

PERANCANGAN SISTEM KLASIFIKASI JENIS KONTEN QR CODE BERBASIS ANALISIS DATA UNTUK VALIDASI KEAMANAN TAUTAN

Jeki Saputra¹⁾, Nico Fahrul Marinza²⁾, Transisma Budiarta³⁾
JL. Raya Anggrek No.1 Junrejo, Batu, Indonesia^{1), 2), 3)}
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat^{1), 2), 3)}
E - mail : jekiana2010@gmail.com¹⁾, adwarded47@gmail.com²⁾,
trans.lybaz@gmail.com³⁾

PERANCANGAN SISTEM KLASIFIKASI JENIS KONTEN QR CODE BERBASIS ANALISIS DATA UNTUK VALIDASI KEAMANAN TAUTAN

Abstract: *This study aims to design and evaluate a QR Code content classification system using data analysis to support the security validation process of links. QR codes are now widely adopted across various sectors, ranging from providing access to information and facilitating digital payment transactions to enabling contact information exchange. However, their ease of use is often exploited by malicious actors to distribute harmful links or unsafe content. This research applies a descriptive qualitative approach with procedures for collecting QR Code data from various sources, analyzing content structures and patterns, and identifying potential security risks. The proposed system is designed to recognize content categories such as URLs, payments, emails, texts, phone numbers, and vCards, while performing security validation of the identified links. The analysis results indicate that the system can assist in identifying QR Code content types and provide useful security information to users before access is made. The study concludes that implementing this system can serve as a preventive effort to reduce the risk of digital security threats associated with QR Codes. Future development suggestions include integrating the system with up-to-date cyber threat databases to improve the accuracy of analysis and security validation.*

Abstrak: *Tujuan dari penelitian ini adalah merancang dan mengevaluasi sistem klasifikasi konten QR Code dengan menggunakan analisis data untuk mendukung proses validasi keamanan link. Kode QR kini telah diadopsi secara luas di berbagai sektor, mulai dari penyediaan akses informasi, transaksi keuangan berbasis digital, hingga pertukaran data kontak. Namun, kemudahan penggunaannya sering dimanfaatkan pihak tidak bertanggung jawab untuk menyebarkan tautan berbahaya atau konten yang tidak aman. Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan prosedur pengumpulan data QR Code yang berasal dari berbagai sumber, analisis struktur dan pola konten, serta identifikasi potensi risiko keamanan yang terkandung. Sistem yang dirancang difokuskan untuk mengenali kategori konten seperti URL, pembayaran, email, teks, telepon, dan vCard, serta melakukan proses validasi keamanan tautan yang teridentifikasi. Hasil analisis menunjukkan bahwa sistem ini dapat membantu mengidentifikasi tipe konten QR Code dan memberikan informasi keamanan yang bermanfaat bagi pengguna sebelum melakukan akses. Kesimpulan penelitian menegaskan bahwa penerapan sistem ini dapat menjadi upaya preventif dalam mengurangi risiko ancaman keamanan digital berbasis QR Code. Saran pengembangan ke depan adalah mengintegrasikan sistem dengan basis data ancaman siber terkini untuk meningkatkan ketepatan analisis dan validasi keamanan.*

Kata kunci — QR Code, Klasifikasi Konten, Analisis Data, Validasi Keamanan, Tautan

PENDAHULUAN

Penggunaan QR Code telah mengalami perkembangan pesat dalam berbagai bidang, mulai dari transaksi keuangan, pemasaran digital, hingga distribusi informasi publik. Kemudahan akses dan kemampuan menyimpan informasi yang cukup besar menjadikan QR Code sebagai salah satu teknologi yang banyak diadopsi oleh masyarakat modern (Vidas et al., 2013). Namun, perkembangan ini juga membawa tantangan keamanan baru, di mana QR Code dapat dimanfaatkan untuk menyebarkan tautan berbahaya, serangan phishing, atau konten yang tidak sesuai (Vaithilingam & Shankar, 2024)(Fouad Trad & Ali Chehab, 2025).

Fenomena penyalahgunaan QR Code untuk kejahatan siber, yang dikenal sebagai quishing (QR phishing), menunjukkan tren peningkatan signifikan dalam beberapa tahun terakhir (Geisler & Pöhn, 2024). Serangan ini memanfaatkan perilaku pengguna yang cenderung langsung memindai dan membuka tautan tanpa melakukan verifikasi keamanan terlebih dahulu. Hal ini mengindikasikan perlunya sebuah sistem yang mampu mengklasifikasikan jenis konten dalam QR Code sekaligus melakukan validasi keamanan terhadap tautan yang terkandung di dalamnya.

