INTISARI

THE IMPACT OF ADVANCED ENCRYPTION STANDARD (AES) ON WIRELESS SENSOR NETWORK DELAY

Internet of Things (IoT) semakin hari semakin populer dan banyak dikembangkan untuk memenuhi kebutuhan komunikasi antar berbagai perangkat. Salah satu bidang teknologi dalam IoT yang banyak dikembangkan adalah *Wireless Sensor Network* (WSN). Dalam implementasi WSN, keamanan jaringan menjadi isu cukup penting. Salah satu fokus keamanan jaringan adalah mengenai integritas data. Algoritma *Advanced Encryption Standard* (AES) adalah salah satu algoritma kriptografi yang dapat mempertahankan integritas data pada WSN. AES bekerja dengan cara merubah data *plaintext* menjadi *chipertex* (enkripsi), dan sebaliknya (dekripsi). Penerapan algoritma AES tentu menambah keamanan, tetapi proses enkripsi dan dekripsi data oleh AES ini secara langsung berpengaruh pada *delay* jaringan. Selisih *delay* antara rangkaian WSN 1 receiver-1 *transmitter* tanpa AES dan rangkaian WSN 1 *receiver*-1 *transmitter* dengan AES adalah 0.347 detik. Selisih *delay* antara rangkaian WSN 1 *receiver*-2 *transmitter* tanpa AES dan rangkaian WSN 1 *receiver*-2 *transmitter* dengan AES adalah 0.358 detik. Selisih *delay* antara rangkaian WSN 1 *receiver*-3 *transmitter* tanpa AES dan rangkaian WSN 1 *receiver*-3 *transmitter* dengan AES adalah 0.366 detik. Jaringan yang menggunakan enkripsi AES terbukti memiliki *delay* yang lebih besar dibandingkan dengan jaringan tanpa AES.

Kata Kunci: *Internet of Things* (IoT), *Wireless Sensor Network* (WSN), *Advanced Encryption Standard* (AES)

ABSTRACT

PENGARUH ENKRIPSI *ADVANCED ENCRYPTION STANDARD* (AES) TERHADAP DELAY PADA *WIRELESS SENSOR NETWORK*

Internet of Things (IoT) is increasingly popular and is being developed to meet the communication needs of various devices. One of the technology fields in IoT that has been developed is the Wireless Sensor Network (WSN). In WSN implementation, network security is one of important issues. One focus of network security is about data integrity. The Advanced Encryption Standard (AES) algorithm is one of the cryptographic algorithms that can maintain data integrity in the WSN. AES works by changing plaintext data to ciphertext (encryption), and vice versa (decryption). The implementation of the AES algorithm certainly adds security, but the process of data encryption and decryption by AES directly affects network delay. This research shows that the delay difference between the WSN circuit 1 receiver-1 transmitter without AES and the WSN circuit 1 receiver-1 transmitter with AES is 0.347 seconds. The delay difference between the WSN circuit 1 receiver-2 transmitter without AES and the WSN circuit 1 receiver-2 transmitter with AES is 0.358 seconds. The delay difference between the WSN circuit 1 receiver-3 transmitter without AES and the WSN circuit 1 receiver-3 transmitter with AES is 0.366 seconds. Networks that use AES encryption are proven to have greater delay compared to networks without AES.

Kata Kunci: Internet of Things (IoT), Wireless Sensor Network (WSN), Advanced Encryption Standard (AES)