

ABSTRAK

Seiringnya perkembangan zaman, bidang teknologi *Internet of Things* (IoT) semakin maju terutama di bidang pengiriman dan penyimpanan data. Tetapi siapa yang menduga jika ternyata dibalik kemajuan teknologi yang pesat menyimpan ketakutan terhadap pencurian data. Adapun solusi untuk mengatasi pencurian data tersebut sistem seharusnya memakai Kriptografi. Kriptografi dapat meminimalisir pencurian data agar tidak disalahgunakan. Pada penelitian tugas akhir ini akan dirancang suatu sistem yang dapat menjaga keamanan pada proses pengiriman data IoT melalui protokol MQTT penyimpanan data pada PHP *MyAdmin* dengan Metode RSA.

Data sensor yang digunakan menggunakan sensor ultrasonik HC-SR04 yang diaplikasikan didalam mikrokomputer Raspberry Pi 4. Data sensor yang masuk kedalam sistem secara otomatis diubah menjadi *chipertext* menggunakan metode RSA dengan dua skenario yaitu RSA 1024 bit dan 2048 bit. Setelah itu data akan dikirimkan melalui MQTT menuju *database* PHP *MyAdmin*. Didalam *database* data yang berbentuk *chipertext* secara otomatis akan di dekripsi.

Berdasarkan hasil pengujian sistem, diketahui bahwa sistem dapat melakukan enkripsi pada data sensor dan dapat mengirimkan data dalam bentuk *chipertext* melalui MQTT menuju *database*. Nilai rata-rata *response times* untuk skenario RSA 1024 bit sebesar 879,4 ms untuk proses enkripsi dan 2189,83 ms untuk proses dekripsi. Untuk skenario RSA 2048 bit didapatkan hasil rata-rata pengujian *Response Times* untuk 10, 20, dan 30 data sebesar 2.859,27 ms untuk proses enkripsi dan 228.060,91 ms untuk proses dekripsi. Proses pengiriman data dari sensor menuju *database* menunjukkan bahwa QoS pada sistem yang telah dibuat termasuk kategori baik dengan masing-masing nilai rata-rata untuk skenario RSA 1024 bit dan RSA 2048 bit yaitu *throughput* 6932,04 Kb/s dan 6167,03 Kb/s, *packet loss* sebesar 0% serta *delay* sebesar 243,3 ms dan 589,5 ms.

Kata Kunci : RSA, *Internet of Things*, Sistem Keamanan, Enkripsi, Dekripsi, MQTT.