BAB 5

SIMPULAN DAN SARAN

5.1. Simpulan

Berdasarkan implementasi, pengujian, dan evaluasi yang telah dilakukan, terdapat beberapa kesimpulan yang dapat ditarik, yaitu.

1. Implementasi *hybrid encryption* menggunakan CRYSTALS-Kyber sebagai *asymmetric encryption* dan AES-256 sebagai *symmetric encryption* berhasil dilakukan pada *smart contract* aplikasi autentikasi produk Oricon.
2. Implementasi halaman key pada aplikasi autentikasi produk Oricon juga berhasil dilakukan yang memungkinkan pengguna *admin* perusahaan untuk mengganti *key size* yang akan digunakan dalam proses enkripsi maupun dekripsi data.
3. *Key size* CRYSTALS-Kyber 768 memiliki performa kriptografi paling optimal dibandingkan dua *key size* lainnya, yang terbukti sesuai dengan *key size* yang disarankan pada CRYSTALS-Kyber. Hal ini terlihat dari hasil evaluasi, di mana peningkatan waktu enkripsi dan dekripsi yang cenderung stabil dibandingkan dengan dua *key size* lainnya saat ukuran data yang digunakan membesar.

4. *Key size* CRYSTALS-Kyber 768 merupakan *key size* yang paling optimal untuk diimplementasikan pada *smart contract* aplikasi autentikasi produk Oricon dibandingkan dengan dua *key size* lainnya. Hal ini terlihat dari nilai transaksi sukses dari *key size* 768 lebih tinggi dibadingkan dengan *key size* 512 dan 1024 pada dua dan empat *workers*, yaitu sebesar 365,6 dan 618,8 transaksi yang sukses. *Key size* 768 memiliki transaksi gagal yang lebih tinggi dibandingkan dua *key size* lainnya karena jumlah *throughput key size* 768 yang paling besar, yaitu sebesar 12,16 TPS pada dua *workers* dan 20,48 TPS pada empat *workers*, sehingga jumlah transaksi terbanyak setiap detiknya dipegang oleh *key size* 768. Selain itu, *key size* 768 memiliki nilai *latency* yang cukup rendah yaitu sebesar 3,396 detik pada dua *workers* dan 3,544 detik pada empat *workers*.
5. Pengimplementasian *key size* 768 berpengaruh pada menurunnya jumlah *throughput* yang dihasilkan, yaitu sebesar -57,03% saat menggunakan dua *workers* dan -52,15% saat menggunakan empat *workers*. Penurunan pada pengimplementasian *key size* 768 terbukti masih lebih baik dibandingkan dengan penurunan saat pengimplementasian *key size* 512 dan *key size* 1024 yaitu sebesar 68,69% pada dua *workers* dan 74,91% pada empat *workers*, serta 66,5% pada dua *workers* dan 62,57% pada empat *workers*.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk peneliti selanjutnya yang akan meneliti hal serupa, yaitu sebagai berikut.

1. Mengimplementasikan algoritma *post-quantum* CRYSTALS-Kyber sebagai algoritma *digital signature* pada Hyperledger Fabric. Hal ini dikarenakan *digital signature* dari Hyperledger Fabric saat ini hanya mendukung RSA dan ECDSA saja.
2. Mengimplementasikan algoritma *post-quantum* CRYSTALS-Kyber sebagai *End-to-End Encryption* pada aplikasi autentikasi produk Oricon dari sisi komunikasi antara *client* dan *server*. Hal ini dikarenakan data yang dikirimkan antara *client* dan *server* masih berupa *plaintext*, sehingga bisa ditingkatkan lagi menjadi *ciphertext* yang juga tahan dari serangan kuantum.