Abstract

Data security in the context of the Internet of Things (IoT) is becoming increasingly important with advancements in information technology, especially in temperature monitoring applications. Although the Advanced Encryption Standard (AES) cryptographic algorithm is often chosen, alternative lightweight algorithms such as Small AES need to be considered. This study aims to implement and evaluate the performance of Small AES on an Arduino platform with a case study of temperature monitoring. The evaluation is conducted by comparing Small AES with the SPECK algorithm in terms of encryption and decryption speed, memory usage, and the Bit Avalanche Test. The results show that Small AES is not superior to SPECK in terms of encryption and decryption speed. However, Small AES excels in using less memory compared to SPECK. From the results of Bit Avalanche Test, Small AES is better for large data while SPECK is better for small data.

Keywords: AES, Bit Avalanche Test, IoT, Small AES, SPECK, Temperature Monitoring