PERANCANGAN DAN IMPLEMENTASI SMART WEIGHT SCALE MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) DALAM SISTEM TELEMEDICINE

DESIGN AND IMPLEMENTATION OF SMART WEIGHT SCALE USING AES ALGORITHM IN TELEMEDICINE SYSTEM

Dwi Sulistyowati[1], Favian Dewanta, Ph.D.[2], Sussi, S,Si., M.T.[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi Fakultas Teknik Elektro, Universitas Telkom
[1]**dwisulistyowati@student.telkomuniversity.ac.id**, [2]**favian@telkomuniversity.ac.id**,
[3]**sussiss@telkomuniversity.ac.id**

Abstrak

Tubuh sehat dengan berat badan yang ideal adalah harapan semua orang. Berat yang ideal menunjang penampilan fisik serta berhubungan dengan kesehatan seseorang. Selama masa pandemi COVID 19 masyarakat dituntut tetap menjaga kesehatan, tetapi terbatas melakukan pemeriksaan ke rumah sakit. Sistem *telemedicine* dengan memanfaatkan teknologi informasi dan komunikasi (TIK) memberikan kemudahan dalam pertukaran informasi medis untuk pemantauan, diagnosis dan pencegahan penyakit secara dini. Sehingga kesehatan masyarakat tetap terpantau dan masih mendapatkan layanan kesehatan dari jarak jauh. Riset ini merancang dan mengimplementasikan *smart weight scale* dengan algoritma enkripsi *Advanced Encryption Standard* (AES) dalam sistem *telemedicine*. Hasil pengukuran berat badan yang diperoleh dari *load cell* akan diproses dan dienkripsi oleh Mikrokontroler ESP32, serta dapat ditampilkan pada TFT ILI 9255 dan aplikasi android kemudian disimpan ke dalam *cloud server* sebagai rekam data berat badan pengguna. Sistem yang telah dirancang memiliki tingkat akurasi alat sebesar 99,74%. Data dikirim secara *realtime* ke aplikasi dan pengiriman ke *server* merupakan data yang telah ter-enkripsi menggunakan algoritma AES 256 bit mode CBC yang terkode dengan algoritma Base64. Berdasarkan pengujian *Quality of Service* (QoS) dengan parameter *delay* dan *throughput* pengiriman menggunakan *Bluetooth* lebih kecil dibanding Wi-Fi. Nilai *delay* rata-rata dan *throughput* sebesar 88.522 ms dan 1.532 bits/s untuk pengiriman *Bluetooth* ke aplikasi sedangkan 323.980 ms dan 7.819 bits/s untuk pengiriman Wi-Fi ke *server*.

Kata kunci : *telemedicine*, berat badan, *smart weight scale*, ESP32, AES

Abstract

A healthy body with an ideal weight is everyone's desire. The ideal weight supports physical appearance and is related to one's health. During the COVID 19 pandemic, people are required to maintain their health, but are restricted to conducting examinations at the hospital. The telemedicine system utilizing information and communication technology (ICT) makes it easy to exchange medical information for early monitoring, diagnosis and prevention of diseases. As a consequence, public health remains monitored and still get health services remotely. This research designs and implements a smart weight scale with the Advanced Encryption Standard (AES) encryption algorithm in the telemedicine system. The results of weight measurement obtained from the load cell will be processed and encrypted by the ESP32 Microcontroller, and can be displayed on the ILI9255 TFT and the android application. Eventually, the result is stored into the server as a user weight data record. The system has an accuracy rate of 99.74 %. Data sent in real time to the application server are encrypted using the AES-CBC algorithm, which is coded with the Base64 algorithm. Based on Quality of Service (QoS) examinations with parameters of delay and throughput, the transmission delay of Bluetooth Low Energy (BLE) is smaller than Wi-Fi, in which average values of delay and throughput of BLE between the device and mobile application are 88,522 ms and 297 bits/s, meanwhile in the Wi-Fi case between the device with the server, the average delay and throughput are 323,980 ms and 3514 bits/s.

Keywords: telemedicine, weight, smart weight Scale, ESP32, AES.

1. Pendahuluan

Perkembangan berat badan menentukan kondisi tubuh seseorang. Selama masa pandemi, penerapan isolasi mandiri dan sosial *distancing* yang meningkatkan prevalensi obesitas global yang disebabkan berkurangnya aktivitas fisik total karena keterbatasan aktivitas di luar ruangan, peningkatan konsumsi makan akibat stres atau kebosanan [1]. Karena itu, diperlukan sebuah sistem yang dapat digunakan untuk melakukan pemeriksaan, dan pemantauan berat badan agar kesehatan tubuh terjaga.

