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 *malware* mirip dengan QRcode originalnya.

Meningkatnya popularitas QRcode sebagai elemen media promosi komersial dapat membuat kode QRcode menjadi target yang menarik bagi penyerang untuk menyisipkan *malware* ke komputer yang memindai QRcode tersebut. Namun, serangan yang mengandalkan QRcode relatif baru. Kami mendefinisikan serangan berbasis QRcode sebagai serangan yang berusaha memikat korban untuk memindai QRcode yang mengarahkan mereka ke URL web berbahaya. Ide utama di balik serangan QRcode adalah dengan asumsi bahwa korban mempercayai halaman web atau materi yang dicetak dalam QRcode dan menganggap bahwa kode terkait tidak berbahaya[6].

Dengan adanya QRcode pengguna membutuhkan sebuah pemindai untuk bisa membaca sebuah QRcode. Dengan demikian, Library Zxing bisa dipakai untuk mendekripsi isi QRcode. Dikarenakan QRcode digunakan untuk komersil, Penyerang banyak menggunakan kesempatan ini untuk menyerang pengguna dengan menggunakan QRcode yang berisi *malware*. Dengan demikian, N-gram dan TF-IDF bisa menjadi peran penting untuk mengatasi masalah ini dengan membagi URL dan juga menghitung frekuensi kemunculan pada setiap N-gram yang ada.

Topik dari tugas akhir ini membahas tentang metode mendeteksi adanya *malware* yang disisipkan kedalam QRcode dengan menggunakan n-gram model,ZXing library serta TF-IDF sebagai cara mengatasi persalahan yang terjadi dengan *malicious* QRcode

Berdasarkan latar belakang di atas, rumusan masalah pada tugas akhir ini adalah bahwa *malware* bisa menyerang smartphone melalui QRcode yang dipindai oleh smartphone tersebut dimana QRcode tersebut berisi alamat URL *malware*.

Berikut adalah asumsi yang digunakan pada tugas akhir ini :

1. Memakai smartphone yang memiliki OS android
2. *Malware* yang menyerang adalah *malware* yang langsung terdownload ke dalam smartphone.

Ruang lingkup dari tugas akhir ini adalah memberikan hasil deteksi berupa kalimat teridentifikasi *malware* atau tidak *malware*. Jika tidak teridentifikasi adanya *malware* maka aplikasi akan mengarahkan smartphone menuju URL yang dituju. Jika teridentifikasi adanya *malware* maka aplikasi akan menampilkan chat dialog menunjukan bahwa URL adalah *malware*.

Tujuan dari diadakannya penelitian ini adalah untuk mencegah smartphone untuk terjangkit *malware* dari QRcode oleh pihak yang tidak bertanggung jawab.Adapun implementasi pemeriksaan QRcode berupa aplikasi yang dapat menunjukan adanya *malware* setelah QRcode dipindai menggunakan ZXing.