

ABSTRAKSI

Aplikasi pembayaran *online* menggunakan mata uang digital sudah menjadi salah satu bagian terpenting dalam melakukan transaksi jarak jauh. Salah satunya yaitu merubah kebiasaan praktik transaksi di masyarakat, metode pembayaran ini tidak hanya berlaku bagi para pelaku penjual barang atau makanan secara *online*, dengan adanya fitur *QR Code* toko offline juga dapat menikmati teknologi pembayaran digital. Namun, platform pembayaran *online* selalu menjadi target utama untuk segala jenis kegiatan ilegal yang berimbas dengan adanya kerugian pada pihak pengguna maupun penyedia, keluhan ini didapat dari postingan beberapa pengguna aplikasi pembayaran *online* disalah satu forum costumer atau Media Konsumen.

Dengan adanya permasalahan tersebut, adanya beberapa upaya keamanan yang dapat di implementasikan untuk mengurangi kebocoran informasi data pengguna. Langkah keamanan ini termasuk pengenalan wajah untuk mengidentifikasi status kepemilikan akun dan *asymmetric encryption* agar isi konten komunikasi antara aplikasi dengan server berupa data aplikasi maupun data pribadi pengguna tidak mudah terbaca. Kedua fitur ini dapat membantu mengurangi risiko kebocoran data. Selain itu dalam praktik pengembangannya, untuk mencegah perbedaan versi yang dimiliki pengguna, melalui integrasi salah satu konsep yang di perkenalkan oleh Google yaitu *on demand module*, penerapan ini dapat dilakukan melalui komunikasi aplikasi dengan *server* dengan tujuan agar aplikasi memiliki versi keamanan yang lebih terbaru dan merata.

Kata Kunci: Pengenalan Wajah, *Machine Learning Kit Android*, Tensorflow, *QR-Code Kotlin*, Enkripsi menggunakan object model

ABSTRACT

Online payment applications utilizing digital currency have become crucial for facilitating long-distance transactions. One significant impact is the shift in transactional practices within society. This payment method extends beyond individuals solely selling goods or food online. The QR Code feature, present in offline stores, is now an integral part of digital payment technology adoption. However, online payment platforms continue to be prime targets for various illegal activities, resulting in financial losses for both users and providers. These concerns, voiced by users in customer forums and Consumer Media, underscore the urgency for enhanced security measures. In response, several security measures have emerged to mitigate data information leaks. These measures include implementing facial recognition for account ownership verification and utilizing asymmetric encryption to secure communication between the application and the server, preventing easy access to application data and user personal information. The incorporation of these features significantly reduces the risk of data leaks. Furthermore, in development practice, to prevent version disparities among users, an integration approach involves adopting the 'on-demand module' concept introduced by Google. This implementation ensures that the application communicates with the server to maintain an up-to-date security version.

Keywords: *Face Recognition, Machine Learning Kit Android, Tensorflow, QR-Code Kotlin, Encryption object model*