ABSTRACT

Checking checking body temperature is part of medical checkup to find out the condition of our bodies. but to do a medical checkup during the COVID-19 pandemic is very dangerous. Therefore, this final project disscuss about telemedicine system to facilitate communication between doctors and patients more efficient. By using the telemedicine system, of course the health data from patients will go through the internet network, and that requires a system that ensure the safety of those data.

The telemedicine system for monitoring body temperature uses MLX90614 infrared sensor. For data communication in this telemedicine system uses Diffie-Hellman key exchange algorithm and AES encryption to ensure the safety of patient data. Body temperature data will be taken from the patient's forehead and encrypted by the ESP32 microcontroller. The encrypted data will be sent to cloud servers and applications for further analysis.

The result of comparison between device and thermometer gun show that the RSME of telemedicine system is 0.305%. The average delay of AES 128-bit and 256-bit encryptions are 201.39 μs and 243.5 μs respectively with the average delay from ESP32 to the cloud server using 128 bit and 256 bit key length are 95.995 ms and 113.02 ms. Whereas for average delay from ESP32 to application via BLE network using 128 bit and 256 bit key length are 500 ms and 505 ms. The throughput result via Wi-Fi network using 128 bit and 256 bit key length are 3579 bit/s and 4846 bit/s. Whereas for throughput result via BLE network using 128 bit and 256 bit key length are 7819 bit/s and 7548 bit/s. For packet loss that is obtained either on the Wi-Fi or BLE network are 0%. The average uptime produced by a device with a 400 mAh battery capacity is 16200 seconds.

***Keywords**: Monitoring, Body Temperature, Telemedicine, AES, ESP32, wearable device, Diffie-Hellman, MLX90614 Sensor*