung Jarak dengan Pseudocode Haversine

Substitusikan nilai-nilai yang sudah diketahui sebelumnya ke dalam Pseudocode Haversine.

$$\Delta\phi = 0.0627 - (-0.1083) = 0.1710 \text{ radian} \quad (6)$$

$$\Delta\lambda = 1.7225 - 1.8644 = -0.1419 \text{ radian} \quad (7)$$

$$a = \sin^2\left(\frac{0.1710}{2}\right) + \cos(-0.1083) \cdot \cos(0.0627) \cdot \sin^2\left(\frac{-0.1419}{2}\right) \quad (8)$$

$$a = \sin^2(0.0855) + \cos(-0.1083) \cdot \cos(0.0627) \cdot \sin^2(-0.07095) \quad (9)$$

$$a = (0.00730) + (0.9941 \cdot 0.9980 \cdot 0.00503) \quad (10)$$

$$a = 0.00730 + 0.00499 = 0.01229 \quad (11)$$

$$c = 2 \cdot \text{asin}(\sqrt{0.01229}) = 2 \cdot \text{asin}(0.1109) = 0.2229 \text{ radian} \quad (12)$$

$$d = 2 \cdot 6371 \cdot 0.2229 = 2,836.5 \text{ km} \quad (13)$$

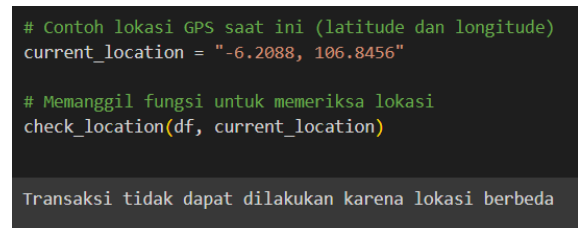
Radius aman yang diizinkan untuk *merchant* pada penelitian ini diatur dalam **1 km**. Jarak hasil

perhitungan adalah **2,836.5 km**, yang jauh melebihi radius aman.

Tabel 9. Perhitungan Radius

Pseudocode Radius
IF distance(current_location,merchant_location)> 1 km, THEN flag as "Transaksi tidak dapat dilakukan karena lokasi berbeda"

Sehingga algoritma mendeteksi bahwa transaksi ini kemungkinan besar merupakan **serangan Quishing** karena jarak transaksi sangat jauh dari lokasi sah *merchant*.



Gambar 2. Notifikasi Transaksi dengan Lokasi QRIS yang Berbeda

Dari Gambar 2 dapat dilihat bahwa sistem mendeteksi lokasi Quishing QRIS berbeda dengan *merchant* awal dan menolak melakukan transaksi.

5. KESIMPULAN

Penelitian ini menyoroti ancaman Quishing pada QRIS dan menawarkan solusi mitigasi berbasis analisis studi literatur. Hasilnya menunjukkan bahwa penerapan autentikasi ganda, verifikasi lokasi, dan edukasi keamanan digital adalah langkah yang efektif untuk melindungi dan mencegah pengguna dari serangan Quishing. Implikasi dari studi ini adalah perlunya pengembangan kebijakan dan teknologi keamanan yang lebih ketat pada QRIS untuk mendukung keamanan transaksi digital di Indonesia.

