ABSTRAK

Arsitektur blockchain *hibrida* (on-chain/off-chain) *pada Hyperledger Fabric menawarkan solusi untuk efisiensi dan skalabilitas sistem rantai pasok farmasi. Namun, arsitektur ini memunculkan serangan baru yang berfokus pada integritas jaringan. Penelitian ini bertujuan untuk menganalisis ketahanan keamanan dan kinerja arsitektur hibrida MediSync terhadap tiga vektor serangan spesifik: (1) Kompromi Kunci Privat, (2) Aktor Jahat* (Malicious Peer)*, dan (3) Serangan Saturasi (DoS).*

Metodologi penelitian yang digunakan adalah simulasi serangan dalam lingkungan terkontrol berbasis Docker. Skenario Kompromi Kunci Privat diuji menggunakan skrip Node.js *kustom untuk memvalidasi keamanan MSP* chaincode*. Skenario Aktor Jahat diuji dengan skrip kustom untuk memvalidasi Kebijakan* Endorsement *(AND).*

Hasil pengujian menunjukkan bahwa arsitektur MediSync berhasil memitigasi serangan terhadap integritas dan otorisasi. Skenario Kompromi Kunci gagal dengan error TransactionError: Organisasi PBFMSP tidak diizinkan. Skenario Aktor Jahat juga gagal dengan status ENDORSEMENT_POLICY_FAILURE. Pada Skenario Serangan Saturasi, sistem mengalami degradasi kinerja di mana latensi rata-rata pengguna sah melonjak dari 186 ms (baseline*) menjadi 1.145 ms (selama serangan), atau terjadi penurunan kinerja sebesar 516%. Meskipun demikian, sistem terbukti resilien; pada beban puncak 1.000* user *yang melumpuhkan penyerang (*error *29.58%), layanan bagi pengguna sah tetap tersedia sepenuhnya* (error *0%) dengan latensi stabil. Penelitian ini membuktikan bahwa arsitektur hibrida Hyperledger Fabric tangguh terhadap ancaman otorisasi dan integritas data, serta mampu mengisolasi dampak serangan ketersediaan (DoS) sehingga layanan bagi pengguna sah tetap terjaga.*

Kata Kunci: *Hyperledger Fabric, Arsitektur Hibrida, Keamanan* Blockchain, *Rantai Pasok Farmasi, Serangan Saturasi, Kompromi Kunci, Kebijakan Endorsement.*