INTISARI

NFC-embeded smartphone mempunyai dua ekosistem, yaitu NFC-SIM-SE dan NFC-HCE. Salah satu kelemahan bagi NFC-HCE dari sisi keamanan adalah letak *secure elemen* di *cloud*. Kelemahan ini diatasi dengan membuat model untuk ekosistem NFC-HCE. Model inisialisasi dan transaksi dikembangkan sebagai solusi untuk dapat meningkatkan keamanan transaksi NFC-*enabled mobile*. Model ini memindahkan letak *secure elemen* ekosistem NFC-HCE dari *cloud* ke *smartphone* sehingga pada saat transaksi dilakukan, *smartphone* tidak perlu berkomunikasi dengan jaringan luar untuk mengakses *secure elemen*.

Model dibuat dengan membagi keseluruhan proses ke dalam dua bagian. Bagian pertama model inisialisasi digunakan untuk mendaftarkan akun dan menyimpan data akun terverifikasi ke *smartphone*, sedangkan bagian kedua model transaksi digunakan untuk transaksi antara pengguna dan POS. Model inisialisasi mendaftar akun pengguna, dikirimkan ke lembaga keuangan dalam bentuk terenkripsi. Data akun yang terverifikasi dikirimkan kembali ke *smartphone* untuk disimpan sebagai data kredensial. Model transaksi memastikan transaksi pembayaran *smartphone* dan POS berjalan dengan aman dan terverifikasi lembaga keuangan.

Model inisialisasi dan transaksi diuji dengan data *dummy* dan dilakukan pengujian sebanyak sekitar 500 kali setiap model, untuk menentukan tingkat keamanan menggunakan data acak. Pengujian mendapatkan nilai entropi 3,9954, nilai P 0,4205 dan waktu proses adalah 2,51 milidetik. Hasil pengujian menunjukkan bahwa proses enkripsi dapat meningkatkan keamanan ekosistem NFC-HCE. Hasil enkripsi yang acak dan waktu yang cepat menunjukkan bahwa transaksi aman. Uji coba model transaksi menunjukkan bahwa transaksi berjalan dengan aman karena data enkripsi terbukti acak dan waktu eksekusi adalah 1,074 milidetik, dibawah waktu yang diperlukan penyerang untuk mengartikan data terenkripsi. Capaian ini membuat peluang pada penyerang untuk memanipulasi data menjadi kecil, sehingga keamanan meningkat.

Kata kunci: NFC, sistem keamanan, ekosistem, *smartphone*

ABSTRACT

NFC-embeded smartphones have two ecosystems, namely NFC-SIM-SE and NFC-HCE. One of the weaknesses for NFC-HCE in terms of security is the location of the secure elements in the cloud. This weakness is overcome by creating a model for the NFC-HCE ecosystem. The initialization and transaction model is developed as a solution to increase the security of NFC-enabled mobile transactions. This model transfers the location of the secure elements of the NFC-HCE ecosystem from the cloud to the smartphone. In this way the smartphone does not need to communicate with an external network to access the secure element in time of transaction

The model is developed by dividing the whole process into two parts. The first part of the initialization model is to register an account and save the verified account data to the smartphone, while the second part of the transaction model is used for transactions between the user and the POS. The initialization model registers user accounts and sends to financial institutions in an encrypted form. The verified account data is sent back to the smartphone to be stored as credential data. The transaction model ensures that smartphone and POS payment transactions run safely. It also ensures that they are verified by financial institutions.

The initialization model and transaction model was tested using dummy data. Each model underwent 500 tests to determine the level of security using random data. The test gets an entropy value of 3.9954, a P value of 0.4205 and a processing time of 2.51 milliseconds. The test results show that the encryption process can increase the security of the NFC-HCE ecosystem. Random and fast encryption results indicate that transactions are secure. The transaction model test shows that the transaction runs safely because the encrypted data is proven to be random and the execution time is 1,074 milliseconds. The time 1,074 ms is far below the time an attacker takes to decipher the encrypted data. This achievement makes the opportunity for attackers to manipulate data to be small, so security is increased.

Keywords: NFC, security system, ecosystem, *smartphone*