ABSTRAK

Pertukaran kunci yang aman sangat penting untuk memastikan integritas dan kerahasiaan komunikasi dalam Sistem Peringatan Dini (*Early Warning System*/EWS) berbasis IoT. Penelitian ini mengevaluasi kinerja skema Boneh-Boyen Hierarchical Identity-Based Encryption (BB-HIBE) sebagai alternatif dari mekanisme pertukaran kunci konvensional seperti TLS/ECDH. Simulasi dilakukan pada lingkungan mesin virtual Microsoft Azure untuk membandingkan BB-HIBE dan TLS/ECDH dari segi *communication overhead* dan kebutuhan penyimpanan kunci. Selain itu, BB-HIBE dievaluasi pada dua tingkat keamanan (ukuran kunci 128-bit dan 256-bit) untuk menilai waktu eksekusi, penggunaan CPU, dan kebutuhan memori. Hasil penelitian menunjukkan bahwa BB-HIBE secara signifikan mengurangi *communication overhead* dan penyimpanan kunci dibandingkan TLS/ECDH, terutama ketika jumlah pengguna meningkat. Lebih lanjut, implementasi BB-HIBE dengan kunci 128-bit memenuhi standar latensi internasional di bawah 100 ms yang direkomendasikan untuk komunikasi IoT secara *real-time*.

Kata Kunci: BB-HIBE, Key Exchange, Early Warning Systems.