

ABSTRAK

Peningkatan pesat penggunaan Wi-Fi publik di berbagai lokasi komersial seperti coffee shop, telah menciptakan tantangan serius terkait keamanan jaringan dan kebutuhan akan analisis data operasional. Proyek akhir ini bertujuan untuk mengembangkan solusi keamanan jaringan nirkabel terintegrasi dengan menggabungkan *Remote Authentication Dial-In User Service* (RADIUS) dan *Automated Password Generator* pada Mikrotik RouterOS. Sistem ini dirancang untuk menghasilkan kredensial unik untuk setiap transaksi pelanggan. Untuk mengatasi potensi serangan otomatis seperti *brute force*, fitur CAPTCHA diimplementasikan pada halaman *login* hotspot. Selain itu, mekanisme *rate limiting* juga diterapkan pada *API backend* sebagai lapisan pertahanan tambahan. Sistem ini juga dirancang untuk mengumpulkan, menyimpan, serta memvisualisasikan data penggunaan Wi-Fi (seperti durasi sesi dan jumlah pengguna) secara kuantitatif untuk analisis bisnis. Hasil pengujian menunjukkan bahwa sistem dapat membuat kredensial dan mencetak struk dengan efisien (dengan rata-rata 3.81 detik). Pengujian CAPTCHA berhasil menahan akses *bot*, sementara mekanisme *rate limiting* efektif melawan serangan permintaan berlebihan (berhasil memblokir 95 dari 100 permintaan pada endpoint `/create-user`). Pengujian keamanan transmisi data menggunakan Wireshark juga mengonfirmasi bahwa kredensial pengguna dikirim dalam format terhash, bukan teks biasa, sehingga aman dari penyadapan. Solusi ini tidak hanya meningkatkan keamanan jaringan, tetapi juga menyediakan wawasan operasional yang berharga bagi pemilik bisnis.

Kata Kunci: *Automated Password Generator*, CAPTCHA, Keamanan Jaringan, Mikrotik, RADIUS, Sistem Kasir, Wi-Fi