ABSTRACT

The rapid increase in public Wi-Fi usage in commercial locations such as coffee shops has created serious network security challenges and a need for operational data analysis. This final project aims to develop a comprehensive wireless network security solution by integrating Remote Authentication Dial-In User Service (RADIUS) and an Automated Password Generator on Mikrotik RouterOS. The system is designed to generate unique credentials for each customer transaction. To counter potential automated attacks like brute force, a custom-built CAPTCHA feature is implemented on the hotspot login page. Furthermore, a rate-limiting mechanism is applied to the backend API as an additional layer of defense. The system is also engineered to automatically collect, store, and quantitatively visualize Wi-Fi usage data (such as session duration and user count) for business analysis. Test results indicate that the system can efficiently generate credentials and print receipts (with an average of 3.81 seconds). CAPTCHA testing successfully resists bot access, while the rate limiting mechanism proves effective against excessive request attacks (successfully blocking 95 out of 100 requests on the /create-user endpoint). Security testing with Wireshark also confirmed that user credentials are sent in a hashed format, not plaintext, ensuring protection against sniffing. This solution not only enhances network security but also provides valuable operational insights for business owners.

Keywords: Automated Password Generator, CAPTCHA, Mikrotik, Network Security, POS System, RADIUS, Wi-Fi, Cashier System, Wi-Fi