

ABSTRACT

Lack of cryptography usage in making Internet of Things (IoT) projects cause many privacy threat for the users. There is a need for a system that guarantees security aspects of IoT network traffic. Modern cryptographic algorithms are used in electrical power consumption monitoring systems to secure data in the form of electrical current from any privacy threats by unwanted parties.

The electrical power consumption monitoring system uses the non-invasive SCT-013-000 sensor on Wemos D1 ESP8266 microcontroller, using the encryption algorithm Advanced Encryption Standard (AES) with Cipher Blocker Chaining (CBC) mode and using 128, 192, and 256 bit key lengths. System integrated with Amazon web server.

The average Avalanche effect value for each key length of 128, 192, and 256 bits is 46% with an electricity consumption of 36 milliAmpere. AES allocates memory of 128, 192, and 256 bits to store each key length with processing times of 830.11 μ s, 850.87 μ s, and 883.26 μ s for key lengths of 128, 192, and 256 bits. The average QoS value of the Wemos D1 ESP8266 microcontroller from / to the cloud server for each different key length are Delay of 0.34 seconds and Throughput of 2244.2 bits/s.

Key words: *Internet of Things, Advanced Encryption Standard, Amazon web server, SCT-013-000, Wemos D1 ESP8266*