BAB V
KESIMPULAN

5.1. Kesimpulan

Dari hasil penelitian yang telah dilakukan, dihasilkan beberapa kesimpulan yang ada:

1. Metode ECIES mengamankan data yang dikirm dari *microcontroller* ke server dengan cara menenkripsi data sensor kedalam bentuk *ciphertext* dan kemudian akan di dekripsi di server sebelum data tersebut disimpan di *database*.
2. Berdasarkan hasil dari pengujian *Man-In-The-Middle* yang telah dilakukan, menunjukkan bahwa sistem yang telah dibuat tahan terhadap serangan yang dilakukan dengan cara mencuri hasil yang dikirimkan oleh perangkat IoT dan melakukan perubahan nilai dengan cara XOR sepanjang 32 bytes hasil tersebut.
3. Sesuai dengan hasil pengujian yang telah dilakukan, tingkat kompleksitas *randomness* pada sistem enkripsi data *smart home* memiliki hasil yang cukup baik dengan *p-values* diatas 0,01 dan ini memenuhi kriteria syarat keacakan dari metode *Run Test*.
4. Sistem enkripsi *Smart Home* yang telah dibangun telah memenuhi aspek *confidentiality* dan *integrity* sesuai dengan hasil pengujian yang menunjukkan data yang telah terenkripsi sulit untuk diketahui data aslinya, dan data yang telah di dekripsi sesuai dengan data asli yang diperoleh dari sensor.

5.2. Saran

Berikut beberapa saran yang dapat diterapkan pada penelitian selanjutnya dalam sistem enkripsi *smart home* dengan menggunakan metode ECIES:

1. Menambahkan variabel pada penghasil kunci yang digunakan untuk enkripsi agar meningkatkan tingkat kompleksitas *randomness*.

2. Implementasi ECIES tidak hanya dapat diterapkan pada perangkat IoT untuk *Smart Home* saja, akan tetapi dapat diterapkan pada perangkat IoT untuk segala lingkungan yang dibutuhkan.