

ANALISIS UNJUK KERJA PROSES KRIPTOGRAFI INTERNET PROTOCOL PADA WIRELESS SENSOR

LAPORAN PENELITIAN

*Sebagai Salah Satu Syarat untuk Menyelesaikan Program Profesi pada Program
Studi Pendidikan Profesi Insinyur Program Pascasarjana Universitas Andalas*



**PROGRAM STUDI PENDIDIKAN PROFESI INSINYUR
SEKOLAH PASCASARJANA
UNIVERSITAS ANDALAS
PADANG
2024**

ABSTRAK

Perkembangan teknologi komunikasi pada aplikasi *Internet of Things* (IoT) yang digunakan pada setiap lini kehidupan mempermudah kehidupan dengan otomatisasinya. Perkembangan teknologi komunikasi sejalan dengan ancaman pada komunikasi data yang terjadi pada IoT. Salah satu langkah antisipasi serangan pada komunikasi data adalah menggunakan kriptografi. Kriptografi berperan untuk mengamankan data yang dikirim pada komunikasi data, sehingga apabila data diperoleh oleh pihak ketiga, data yang diperoleh akan berupa data hasil enkripsi. Proses kriptografi menggunakan langkah ekstra untuk mengamankan data dan dapat berpengaruh pada *Quality of Service* (QoS) jaringan. Hasil penelitian ini memperlihatkan pengaruh 2 jenis kriptografi yang paling di umum digunakan yaitu *Rivest-Shamir-Adleman* (RSA) dan *Advanced Encryption Standard* (AES). Kriptografi AES yang lebih sederhana dengan maksimal pengkodean 254 bit terbukti memiliki delay transmisi yang lebih kecil yaitu sebesar 3,02 ms dibanding dengan RSA yang melibatkan pengkodean 2048 bit dan lebih kompleks proses komputasinya. Throughput yang lebih besar pada transmisi menggunakan protocol *User Datagram Protocol* (UDP) pada AES yaitu sebesar 250,93 Kbps terbukti jumlah data sensor lebih banyak dapat dikirimkan karena protocol UDP yang lebih sederhana dibanding *Transmission Control Protocol* (TCP). Penggunaan AES dengan protocol UDP lebih direkomendasikan untuk digunakan untuk memproteksi data dalam transmisi Jaringan Sensor Nirkabel (JSN).

Kata Kunci: TCP, UDP, AES, RSA, JSN



ABSTRACT

The development of communication technology in Internet of Things (IoT) applications used in every line of life makes life easier with automation. The development of communication technology is in line with the threats to data communication that occur in IoT. One of the steps to anticipate attacks on data communication is using cryptography. Cryptography plays a role in securing the data sent in data communications so that if a third party obtains the data, the data obtained will be in the form of encrypted data. The cryptography process uses extra steps to secure the data and can affect the Quality of Service (QoS) of the network. The results of this study show the effect of the two most commonly used cryptography types, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). The simpler AES cryptography, with a maximum encoding of 254 bits, proved to have a smaller transmission delay of 12.96 ms compared to RSA, which involves encoding 2048 bits and is more complex to compute. The greater throughput in transmission using the User Datagram Protocol (UDP) protocol on AES, which is 250.93 Kbps, proves that more sensor data can be sent because the UDP protocol is simpler than Transmission Control Protocol (TCP). The use of AES with UDP protocol is more recommended to protect data in Wireless Sensor Network (WSN) transmission.

Keywords: TCP, UDP, RSA, AES, WSN