Pemeriksaan kesehatan secara rutin penting dilakukan untuk mengetahui kondisi kesehatan serta mendeteksi suatu penyakit sejak dini [2]. Pemeriksaan kesehatan dapat dilakukan di rumah sakit dengan bantuan petugas kesehatan akan tetapi pada masa pandemi COVID-19 para pasien disarankan untuk tidak datang ke rumah sakit, kecuali ada kebutuhan darurat. Oleh karena itu pengembangan sistem *telemedicine* dapat menjadi solusi untuk pemantauan, pemeriksaan, konsultasi serta evaluasi kesehatan tanpa terhalang waktu dan tempat. Sistem *telemedicine* memanfaatkan perkembangan teknologi *Internet of Things* (IoT) yang digabungkan dengan kepakaran medis mampu terintegrasi dengan peralatan medis untuk pertukaran data antara peralatan dengan aplikasi serta menyimpan hasil pemeriksaan secara *realtime* sebagai rekam medis pengguna.

Berdasarkan permasalahan yang ada, pada Tugas Akhir ini penulis akan merancang dan mengimplementasikan *smart weight scale* pada sistem *telemedicine* untuk pemantauan berat badan menggunakan *load cell* sebagai sensor berat dan mikrokontroler ESP32 untuk memproses data serta mengaktifkan modul *Bluetooth Low Energy (BLE)* dan Wi-Fi untuk komunikasi dengan aplikasi dan *server*. Karena data kesehatan itu bersifat penting dan rahasia, penulis juga mengimplementasikan algoritma enkripsi *Advanced Encryption Standard* (AES) untuk mengamankan lalu lintas jaringan selama pertukaran data. Harapannya dengan ada sistem *telemedicine* ini, pengguna dapat rutin melakukan pemeriksaan dan pemeliharaan kesehatan sendiri dengan aman serta mendapatkan pelayanan kesehatan berdasarkan rekam medis yang tersimpan.

2. Dasar Teori

2.2 Berat Badan

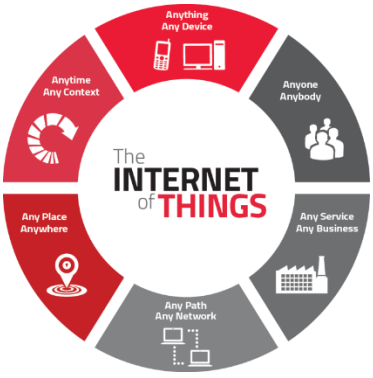
Berat badan merupakan salah satu parameter kesehatan secara fisik yang sering diperiksa saat melakukan pemeriksaan kesehatan untuk menggambarkan massa tubuh seseorang dengan satuan Kg. Tubuh sehat dengan berat badan yang ideal adalah harapan semua orang. Orang yang memiliki berat badan yang berlebih beresiko terkena penyakit seperti: obesitas, tekanan darah tinggi, diabetes, kadar kolesterol tinggi dan sakit jantung. Sedangkan orang yang memiliki berat badan kurang dapat disebabkan karena kekurangan gizi dalam tubuh. Pada penelitian ini, berat badan akan diukur menggunakan *smart weight scale* yang dirancang untuk memantau perkembangan berat badan[3].

2.2 Definisi *Telemedicine*

Telemedicine adalah pelayanan kesehatan secara jarak jauh. Sistem *telemedicine* memberikan solusi bantuan medis dengan kemudahan pemantauan kesehatan, melakukan konsultasi, pertukaran data medis dan diskusi ilmiah tanpa terkendala letak geografis. Sistem ini mencakup berbagai aplikasi dan layanan dengan memanfaatkan komunikasi audio, visual maupun pertukaran data. Sistem *telemedicine* dapat diakses kapanpun dan dimanapun sehingga pengguna dan tenaga medis dapat lebih fleksibel dan efektif tanpa terkendala waktu dan letak geografis [4].

2.2 *Internet of Thing*

Internet of Things (IoT) adalah konsep sebuah infrastruktur jaringan secara global, yang digunakan untuk melakukan komunikasi antara manusia dan antar perangkat pintar yang dihubungkan dengan internet. Perangkat pintar dapat saling berbagi informasi berdasarkan protokol yang sudah ditetapkan untuk melacak, mengamankan data bahkan untuk pemantauan secara online [5]. Dengan menggunakan konsep jaringan IoT semua data dari perangkat dapat disimpan untuk pemantauan kesehatan pasien secara rutin dari jarak jauh agar data hasil pemeriksaan dapat dianalisis untuk pengambilan keputusan oleh petugas kesehatan.



Gambar 1. *Internet of Things*[5].

