Pencegahan Serangan Malware terhadap Mobile Phone melalui QR Code

Admiral Rizki Maulana Hidayat[1], **Ari Moesriami Barmawi,** [2]

[1]kikisuriki@students.telkomuniversity.ac.id, [2]Mbarmawi@melsa.net.id

Abstrak

Pada era kehidupan modern dan teknologi yang sudah sangat maju, QRcode sering dipakai untuk keperluan komersial pada perusahaan ataupun bisa juga dipakai untuk keperluan pribadi. Dengan demikian penyerang bisa menipu pengguna awam untuk memindai QRcode yang sudah berisi *malware*. Oleh karena itu, tujuan dari penelitian ini adalah melakukan perancangan aplikasi scanner QRcode dengan keamanan yang lebih baik dengan menggunakan N-gram model untuk membelah URL dan dilanjut menggunakan metode TF-IDF untuk mencari pola yang merepresentasikan URL dari QRcode baik yang asli dari sebuah perusahaan ataupun yang dipakai penyerang. Dua cara itu digunakan untuk mencegah masuknya *malware* ke dalam smartphone yang memindainya.

Hasil yang ditemukan pada penelitian ini menunjukan kedua metode yang dipakai bisa mencegah sebuah URL masuk ke dalam smartphone yang memindai QRcode yang memiliki *malware*.Dengan hasil akurasi model mencapai 94%.

Kata Kunci: QRcode,TF-IDF,*malware*,N-gram

Abstract

In the era of modern life and very advanced technology, QRcodes are often used for commercial purposes in companies or can also be used for personal purposes. Thus, attackers can trick ordinary users into scanning QRcodes that already contain *malware*. Therefore, the purpose of this study is to design a QRcode scanner application with better security by using the N-gram model to split URLs and also using TF-IDF method to look for patterns that represent URLs from QRcodes, whether original from a company or used by the attacker. These two methods are used to prevent the entry of *malware* into the smartphone that scans it.

The results found in this study show that the two methods used can prevent a URL from entering a smartphone that scans a QRcode that has *malware*. With the results of the model accuracy reaching 94%.

Keywords: QRcode,TF-IDF,*malware*,N-gram

1. Pendahuluan

Persebaran internet yang semakin luas mengakibatkan meningkatnya jumlah pengguna internet. Hal ini membuat pengguna semakin mudah dalam bertukar informasi dengan pengguna lainnya. Informasi yang diperoleh berupa gambar, *text*, audio maupun video. Satu bentuk informasi yang saat ini sering digunakan adalah QRcode, QRcode sering digunakan untuk promosi komersil ataupun juga promosi pribadi melalui smartphone.Hal ini disebabkan masyarakat mulai banyak yang menggunakan smartphone. Hal ini juga dipicu karena mudahnya membuat QRcode dan juga flexibel dalam penyimpanan datanya. Tercatat pada website https://blog.beaconstac.com/2019/12/qr-code-statistics, pada tahun 2020 ada sekitar 11M orang yang memindai QRcode di USA, penggunaan QRcode di eropa mencapai 10.1 juta penggunaan, lalu Asia Tenggara dan India akan menjadi wilayah terbesar yang akan memindai QRcode yang angkanya mencapai 15 juta dan 8 juta. Kemudahan dalam mendapatkan informasi melalui QRcode menyebabkan penyerang dapat menyisipkan sebuah *malware* atau URL berbahaya.Dengan contoh pada saat seorang user memindai QRcode dari *merchant*(penjual). QRcode tersebut dapat berisi *malware* untuk mengambil informasi yang ada pada smartphone yang memindai dan juga *malware* ini dapat merusak sistem yang memindai QRcode tersebut. Disamping itu *malware* juga dapat mengambil informasi penting dari komputer yang berisi scan QRcode atau dari komputer yang memindai QRcode. Salah satu cara menyisipkan *malware* atau URL berbahaya itu melalui *malicious* QRcode. *Malicious* QRcode ini berbeda dengan QRcode original karena *malicious* QRcode merupakan QRcode yang dibuat sedemikian rupa sehingga hasilnya mirip dengan QRcode original tetapi mengandung alamat website yang mencurigakan. Sedangkan QRcode original merupakan QRcode yang berisi data asli untuk dipindai. Oleh karena itu, Pengguna sering tertipu karena bentuk fisik QRcode yang berisi