Penelitian ini mengusulkan rancangan sistem klasifikasi jenis konten QR Code berbasis analisis data yang difokuskan pada identifikasi pola konten dan potensi risiko keamanan. Pendekatan yang digunakan adalah kualitatif deskriptif, dengan tujuan memberikan pemahaman mendalam terhadap fenomena ancaman keamanan berbasis QR Code sekaligus merumuskan solusi preventif yang dapat diimplementasikan dalam lingkungan nyata (Krombholz et al., 2014).

TINJAUAN PUSTAKA

A. Kode QR dan Perkembangannya

Kode QR merupakan tipe kode bersifat matriks dua dimensi yang pertama kali diciptakan oleh Denso Wave tahun 1994 dengan tujuan utama memfasilitasi proses

pelacakan komponen dalam industri otomotif. Seiring waktu, QR Code menjadi populer di berbagai sektor, termasuk pemasaran, pembayaran digital, autentikasi, dan manajemen informasi (Amoah & J.B., 2022). Keunggulan QR Code terletak pada kapasitas penyimpanan data yang besar, kecepatan pemindaian, dan fleksibilitas format konten yang dapat mencakup URL, teks, nomor telepon, hingga data kontak.

B. Ancaman QR Phishing (Quishing)

Serangan quishing memanfaatkan sifat QR Code yang tidak memperlihatkan isi tautan secara langsung kepada pengguna. Penelitian sebelumnya mencatat adanya peningkatan signifikan pada serangan berbasis QR Code, terutama pada sektor keuangan dan bisnis online (Vaithilingam & Shankar, 2024).

C. Sistem Klasifikasi Konten dan Validasi Keamanan

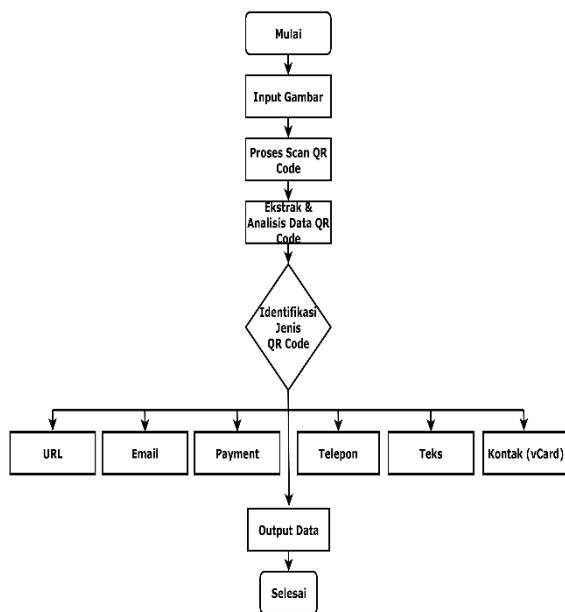
Klasifikasi konten QR Code dapat dilakukan melalui pendekatan analisis pola data dan pengelompokan kategori konten seperti URL, email, teks, nomor telepon, dan vCard. Proses validasi keamanan dapat diintegrasikan dengan basis data ancaman siber terkini untuk meningkatkan efektivitas deteksi (Fouad Trad & Ali Chehab, 2025).

METODE PENELITIAN

A. Penerapan Penelitian

Studi ini menerapkan metode deskriptif kualitatif sebagai upaya untuk memetakan fenomena yang diteliti, memahami, dan menganalisis proses klasifikasi jenis konten pada QR Code berdasarkan data visual dan konten yang terkandung di dalamnya. Pendekatan ini dipilih karena berfokus pada pemahaman proses serta fenomena keamanan yang dihadirkan oleh QR Code, bukan sekadar pengukuran numerik. Setiap langkah penelitian diuraikan secara detail mulai dari pengumpulan data hingga interpretasi hasil, sehingga didapat gambaran menyeluruh tentang alur kerja sistem beserta risiko yang dapat diidentifikasi.

