BAB V
SIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1 Simpulan

Berdasarkan penelitian yang telah dilakukan oleh penulis, didapatkan simpulan dengan *point-point* sebagai berikut:

1. Pengembangan sistem pengamanan pintu RFID berbasis IoT dengan algoritma enkripsi AES-128 pada protokol komunikasi MQTT berhasil terbuat. Penelitian yang dilakukan menggunakan metode penelitian DRM (*Design Research Methodology*) dengan metode pengembangan sistemnya adalah *Agile.*
2. Pengujian untuk pengembangan sistem dilakukan dengan menggunakan metode *Black-box Testing*. Hasilnya memenuhi kebutuhan fungsionalitas dan semua fitur bekerja.
3. Pengaruh dari implementasi algoritma enkripsi AES-128 dalam sistem pengamanan pintu RFID berbasis IoT adalah positif untuk berhasil mencegah penyalahgunaan hak akses otorisasi pintu RFID yang dapat dilakukan oleh penyerang dalam menduplikasi UID kartu *tag* RFID dan meminimalisir terjadinya serangan *network sniffing* dan MiTM.
4. Evaluasi performa dari hasil pengujian sistem pada proses *scanning Tap IN dan Tap OUT* menggunakan kartu eKTP didapat lebih lambat ketimbang *contactless card tag* RFID lainnya. Serta mengkaji proses kecepatan enkripsi AES-128 pada beberapa *hardware microcontroller* yang dimana dimenangkan oleh ESP32 pada **Sub-bab 4.3.2**.
5. Kemudian ketahanan dari *decode ciphertext* yang dihasilkan oleh AES-128 sangatlah kuat dan aman dari berbagai serangan *bruteforce* dikarenakan mendapatkan hasil korelasi koefisien Pearson yang sangat rendah hampir mendekati 0.

5.2 Implikasi

Berkembangnya pasar sistem RFID menjadikan implikasi dari penelitian ini yaitu sistem pengamanan pintu RFID berbasis IoT yang dikembangkan dengan implementasi algoritma enkripsi AES-128 digunakan untuk standar industri

ruangan dengan kredensial objek atau data yang tinggi seperti ruangan server, ruangan balita rumah sakit, laboratorium, gudang, dan brankas. Tujuannya agar mencegah terjadinya kejahatan pencurian data pada ekosistem IoT (*insecure data transfer and storage*) terutama UID kartu RFID dari serangan *network sniffing* dan MiTM (*Man-in-the-Middle*) yang mengancam data atau objek kredensial ruangan yang penting.

5.3 Rekomendasi

Berdasarkan proses dan hasil penelitian yang telah dilakukan, adapun rekomendasi terhadap penelitian selanjutnya adalah sebagai berikut:

1. Pengujian untuk kecepatan enkripsi AES-128 pada perangkat *lightweight* IoT seperti *microcontroller* belum sepenuhnya lengkap, perlu dilakukan pengujian pada perangkat seperti ESP8266, STM32, Teensy4.0, dan Tiva C *Series* agar lengkap dan tidak bias.
2. Kecocokan pemilihan penggunaan *module* RFID *reader* perlu dikaji ulang, berdasarkan pengujian pada **Sub-bab 4.3.1** didapatkan bahwasannya untuk pembacaan eKTP Indonesia membutuhkan waktu pembacaan lebih lama ketimbang *contactless card* lainnya.
3. Pengembangan lebih lanjut untuk kebaruan sistem dari penambahan sensor untuk mengetahui apakah *doorlock* solenoid sudah tertutup rapat atau belum, hal ini agar memastikan pintu telah tertutup rapat.
4. Pengembangan lebih lanjut dalam pengimplementasian sumber daya cadangan menggunakan energi terbarukan seperti panel surya untuk studi kasus jika sistem pengamanan pintu RFID tidak dapat beroperasi karena mati listrik dalam sumber daya utamanya.