ABSTRAK

Deteksi *Rogue Access Point* (RAP) sangat penting untuk menghindari serangan *Evil Twin Attack* (ETA) di lingkungan kampus, seperti yang dilakukan di Telkom University, khususnya di gedung TULT. Penelitian ini bertujuan untuk mengembangkan dan menguji model *Machine Learning* (ML) yang mampu mendeteksi RAP berdasarkan data yang dikumpulkan menggunakan airodump-ng. Data yang diperoleh mencakup berbagai parameter jaringan, seperti *Channel, Speed, Privacy, Cipher, Authentication, Power,* dan *beacons*.

Proses pengujian dimulai dari pengumpulan data menggunakan perangkat TP-Link WN821N dan airodump-ng Linux Ubuntu. Data yang dikumpulkan kemudian disimpan dalam format CSV dan diunggah ke Firebase Realtime Database. Data ini kemudian diolah menggunakan teknik *encoding* dengan metode *one-hot encoding* pada fitur kategorikal, seperti *Privacy*, *Cipher, dan Authentication.* Setelah itu, data yang sudah diolah digunakan untuk melatih model ML menggunakan algoritma *Feedforward Neural Network* (FNN) dengan *arsitektur sequential*.

Hasil pengujian menunjukkan bahwa model mengalami peningkatan akurasi dan penurunan nilai *loss* yang signifikan. Pada beberapa epoch, nilai loss melonjak dan akurasi menurun drastis, yang menunjukkan adanya potensi masalah seperti *overfitting* dan *underfitting*. Model mencapai akurasi tertinggi sebesar 99.72% dengan nilai *loss* 0.04296. Pengujian *Quality of Service* (QoS) juga dilakukan untuk mengukur *throughput, delay*, dan *packet loss* dalam mengakses database Firebase dan *dashboard*. Hasil pengujian menunjukkan bahwa *throughput* rata-rata adalah 12416.03 bits/detik. *Delay* rata-rata tercatat sebesar 0.18 detik, dengan variasi antara 0.12 hingga 0.29 detik. Tidak ada *packet loss* yang terdeteksi dalam pengujian ini, dengan rata-rata 0.000%. Penelitian ini menunjukkan bahwa model ML efektif dalam mendeteksi RAP dan dapat diandalkan untuk diterapkan dalam lingkungan jaringan yang lebih luas. Hasil pengujian QoS menunjukkan kinerja jaringan yang baik. Hal ini memberikan dasar yang kuat untuk pengembangan lebih lanjut dan implementasi praktis dalam meningkatkan keamanan jaringan nirkabel di lingkungan kampus.

Kata Kunci : *Rogue Access Point* (RAP), *Evil Twin Attack* (ETA), *Machine Learning* (ML), *Feedforward Neural Network* (FNN), *Quality of Service* (QoS).