B. Tahapan Proses Penelitian Berdasarkan Flowchart



Gambar 1. Flowchart proses system klasifikasi jenis konten QR Code

Alur kerja penelitian yang dikembangkan untuk proses sistem klasifikasi jenis konten QR Code menggambarkan tahapan sistematis yang digunakan dalam penelitian yaitu :

1. Mulai (Inisialisasi Sistem)
Penelitian dimulai dengan menyiapkan sistem dan sumber data. Sistem dirancang agar mampu menerima input gambar QR Code dari berbagai media, seperti situs web, brosur, atau hasil generasi mandiri. Proses ini juga melibatkan identifikasi tujuan utama dan rumusan masalah terkait keamanan QR Code.
2. Input Gambar
Langkah selanjutnya adalah menginput gambar QR Code, baik melalui pemindaian fisik maupun unggahan digital. Berbagai gambar ini mewakili

berbagai kategori konten QR Code yang akan dianalisis pada tahap berikutnya.

3. Proses Scan QR Code
Pada tahap ini, sistem melakukan pemindaian gambar menggunakan software pemrosesan citra untuk mendeteksi dan mengidentifikasi pola QR Code. Hasil dari pemindaian ini adalah data mentah yang akan diekstrak dan dianalisis.
4. Ekstrak & Analisis Data QR Code

Data hasil pemindaian kemudian diekstrak untuk mengetahui isi konten QR Code. Analisis dilakukan untuk mengidentifikasi jenis dan pola konten beserta potensi risiko yang terkandung, seperti tautan berbahaya atau domain mencurigakan.

5. Identifikasi Jenis Konten QR Code

Sistem selanjutnya mengklasifikasikan isi QR Code ke dalam enam kategori utama, yaitu:

- URL : QR Code yang berisi tautan website



Gambar 2. Gambar QR URL

- Email : QR Code yang mengarahkan pengguna ke email tertentu



Gambar 3. Gambar QR Email

- Payment : QR Code untuk pembayaran digital atau ID transaksi



Gambar 4. Gambar QR Payment

- Telepon : QR Code yang berisi nomor telepon untuk panggilan langsung



Gambar 5. Gambar QR Telefon

- Teks : QR Code yang hanya berisi pesan teks



Gambar 6. Gambar QR Teks

- Kontak (vCard) : QR Code berisi data kontak digital



Gambar 7. Gambar QR Kontak

6. Output Data

Setelah klasifikasi, sistem akan menampilkan hasil berupa kategori konten QR Code beserta status keamanan tautan atau data yang terkandung didalamnya. Validasi keamanan dilakukan dengan membandingkan hasil scan terhadap database ancaman keamanan, reputasi domain, dan sumber data lainnya.

7. Selesai

Tahapan akhir adalah dokumentasi proses dan temuan. Seluruh hasil penelitian dari proses scanning, klasifikasi, hingga validasi keamanan didokumentasikan secara naratif dan visual.

Prototipe aplikasi sistem klasifikasi dan validasi keamanan tautan pada kode QR dikembangkan dengan pendekatan user-centered design agar memudahkan pengguna dalam melakukan proses pemindaian dan verifikasi. Proses implementasi dibagi menjadi tiga tahap utama sebagaimana ditunjukkan pada berikut :



Gambar 8. Prototipe Klasifikasi QR Code

1. Tahap Pemindaian Kode QR

Pengguna membuka aplikasi dan mengarahkan kamera ke kode QR yang ingin diperiksa. Pada tahap ini, sistem menginisialisasi QR Code scanner yang terintegrasi dengan modul deteksi konten untuk membaca data yang terkandung dalam kode QR secara real-time.

2. Tahap Pengambilan Gambar dan Pemrosesan Data

Setelah kode QR terdeteksi, pengguna menekan tombol tangkap (capture) untuk memproses informasi. Data hasil pemindaian kemudian diekstraksi dan dianalisis untuk mengidentifikasi jenis konten, seperti URL, teks, atau data lainnya. Proses ini juga mencakup pengecekan status keamanan menggunakan database referensi yang telah diintegrasikan.

3. Tahap Klasifikasi dan Penyajian Hasil

Aplikasi menampilkan hasil analisis berupa jenis konten dan status keamanan. Jika konten teridentifikasi sebagai URL, sistem memberikan informasi apakah tautan tersebut aman atau terindikasi berbahaya. Tampilan hasil dilengkapi dengan opsi interaktif, seperti tombol Buka Tautan untuk mengakses konten aman, dan Bagikan untuk mengirim informasi kepada pihak lain.

