

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian tersebut dapat disimpulkan bahwa:

1. Implementasi sistem keamanan data pada perangkat IoT menggunakan kriptografi AES terbukti sesuai dengan studi literatur yang telah dilakukan, sehingga dapat disimpulkan bahwa algoritma AES ini dapat digunakan pada perangkat IoT sesuai dengan daya komputasi yang dimilikinya serta tidak mengganggu jalannya sistem yang sudah berjalan sebelumnya.
2. Dengan menambahkan identitas pada ciphertext menjadikan ciri unik agar web server dapat mengidentifikasi bahwa ciphertext tersebut berasal dari perangkat IoT.

5.2 Saran

Berdasarkan hasil penelitian tersebut terdapat beberapa hal yang menjadi saran untuk penelitian selanjutnya yaitu:

1. Memodifikasi algoritma AES supaya menghasilkan performa yang lebih cepat sehingga waktu *delay* transmisi data menjadi berkurang dan lebih baik.
2. Permasalahan penyimpanan kunci pada perangkat IoT menjadi hal yang perlu dipertimbangkan, mengingat pelaku usaha sendiri belum tentu dari kalangan yang mengerti perihal pengkodean sistem, kedepannya bisa memodifikasi perangkat IoT agar dapat menyimpan kunci dengan otomatis tanpa melibatkan pelaku usaha untuk melakukan *hardcode*.