REFERENSI

- [1] P. Chamika Hewawasam, A. Khatibi, and S. M. Ferdous Azam, "Sri Lankan Consumers' Recommendations Of Qr Code-Enabled Payment Solutions To Create A Cashless Society: Do Moderating Variables Collaborate?," *Baltic Journal of Law & Politics*, 2023, doi: 10.2478/bjlp-2023-0000022.
- [2] P. Yadav, A. Jain, and K. Kochhar, "An Integrated Model for Acceptance of QR Code Mobile Payment: A Comparative Study Between Male and Female," 2023, pp. 659–675. doi: 10.1007/978-981-99-6550-2_49.
- [3] C. He, L. He, Z. Lu, and B. Li, "'I Have to Use My Son's QR Code to Run the Business': Unpacking Senior Street Vendors' Challenges in Mobile Money Collection in China," *Proc ACM Hum Comput Interact*, vol. 7, no. CSCW1, pp. 1–28, Apr. 2023, doi: 10.1145/3579493.
- [4] T. Beck, L. Gambacorta, Y. Huang, Z. Li, and H. Qiu, "BIS Working Papers No 1011 Big techs, QR code payments and financial inclusion," May 2022. [Online]. Available: www.bis.org
- [5] M. Committee, *Committee on Payments and Market Infrastructures Markets Committee Central bank digital currencies*. Bank for International Settlements, 2018. [Online]. Available: www.bis.org
- [6] B. A. Eren, "QR code m-payment from a customer experience perspective," *Journal of Financial Services Marketing*, vol. 29, no. 1, pp. 106–121, Mar. 2024, doi: 10.1057/s41264-022-00186-5.
- [7] A. Shasanti and B. D. Bagana, "Preferensi Minat Penggunaan Quick Response Code Indonesian Standard (QRIS) Sebagai Alat Pembayaran Digital (Studi Kasus: Konsumen Burjo Dan Warmino Di Kota Semarang)," *Management Studies and Entrepreneurship Journal (MSEJ)*, vol. 5, no. 1, pp. 3259–3272, Feb. 2024, doi: 10.37385/msej.v5i2.4430.
- [8] U. Djanar, Sukriyadi, M. Munizu, S. Tomadehe, and A. Ady Bakri, "Analysis of The Influence of Perceived Usefulness Factors and Subjective Norm on Intention to Use QR Code of Digital Wallet Users," *Jurnal Informasi dan Teknologi*, pp. 240–244, Mar. 2024, doi: 10.60083/jidt.v6i1.506.
- [9] A. J. Lewa Djo, N. Tameno, and N. Theresia Kiak, "Analisis Persepsi Penggunaan Qris (Quick Response Indonesia Standard) Sebagai Alat Transaksi UMKM di Kota Bajawaj," *COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat*, vol. 3, no. 09, pp. 3449–3463, Jan. 2024, doi: 10.59141/comserva.v3i09.1155.
- [10] E. Hamzah Muchtar *et al.*, "Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective," *Cogent Business & Management*, vol. 11, no. 1, Dec. 2024, doi: 10.1080/23311975.2024.2316044.
- [11] S. Erika, M. R. Wahyudi, N. B. Maharani, and F. A. Nofirda, "Analisis Pembayaran dengan Menggunakan Sistem Qris Untuk Meningkatkan Kinerja UMKM di Pekanbaru," *Jurnal Pendidikan Tambusai*, vol. 8, no. 1, pp. 499–505, Jan. 2024, doi: 10.31004/jptam.v8i1.12420.
- [12] Fitri Raudah Rahmah, Nur Rahayu Sabrina Damayanti, Raffly Armazumi, and Zul Azmi, "Penggunaan QRIS Untuk Kemudahan Pembayaran Digital Dari Perspektif Kepuasan Konsumen," *Akuntansi*, vol. 3, no. 1, pp. 82–90, Jan. 2024, doi: 10.55606/akuntansi.v3i1.1468.
- [13] E. D. Asofa and D. D. Sholihah,

