

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, dan pengujian, sistem Smart Padlock yang menggunakan ESP32, sensor sidik jari AS608, RFID RC522, serta integrasi IoT melalui aplikasi Blynk, terbukti berhasil mengimplementasikan autentikasi ganda berbasis sidik jari dan kartu RFID untuk membuka dan mengunci solenoid lock pada kendaraan roda dua. Mikrokontroler ESP32 mampu menjalankan seluruh logika sistem secara mandiri tanpa bantuan mikrokontroler lain, serta terhubung ke internet untuk mengirim notifikasi real-time ke aplikasi Blynk. Sistem menunjukkan performa yang cepat dan efisien dengan rata-rata waktu respon 2,2–2,9 detik dari proses input autentikasi hingga aktivasi solenoid. Selain itu, sistem mampu memberikan notifikasi status terkini kepada pengguna, seperti status TERBUKA dan TERKUNCI, melalui aplikasi Blynk. Berdasarkan hasil uji coba sebanyak 20 kali, tingkat keberhasilan autentikasi mencapai 95%, dengan kesalahan yang hanya disebabkan oleh posisi jari yang tidak tepat atau tag RFID yang rusak. Dengan demikian, sistem Smart Padlock ini layak menjadi alternatif solusi keamanan modern untuk kendaraan roda dua, menggantikan metode kunci konvensional yang lebih rentan terhadap pencurian.

5.2 Saran

Untuk pengembangan lebih lanjut dari penelitian ini, beberapa saran yang dapat dipertimbangkan antara lain adalah menambahkan fitur penyimpanan data histori autentikasi dengan menggunakan memori eksternal seperti SD Card atau mengintegrasikannya ke database online seperti Firebase, sehingga data dapat tersimpan dan diakses dengan lebih aman serta terstruktur. Selain itu, disarankan untuk menyediakan aplikasi mobile khusus yang memungkinkan pengguna membuka kunci melalui koneksi Bluetooth atau internet, sehingga tidak selalu bergantung pada sensor fisik. Pengembangan juga dapat mencakup penambahan sensor tambahan, seperti sensor getaran atau GPS, guna meningkatkan cakupan sistem keamanan terhadap pencurian atau gangguan fisik. Terakhir, penting untuk mengintegrasikan sistem proteksi otomatis, seperti alarm atau notifikasi darurat kepada pengguna, apabila terdeteksi percobaan akses berturut-turut yang gagal, sebagai bentuk pencegahan terhadap upaya pembobolan.