ABSTRAK

Internet of Health Things (IoHT) memainkan peran penting dalam layanan kesehatan modern, memungkinkan pemantauan pasien secara real-time dan diagnostik jarak jauh melalui perangkat yang saling terhubung. Namun, protokol seperti MQTT, meskipun efisien, masih memiliki kelemahan dalam fitur keamanannya, sehingga data kesehatan yang sensitif rentan terhadap serangan siber. Seiring dengan berkembangnya teknologi IoT dalam dunia kesehatan, perlindungan terhadap data utama (*payload*) maupun metadata menjadi sangat penting demi menjaga privasi dan kepercayaan pasien.

Studi ini mengusulkan skema keamanan dua lapisan yang dirancang untuk mengatasi kerentanan tersebut dengan mengintegrasikan enkripsi ASCON (*Authenticated Encryption with Associated Data*) untuk perlindungan *payload*, serta *Zero-Width Characters* (ZWC) untuk penyembunyian metadata secara terselubung. Kombinasi dari dua teknik ini memberikan solusi keamanan yang menyeluruh, memastikan bahwa baik data medis maupun metadata terkait seperti pengenal perangkat, informasi pasien, dan level QoS dapat ditransmisikan secara aman tanpa terekspos pada ancaman seperti serangan inferensi metadata atau analisis lalu lintas jaringan. Hasil eksperimen menunjukkan bahwa penerapan ASCON bersama ZWC menyebabkan sedikit peningkatan latensi, yaitu dari 0,54 milidetik untuk payload kecil (8 KB) hingga 18,93 milidetik untuk payload besar (1 MB). Namun, kompromi antara kinerja dan keamanan ini masih dalam batas yang dapat diterima. Sistem ini juga menunjukkan efek avalanche yang kuat, berkisar antara 51,02% hingga 51,25%, menandakan sensitivitas tinggi terhadap perubahan input dan memperkuat ketahanannya terhadap serangan kriptografi. Selain itu, beban komputasi tetap terkendali, dengan peningkatan penggunaan CPU yang relatif kecil, yaitu hanya 1,2%, dari 88,93% menjadi 90,14% seiring bertambahnya ukuran *payload*.

Dengan menyediakan enkripsi untuk payload serta penyembunyian metadata, pendekatan ini berhasil mengatasi masalah keamanan kritis dalam aplikasi layanan kesehatan real-time. Integrasi ZWC sebagai saluran terselubung memastikan bahwa metadata sensitif dapat disembunyikan tanpa mengganggu struktur protokol MQTT, sehingga menjadikan solusi ini ideal untuk komunikasi dalam IoHT.

Keywords: MQTT, AEAD, ASCON, Saluran Terselubung, Perlindungan Metadata, Enkripsi Ringan, Komunikasi Aman, IoT Kesehatan.