- “Implementasi QRIS (QR Code Indonesian Standard) sebagai Media Pembayaran Elektronik bagi UMKM di Kelurahan Gunung Anyar Tambak,” *Journal Of Human And Education (JAHE)*, vol. 4, no. 1, pp. 42–48, Jan. 2024, doi: 10.31004/jh.v4i1.511.
- [14] R. A. Nugroho, “BI: Transaksi QRIS UMKM Tembus 1 Miliar,” *cncindonesia.com*, Oct. 11, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://www.cncindonesia.com/market/20231011135900-17-479712/bi-transaksi-qris-umkm-tembus-1-miliar>
- [15] M. Febriyanti, E. Ulza, and U. S. Al Azizah, “Dataset on Determinants of Use Mobile Payment (QRIS) Amongst Generation Z,” *Revista de Gestão Social e Ambiental*, vol. 18, no. 3, p. e05067, Mar. 2024, doi: 10.24857/rgsa.v18n3-087.
- [16] N. E. Rafferty and A. N. Fajar, “Integrated QR Payment System (QRIS): Cashless Payment Solution in Developing Country from Merchant Perspective,” *Asia Pacific Journal of Information Systems*, vol. 32, no. 3, pp. 630–655, Sep. 2022, doi: 10.14329/apjis.2022.32.3.630.
- [17] E. D. Paramita and E. R. Cahyadi, “The Determinants of Behavioral Intention and Use Behavior of QRIS as Digital Payment Method Using Extended UTAUT Model,” *Indonesian Journal of Business and Entrepreneurship*, Jan. 2024, doi: 10.17358/ijbe.10.1.132.
- [18] M. Afan Suyanto, L. K. Candra Dewi, D. Dharmawan, D. Suhardi, and S. Ekasari, “Analysis of The Influence of Behavior Intention, Technology Effort Expectancy and Digitalization Performance Expectancy on Behavior To Use of QRIS Users in Small Medium Enterprises Sector,” *Jurnal Informasi dan Teknologi*, pp. 57–63, Jan. 2024, doi: 10.60083/jidt.v6i1.472.
- [19] Y. F. E. Saputra and A. Bahari, “Analisis Determinan Dan Antecedent Penggunaan Quick Response Indonesian Standard (QRIS) Pada Pembayaran Digital,” *Management Studies and Entrepreneurship Journal (MSEJ)*, vol. 5, no. 1, pp. 3026–3037, Feb. 2024, doi: 10.37385/msej.v5i1.4428.
- [20] K. Ponsree, “QR code payment in Thailand 4.0 era: expand the understanding of perceived susceptibility to COVID-19 in the TAM theory,” *Current Psychology*, vol. 43, no. 26, pp. 22637–22655, Jul. 2024, doi: 10.1007/s12144-023-05605-x.
- [21] C. Türker, B. C. Altay, and A. Okumuş, “Understanding user acceptance of QR code mobile payment systems in Turkey: An extended TAM,” *Technol Forecast Soc Change*, vol. 184, p. 121968, Nov. 2022, doi: 10.1016/j.techfore.2022.121968.
- [22] M. I. Hamzah, F. A. A. Ramli, and N. Shaw, “The moderating influence of brand image on consumers’ adoption of QR-code e-wallets,” *Journal of Retailing and Consumer Services*, vol. 73, p. 103326, Jul. 2023, doi: 10.1016/j.jretconser.2023.103326.
- [23] F. A. A. Ramli, M. I. Hamzah, S. N. Wahab, and R. Shekhar, “Modeling the Brand Equity and Usage Intention of QR-Code E-Wallets,” *FinTech*, vol. 2, no. 2, pp. 205–220, Mar. 2023, doi: 10.3390/fintech2020013.
- [24] A. Laras, “Banyak Kasus Penipuan, Bank Indonesia Tegaskan Transaksi QRIS Aman,” *finansial.bisnis.com*, Aug. 17, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://finansial.bisnis.com/read/20230817/901685842/banyak-kasus-penipuan-bank-indonesia-tegaskan-transaksi-qr-is-aman>
- [25] CNN Indonesia, “Penipuan Modus Ganti QRIS Kotak Amal Terjadi di Beberapa Masjid Jaksel,” *cnnindonesia.com*, Apr. 10, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://www.cnnindonesia.com/nasional/20230410180339-12-935868/penipuan-modus-ganti-qr-is-kotak-amal-terjadi-di-beberapa-masjid-jaksel>
- [26] M. F. Lahur, “Kasus Penipuan dengan Mengganti QRIS Kotak Amal Masjid, Ini Saran Ahli,” *tekno.tempo.co*, Apr. 10, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://tekno.tempo.co/read/1713360/kasus-penipuan-dengan-mengganti-qr-is-kotak-amal-masjid-ini-saran-ahli>
- [27] L. N. Dewi R and Daryono, “Viral Pria Ganti Stiker QRIS Masjid Jaksel dengan Rekening Pribadi, Disebut Mantan Pegawai Bank,” *tribunnews.com*, Apr. 10, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://www.tribunnews.com/metropolitan/2023/04/10/viral-pria-ganti-stiker-qr-is-masjid-jaksel-dengan-rekening-pribadi-disebut-mantan-pegawai-bank>
- [28] A. T. Haryanto, “QRIS Mudah Diganti yang Palsu, Bukti Lemahnya Pembayaran QR Code,” *inet.detik.com*, Apr. 12, 2023. Accessed: Oct. 21, 2024. [Online]. Available: <https://inet.detik.com/security/d-6668665/qr-is-mudah-diganti-yang-palsu-bukti-lemahnya-pembayaran-qr-code>
- [29] M. A. H. Pontoh, F. G. Worang, and F. J. Tumewu, “The Influence of Perceived Ease of Use, Perceived Risk and Consumer Trust towards Merchant Intention in using QRIS as a Digital Payment Method,” *Jurnal EMBA : Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi*, vol. 10, no. 3, p. 904, Sep. 2022, doi: 10.35794/emba.v10i3.42664.
- [30] S. Nathasya and M. Maysha, “QRIS use Preference by MSME Consumers,”