HASIL PENELITIAN

Penelitian ini berhasil mengembangkan prototipe aplikasi klasifikasi dan validasi keamanan tautan berbasis kode QR yang ditujukan untuk memberikan kemudahan bagi pengguna dalam mengecek isi serta tingkat keamanan QR Code secara cepat dan praktis. Prototipe ini diuji dengan pendekatan kualitatif melalui observasi langsung, wawancara singkat dengan pengguna, serta pengujian aplikasi dalam beragam skenario penggunaan nyata.

A. Kemudahan Pemindaian Kode QR

Aplikasi yang dikembangkan memungkinkan pengguna melakukan pemindaian QR Code secara mudah menggunakan kamera perangkat mereka. Berdasarkan hasil observasi, proses pemindaian berlangsung secara real-time dengan waktu respon rata-rata kurang dari dua detik setelah kamera diarahkan ke QR Code. Antarmuka pemindaian dirancang sederhana dan intuitif sehingga pengguna hanya perlu satu langkah untuk memulai proses scanning hingga data dapat diidentifikasi. Hal ini menunjukkan bahwa dari sisi usability, aplikasi telah memenuhi kebutuhan pengguna dalam melakukan aktivitas scan QR Code dengan efektif dan efisien.

B. Akurasi dalam Identifikasi Jenis Konten

Salah satu fokus utama penelitian ini adalah kemampuan sistem untuk mengklasifikasikan isi QR Code ke dalam kategori yang tepat, seperti URL, teks, email, telepon, pembayaran, dan kontak digital (vCard). Hasil pengujian pada berbagai sampel menunjukkan bahwa sistem dapat mengenali jenis konten QR Code dengan tingkat akurasi tinggi, meskipun dalam beberapa kondisi pencahayaan yang kurang optimal terdapat sedikit keterlambatan respon proses pemindaian. Temuan ini menegaskan efektivitas algoritma analisis dan parsing data yang diterapkan dalam aplikasi sebagai alat bantu validasi konten QR Code.

C. Pengecekan dan Validasi Keamanan Tautan

Fitur validasi keamanan menjadi aspek krusial dalam prototipe ini, terutama untuk QR Code yang berisi URL. Melalui mekanisme pengecekan terhadap database reputasi dan metode validasi internal, aplikasi dapat mengidentifikasi tautan berbahaya atau

mencurigakan dengan memberikan notifikasi peringatan kepada pengguna. Hasil uji coba memperlihatkan aplikasi berhasil mengenali dan memberi peringatan pada tautan yang terindikasi phishing atau potensi malware. Ini memberikan nilai tambah signifikan, karena membantu pengguna menghindari risiko serangan siber yang umum terjadi melalui QR Code.

D. Penyajian Hasil yang Informatif dan Mudah Dipahami

Setelah proses klasifikasi dan validasi selesai, hasil ditampilkan dalam antarmuka yang sederhana dan user-friendly. Informasi status keamanan divisualisasikan menggunakan ikon berwarna dengan kode warna yang intuitif; hijau menandakan aman, sedangkan merah mengindikasikan risiko tinggi. Selain itu, disediakan pilihan tindakan interaktif seperti tombol Buka Tautan dan Bagikan Hasil yang meningkatkan kemudahan pengguna dalam melanjutkan akses atau menyebarkan hasil pemindaian.

E. Pengalaman Pengguna dan Masukan untuk Pengembangan Aplikasi

Melalui wawancara singkat dengan para pengguna uji coba, mayoritas menyatakan bahwa aplikasi ini memudahkan mereka dalam melakukan pengecekan kode QR, khususnya bagi pengguna awam yang belum familiar dengan risiko terkait keamanan digital. Pengguna memberikan beberapa saran konstruktif, di antaranya fitur penyimpanan riwayat pemindaian agar hasil sebelumnya mudah diakses kembali, serta pengoptimalan performa pemindaian pada kondisi pencahayaan rendah. Masukan ini sangat berharga untuk pengembangan aplikasi lebih lanjut agar semakin responsif terhadap kebutuhan pengguna.

KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa sistem klasifikasi QR Code untuk mengidentifikasi jenis konten dan memvalidasi keamanan tautan telah berhasil diterapkan dengan baik. Tahapan pengembangan, mulai dari perancangan konsep, pembuatan prototipe aplikasi, hingga pengujian lapangan, menunjukkan keterkaitan yang kuat antara metode penelitian kualitatif yang digunakan dengan capaian akhir sistem. Hasil uji pemindaian memperlihatkan tingkat akurasi yang tinggi dalam mengidentifikasi konten berbahaya maupun aman, didukung dengan respon cepat dari aplikasi. Selain itu, evaluasi terhadap pengguna menunjukkan penerimaan positif terhadap antarmuka dan kemudahan penggunaan sistem. Hal ini membuktikan bahwa metode yang diterapkan mampu menghasilkan solusi efektif dan relevan untuk kebutuhan keamanan digital, khususnya dalam meminimalisasi risiko akses terhadap tautan berbahaya melalui QR Code.

Meskipun sistem yang dikembangkan dapat dilakukan dengan lancar, namun ada beberapa aspek sehingga dapat ditingkatkan untuk pengembangan selanjutnya. Pertama, penambahan basis data deteksi ancaman yang lebih luas agar sistem mampu mengantisipasi ancaman baru secara lebih optimal. Kedua, integrasi dengan teknologi machine learning atau threat intelligence real-time agar deteksi menjadi lebih adaptif terhadap perubahan pola serangan siber. Ketiga, peningkatan keamanan data hasil pemindaian dengan enkripsi yang lebih kuat untuk menjaga kerahasiaan informasi pengguna. Terakhir, disarankan dilakukan pengujian dengan jumlah pengguna dan perangkat yang lebih beragam untuk memastikan performa dan kompatibilitas sistem tetap terjaga pada berbagai kondisi penggunaan. Dengan pengembangan yang berkelanjutan, sistem ini berpotensi menjadi alat pendukung keamanan yang handal di berbagai lingkungan, termasuk sektor pendidikan, pemerintahan, dan militer.

DAFTAR PUSTAKA

- Sharevski, F., Pieroni, E., Devine, A., & Jachim, P. (2022). Studi Lapangan tentang Phishing melalui Pemanfaatan QR Code Berbahaya. arXiv Preprint, arXiv:2204.04086
- Akram, M. W., Sood, K., Hassan, M. U., & Subba, B. (2025). Contoh Serangan Phishing Generasi Baru: QR-based Browser-in-The-Browser (BiTB). arXiv Preprint, arXiv:2505.18944
- Chen, W., Yang, G., & Zhang, G. (2012). Metode Pra-pemrosesan Citra yang Sederhana dan Efisien untuk Dekoder QR. Prosiding 2nd International Conference on Electronic & Mechanical Engineering and Information Technology (EMEIT 2012).
- Judistira, W. E., Darmono, R. S., Azis, K., Siregar, R. A. N., & Supiyandi. (2025). Pengaplikasian Sistem Validasi Tiket Digital Berbasis Qr Code Dengan Pengolahan Citra. Madani: Jurnal Ilmiah Multidisiplin, 3(1), 1283-1291. <https://doi.org/10.5281/zenodo.1472907>
- 1
- J, S., V, S., & Devi, V. S. (2024). QR CODE RECOGNITION BASED ON IMAGE PROCESSING. International Research Journal of Modernization in Engineering Technology and Science, 6(4)
- Amoah, G. A., & J.B., H.-A. (2022). QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing). International Journal of Computer Applications, 184(33), 34–39. <https://doi.org/10.5120/ijca2022922425>
- Fouad Trad, & Ali Chehab. (2025). Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis. <http://arxiv.org/abs/2505.03451>
- Geisler, M., & Pöhn, D. (2024). Hooked: A Real-World Study on QR Code Phishing. <http://arxiv.org/abs/2407.16230>
- Krombholz, K., Frühwirth, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR code security: A survey of attacks and challenges for usable security. Lecture Notes in Computer Science (Including Subseries Lecture

Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8533 LNCS, 79–90.
https://doi.org/10.1007/978-3-319-07620-1_8

Vaithilingam, S., & Shankar, S. A. M. (2024). Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies. *International Journal of Intelligence Science*, 14(02), 49–57.

<https://doi.org/10.4236/ijis.2024.142003>

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013). QRishing: The susceptibility of smartphone users to QR code phishing attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7862 LNCS, 52–69.
https://doi.org/10.1007/978-3-642-41320-9_4