Abstrak

Jumlah ancaman pada perangkat seluler meningkat 261% pada tahun 2013. Salah satu faktor yang memicu peningkatan jumlah ancaman tersebut adalah meningkatnya transaksi pembayaran menggunakan *mobile payment*. Usaha untuk mengatasi ancaman tersebut telah dilakukan, seperti menggunakan metode enkripsi, *Public Key Infrastucture* (PKI) dan penerapan *One Time Password* pada transaksi perbankan. Namun demikian, cara-cara konvensional seperti ini menimbulkan masalah pada *constrained device*. Metode *public key cryptosystem Identity Based Encryption - Elliptic Curve Cryptography* (IBE-ECC) telah diusulkan untuk mengatasi kelemahan yang ada di sistem tradisisonal tersebut. Ini disebabkan fitur IBE yang dapat menerima semua *String* sebagai *Public Key* yang valid. IBE juga dapat mempermudah manajemen sertifikat. Namun, sayangnya baru beberapa penelitian yang telah menguji metode IBE-ECC dengan metode yang lainnya, seperti IBE-RSA. Masih sedikit pula metode IBE-ECC yang diimplementasikan pada *smartphone android*. Selain itu IBE-ECC yang sudah ada kurang optimal dalam hal *running time* dan *memory usage*. Oleh karena itu, penelitian ini merancang desain IBE-ECC yang diusulkan dan mengimplementasikannya pada *smartphone android* serta mengujinya dengan metode IBE-RSA. Diharapkan dengan mengoptimalkan jumlah multiplikatif poin ECC akan meringankan beban komputasi dan mempercepat *running time* sistem IBE-ECC. Metoda yang dipakai dalam penelitian ini sebagai berikut : 1) Melakukan studi pustaka terhadap metode IBE-ECC, 2) Memodifikasi metode tersebut, 3)Pengujian performansi metode yang diusulkan tersebut dengan pembanding metode yang sudah ada dan kami analisis hasilnya. Berdasarkan pengujian, performa metode yang diusulkan pada tugas akhir ini dinilai lebih baik, yaitu rata-rata 5,5% *running time* lebih cepat dari metode IBE-ECC BF dan rata-rata 89,9% *running time* lebih cepat dari metode IBE-RSA. Selain itu, metode yang diusulkan rata-rata lebih hemat dalam penggunaan *Random Access Memory* (RAM) 20,46 kB dari IBE-ECC BF dan 6287,46 kB dari IBE-RSA. IBE-ECC yang diusulkan memiliki ketahanan yang sama terhadap *Bruteforce Attack* dengan IBE-ECC BF dan lebih baik 564% dibanding metode IBE-RSA dengan besar kunci *private* yang sama.

Kata Kunci: Enkripsi, ECC, RSA, IBE, Smartphone.