

ABSTRAK

Perkembangan *Internet of Things* (IoT) yang pesat telah meningkatkan ancaman siber terhadap perangkat *edge* dengan sumber daya terbatas. Penelitian ini mengusulkan SATSET (*Spiking-based Antifragile Twin for Self-healing Edge Technology*), sebuah sistem deteksi anomali berbasis *Spiking Neural Network* (SNN) dengan mekanisme antifragilitas dan *self-healing* yang diimplementasikan pada perangkat edge Raspberry Pi 5. Sistem ini menggabungkan pendekatan deteksi *cross-layer* antara fitur jaringan (*n_packets*, *total_bytes*) dan *Hardware Performance Counter* (HPC) (*cache_misses*, *instructions*) untuk meningkatkan akurasi deteksi terhadap serangan yang tidak terlihat di lapisan jaringan. Model SNN dilatih menggunakan dataset IoT-23 dan divalidasi pada CICIoT2023, dengan arsitektur 4 neuron input, 64 dan 32 neuron hidden LIF, serta 2 neuron output. Hasil pengujian menunjukkan akurasi lintas-dataset sebesar 94,66% dan F1-Score 97,13%. Ablation study membuktikan kontribusi HPC meningkatkan F1-Score sebesar 17,35% dan menurunkan False Negative Rate dari 31% menjadi 1,57%. Mekanisme antifragile diimplementasikan melalui Spike-Timing Dependent Plasticity (STDP) yang memperbarui bobot sinapsis secara online setiap kali serangan terdeteksi. Mean Time To Recovery (MTTR) self-healing tercatat rata-rata 4,3 detik pada perangkat edge. Penelitian ini membuktikan bahwa integrasi SNN, deteksi cross-layer, dan mekanisme antifragile layak diimplementasikan pada perangkat edge berbiaya rendah untuk keamanan IoT yang adaptif dan otonom.

Kata Kunci: Spiking Neural Network, Antifragilitas, Self-Healing, Edge Computing, IoT Security, Hardware Performance Counter.