ABSTRAK

RAVELIANA. Analisis Keamanan Transmisi Data Menggunakan Algoritma PRESENT pada Sistem Monitoring PM2.5 Berbasis IoT. Dibimbing oleh HENDRA KURNIAWAN dan BERTA ERWIN SLAM.

Sistem monitoring PM2.5 berbasis *Internet of Things* (IoT) membutuhkan mekanisme keamanan data karena informasi sensor dikirim melalui komunikasi nirkabel dan berpotensi mengalami penyadapan maupun manipulasi. Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi ringan PRESENT-80 mode *Counter* (CTR) pada sistem monitoring PM2.5 berbasis IoT serta menganalisis efektivitasnya dalam menjaga kerahasiaan data dan mengidentifikasi indikasi manipulasi data melalui validasi hasil dekripsi pada sisi *receiver/gateway*. Sistem yang dibangun terdiri atas *node sensor* berbasis ESP32-S3, sensor PMS5003, modul LoRa SX1262, *receiver/gateway* ESP32, server web Laravel, dan *database* MySQL. Data sensor dibentuk dalam format JSON, kemudian dienkripsi pada *node sensor* sebelum dikirim melalui LoRa. Data terenkripsi diterima oleh *receiver/gateway*, didekripsi, lalu dikirim ke server web untuk disimpan dan ditampilkan pada *dashboard monitoring*. Pengujian dilakukan melalui pengujian fungsional, pengujian performa, pengujian *sniffing*, dan simulasi *Man-in-the-Middle* (MitM). Hasil pengujian menunjukkan bahwa seluruh fungsi sistem berjalan dengan baik. Rata-rata waktu enkripsi sebesar 21,20 ms, rata-rata waktu dekripsi sebesar 21,36 ms, dan rata-rata latensi transmisi sebesar 240,3 ms. Data yang dikirim tidak dapat dibaca secara langsung karena berada dalam bentuk *ciphertext*, sedangkan pada pengujian simulasi *Man-in-the-Middle (MitM)*, indikasi manipulasi data berhasil dikenali melalui validasi hasil dekripsi yang menampilkan status *SUSPECT_MODIFIED*, sehingga mekanisme ini tidak mengganggu alur pengambilan data secara normal. Dengan demikian, algoritma *PRESENT-80* mode CTR dapat diterapkan sebagai solusi keamanan ringan yang efisien untuk menjaga kerahasiaan transmisi data pada sistem monitoring PM2.5 berbasis IoT.

Kata kunci*: Internet of Things*, LoRa, PM2.5, *PRESENT*, transmisi data.

ABSTRACT

RAVELIANA. Security Analysis of Data Transmission Using the PRESENT Algorithm in an IoT-Based PM2.5 Monitoring System. Supervised by HENDRA KURNIAWAN and BERTA ERWIN SLAM.

An *Internet of Things* (IoT)-based PM2.5 monitoring system requires a data security mechanism because sensor information is transmitted through wireless communication and may be exposed to eavesdropping or manipulation. This research aims to implement the lightweight PRESENT-80 cryptographic algorithm in *Counter* (CTR) mode in an IoT-based PM2.5 monitoring system and to analyze its effectiveness in maintaining data confidentiality and identifying indications of data manipulation through decryption result validation on the receiver/gateway side. The developed system consists of an ESP32-S3 sensor node, PMS5003 sensor, SX1262 LoRa module, ESP32 receiver/gateway, Laravel web server, and MySQL database. Sensor data are formatted as JSON and encrypted at the sensor node before being transmitted through LoRa. The encrypted data are received by the receiver/gateway, decrypted, and then sent to the web server to be stored and displayed on the monitoring dashboard. The tests included functional testing, performance testing, sniffing testing, and *Man-in-the-Middle* (MitM) simulation. The results show that all system functions operated properly. The average encryption time was 21.20 ms, the average decryption time was 21.36 ms, and the average transmission latency was 240.3 ms. The transmitted data could not be read directly because they were in ciphertext form, while during the MitM simulation testing, indications of data manipulation were successfully identified through decryption result validation displaying the SUSPECT_MODIFIED status, without affecting the normal data acquisition flow. Therefore, PRESENT-80 in CTR mode can be applied as an efficient lightweight security solution to maintain the confidentiality of data transmission in an IoT-based PM2.5 monitoring system.

Keywords: data transmission, Internet of Things, LoRa, PM2.5, PRESENT.