- Gorontalo Development Review*, p. 11, Apr. 2024, doi: 10.32662/golder.v0i0.3075.
- [31] W. Seputri, A. Soemitra, and N. A. Bi Rahmani, "Pengaruh Technology Acceptance Model terhadap Minat Mahasiswa Menggunakan Quick Response Code Indonesia Standard (QRIS) sebagai Cashless Society," *MES Management Journal*, vol. 2, no. 2, pp. 116–126, Oct. 2022, doi: 10.56709/mesman.v2i2.57.
- [32] B. W. Djoyo, S. Nurzaqia, S. I. Budiarti, and S. Agustin, "Examining the Determinant Factors of Intention to Use of Quick Response Code Indonesia Standard (QRIS) as a Payment System for MSME Merchants," in *2022 International Conference on Information Management and Technology (ICIMTech)*, IEEE, Aug. 2022, pp. 676–681. doi: 10.1109/ICIMTech55957.2022.9915238.
- [33] R. Nurhapsari and E. Sholihah, "Analysis of the factors of intention to use QRIS for MSMEs in Semarang City's traditional market," *Jurnal Ekonomi Modernisasi*, vol. 18, no. 2, pp. 199–211, Sep. 2022, doi: 10.21067/jem.v18i2.7291.
- [34] K. Wulansari, D. O. C. Kalangit, S. Satryawati, and R. Kawuryan, "Taxpayers' Trust on Rural and Urban Lands and Building Tax Online Payment Using QRIS," *Interdisciplinary Social Studies*, vol. 2, no. 2, pp. 1633–1641, Nov. 2022, doi: 10.55324/iss.v2i2.321.
- [35] A. M. Musyaffi *et al.*, "Digital Payment During Pandemic: An Extension of The Unified Model of QR Code," *Academic Journal of Interdisciplinary Studies*, vol. 10, no. 6, p. 213, Nov. 2021, doi: 10.36941/ajis-2021-0166.
- [36] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C.-C. Chang, "Multiple Schemes for Mobile Payment Authentication Using QR Code and Visual Cryptography," *Mobile Information Systems*, vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/4356038.
- [37] S. Nathasya and M. Maysha, "QRIS use Preference by MSME Consumers," *Gorontalo Development Review*, p. 11, Apr. 2024, doi: 10.32662/golder.v0i0.3075.
- [38] R. Nurhapsari and E. Sholihah, "Analysis of the factors of intention to use QRIS for MSMEs in Semarang City's traditional market," *Jurnal Ekonomi Modernisasi*, vol. 18, no. 2, pp. 199–211, Sep. 2022, doi: 10.21067/jem.v18i2.7291.
- [39] A. A. Ajhari, M. A. Manaon, and Dimas, "Security Awareness Framework untuk Usaha Mikro, Kecil dan Menengah di Indonesia," *Info Kripto*, vol. 17, no. 3, pp. 85–91, Dec. 2023, doi: 10.56706/ik.v17i3.80.
- [40] A. A. Ajhari, D. F. Priambodo, and H. Yulianti, "Automated Matching Skills to Improve the Accuracy of Job Applicant Selection Using Indonesian National Work Competency Standards," *JOIV: International Journal on Informatics Visualization*, vol. 8, no. 2, p. 635, May 2024, doi: 10.62527/joiv.8.2.2017.
- [41] A. A. Ajhari, D. Febriyan, R. Hilya, and H. Yulianti, "PROCTOR: A Robust URL Protection System Against Fraudulent, Phishing, and Scam Activities," *International Journal of Computing and Digital Systems*, vol. 14, no. 1, pp. 1013–1021, Sep. 2023, doi: 10.12785/ijcds/140179.