PERANCANGAN MULTIPLE JARINGAN SENSOR NIRKABEL MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD

TUGAS AKHIR

Karya Ilmiah sebagai salah satu syarat untuk menyelesaikan jenjang Strata Satu (S-1) di Departemen Teknik Elektro, Fakultas Teknik, Universitas Andalas

Oleh:

Muhammad Fauzan Fadhilah

NIM. 1910952036

Pembimbing:

Darmawan, M.Sc

NIP. 197708162005011002

Program Studi Sarjana Teknik Elektro

Fakultas Teknik

Universitas Andalas

2024

Judul	Perancangan Multiple Jaringan Sensor Nirkabel Menggunakan Algoritma Kriptografi *Advanced Encryption Standard*	Muhammad Fauzan Fadhilah
Program Studi	Teknik Elektro	1910952036
Fakultas Teknik Universitas Andalas		

Abstrak

Indonesia telah mengalami peningkatan signifikan dalam pengembangan teknologi *Internet of Things* (IoT) dalam beberapa tahun terakhir. IoT memungkinkan perangkat dengan sensor untuk berkomunikasi dan bertukar data melalui internet, memainkan peran penting dalam mendukung revolusi industri 4.0. Salah satu komponen utama IoT adalah Jaringan Sensor Nirkabel (JSN), yang memungkinkan pengumpulan dan transmisi data tanpa batasan fisik kabel. Namun, dengan meningkatnya aplikasi IoT, serangan siber juga meningkat, di mana *router* menjadi target utama serangan. Studi terbaru menunjukkan pentingnya desain JSN yang mampu mengirim data dengan cepat dan aman. Teknologi kriptografi, seperti AES, digunakan untuk melindungi transmisi data dari ancaman serangan siber. Penelitian ini bertujuan untuk mengembangkan jaringan sensor dengan menggunakan protokol komunikasi TCP dan UDP, yang memungkinkan transmisi data sensor secara *real-time* dan aman menggunakan algoritma kriptografi AES. Hasil penelitian akan mengevaluasi kinerja jaringan, khususnya terkait kualitas layanan (QoS) dan dampak dari teknik kriptografi yang digunakan. Hasil penelitian menunjukan, *throughput* TCP dengan enkripsi AES tercatat sebesar 21,55 Kbps, sementara tanpa enkripsi mencapai 188,5 Kbps. *Delay* pada TCP dengan enkripsi adalah 60,914 ms, sedangkan tanpa enkripsi mencapai 12,41 ms. *Overhead* dari enkripsi memperkecil *throughput* karena pengolahan tambahan dan kontrol aliran. *Throughput* UDP dengan enkripsi mencapai 322,28 Kbps, dan tanpa enkripsi 476,45 Kbps. *Delay* pada UDP dengan enkripsi tercatat 12,972 ms, sementara tanpa enkripsi adalah 3,5704 ms. Peningkatan *delay* pada kedua protokol disebabkan oleh kebutuhan pengiriman kunci enkripsi. Dalam pengujian 2 dan 3 *client* pada TCP dengan enkripsi, *throughput* masing-masing mencapai 8,7 Kbps dan 11,878 Kbps, dengan *delay* sebesar 125,30 ms untuk 2 *client*, dan 85,96 ms untuk 3 *client*. Pada pengujian UDP dengan enkripsi, *throughput* tercatat sebesar 198,08 Kbps untuk 2 *client*, dan 352,71 Kbps untuk 3 *client*, dengan *delay* masing-masing sebesar 15,661 ms dan 8,104 ms. Kriptografi AES memberikan keunggulan dalam menjaga data

tanpa menyebabkan penurunan performa yang signifikan. Penggunaan kriptografi AES tetap direkomendasikan karena dampak terhadap QoS tidak signifikan, terutama jika menggunakan mekanisme distribusi kunci yang lebih efisien pada protokol UDP yang mampu menghasilkan jumlah *troughput* yang besar dengan *delay* yang sangat kecil sehingga memungkinkan pengiriman data sensor secara *real-time* tetap cepat dan aman.

Kata kunci: *IoT (Internet of Things), kriptografi, QoS (Quality of Service), Advanced Encryption Standard, socket programming*, *TCP (Transmission Control Protocol), UDP (User Datagram Protocol).*

Title	*Design Of Multiple Wireless Sensor Network Using Advanced Encryption Standars Cryptograhy Algorithm*	Muhammad Fauzan Fadhilah
Mayor	*Electrical Engineering Department*	1910952036
Engineering Faculty of Andalas University		

Abstract

Indonesia has experienced a significant increase in technological development Internet of Things (IoT) in recent years. IoT allows devices with sensors to communicate and exchange data over the internet, playing an important role in supporting the industrial revolution 4.0. One of the main components of IoT is Wireless Sensor Networks (WSN), which enable data collection and transmission without the physical limitations of cables. However, with the increase in IoT applications, cyber attacks have also increased, with routers becoming the main target of attacks. Recent studies show the importance of WSN designs that are capable of sending data quickly and securely. Cryptographic technologies, such as AES, are used to protect data transmission from the threat of cyber attacks. This research aims to develop a sensor network using TCP and UDP communication protocols, which allows the transmission of sensor data real-time and safe using the AES cryptographic algorithm. The research results will evaluate network performance, especially regarding quality of service (QoS) and the impact of the cryptographic techniques used. The research results show, throughput TCP with AES encryption was recorded at 21.55 Kbps, while without encryption it reached 188.5 Kbps. Delay on TCP with encryption it is 60.914 ms, while without encryption it reaches 12.41 ms. Overhead of encryption minimizes throughput due to additional processing and flow control. UDP throughput with encryption reaches 322.28 Kbps, and without encryption 476.45 Kbps. Delay on UDP with encryption it was recorded at 12.972 ms, while without encryption it was 3.5704 ms. Improvement delay in both protocols is due to the need to transmit the encryption key. In tests 2 and 3 client on TCP with encryption, throughput respectively reaching 8.7 Kbps and 11.878 Kbps, with delay of 125.30 ms for 2 client, and 85.96 ms for 3 client. In testing UDP with encryption, throughput recorded at 198.08 Kbps for 2 client, and 352.71 Kbps for 3 client, with delay respectively 15.661 ms and 8.104 ms. AES cryptography provides superior security data without causing significant performance degradation. The use of AES cryptography is still recommended because the impact on QoS is not

significant, especially if using a more efficient key distribution mechanism on the UDP protocol that is capable of generating large numbers of troughput the big one with delay which is so small that it allows sending sensor data directly real-time stay fast and safe

Key Words: *IoT (Internet of Things), kriptografi, QoS (Quality of Service), Advanced Encryption Standard, socket programming*, *TCP (Transmission Control Protocol), UDP (User Datagram Protocol).*