2.3 *Load Cell*

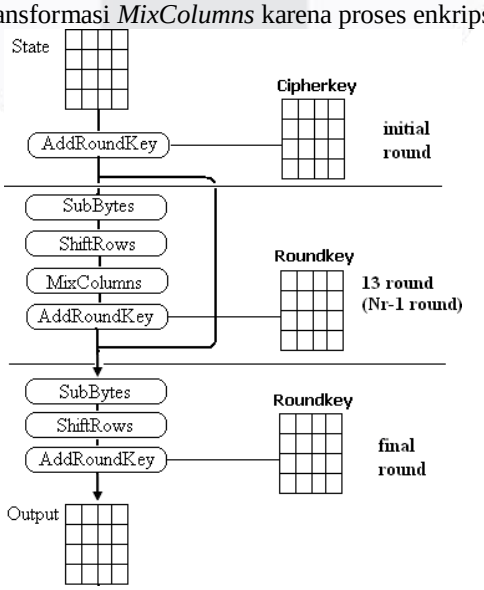
Load cell adalah sensor yang bekerja secara mekanis untuk mendeteksi perubahan tekanan atau berat suatu benda. *Load cell* terdiri dari konduktor *Strain Gauge* sebagai pengindera (sensor) dan Jembatan *Wheatstone*. *Strain gauge* termasuk transduser pasif diberikan pada suatu logam maka dari logam tadi akan menghasilkan perubahan resistansi yang nilainya sebanding dengan bentuk perubahannya. Perubahan ini kemudian diukur dengan konsep Jembatan *Wheatstone* untuk menentukan referensi nilai keluaran yang diterima *load cell*[6].

2.2 Mikrokontroler ESP32

ESP32 merupakan sebuah *board* mikrokontroler 32bit yang sudah dilengkapi dengan modul Wi-Fi dengan jaringan wifi 802.11b/g/n, *Bluetooth* V4.2 yang bekerja pada frekuensi 2.4 GHz dan *Bluetooth* Low Energy (BLE) sehingga mendukung untuk membuat sistem *Internet of Things*. ESP32 memiliki 18 pin ADC (*Analog Digital Converter*), 2 DAC, 16 PWM, 10 Sensor sentuh, 2 jalur antarmuka UART serta mendukung antarmuka dengan pin I2C, I2S, dan SPI [7].

2.2 *Advanced Encryption Standard* (AES)

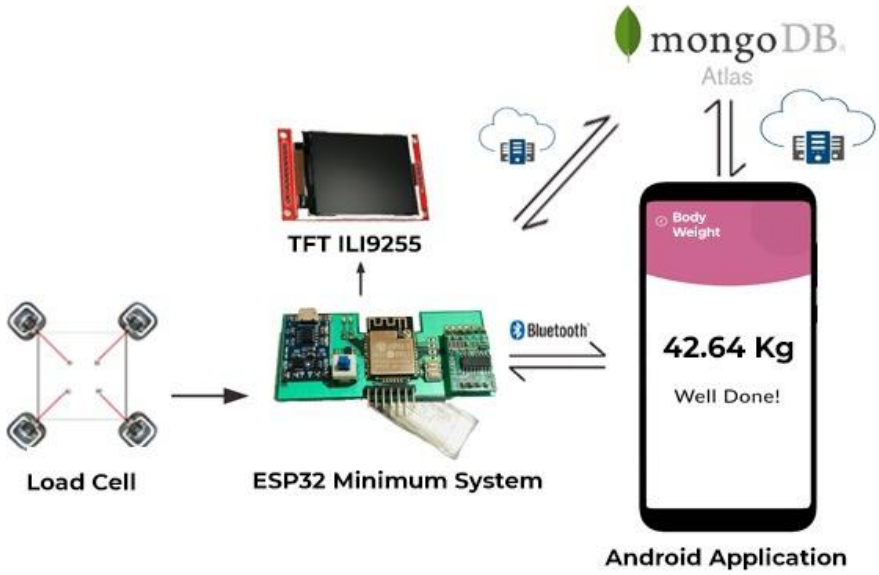
AES merupakan algoritma kriptografi simetris dengan kunci yang sama untuk setiap enkripsi. Algoritma ini bertipe *block cipher* dengan panjang blok 128 bit. Dalam proses pengiriman data terdapat *plaintext* yang merupakan pesan awal yang belum dienkripsi dan *ciphertext* merupakan pesan yang sudah terenkripsi. AES memiliki tiga tipe pilihan kunci yang berbeda yaitu AES-128 bit, AES-192 bit dan AES-256 bit dan masing – masing memiliki spesifikasi panjang blok 128-bit. Setiap tipe kunci menggunakan kunci internal (*round key*) yang berbeda untuk setiap putaran. AES terdiri dari empat proses transformasi *bytes*. Pertama *plaintext* disalin ke dalam *state* selanjutnya mengalami transformasi *bytes AddRoundKey*, *SubBytes*, *ShiftRows* dan *MixColumns*. Proses ini disebut *round function* yang dilakukan secara berulang-ulang sebanyak *Nr*. Pada putaran terakhir *state* tidak tidak mengalami transformasi *MixColumns* karena proses enkripsi telah selesai[8].



Gambar 2. Diagram Proses *Round Function* AES [8].

3. Pembahasan

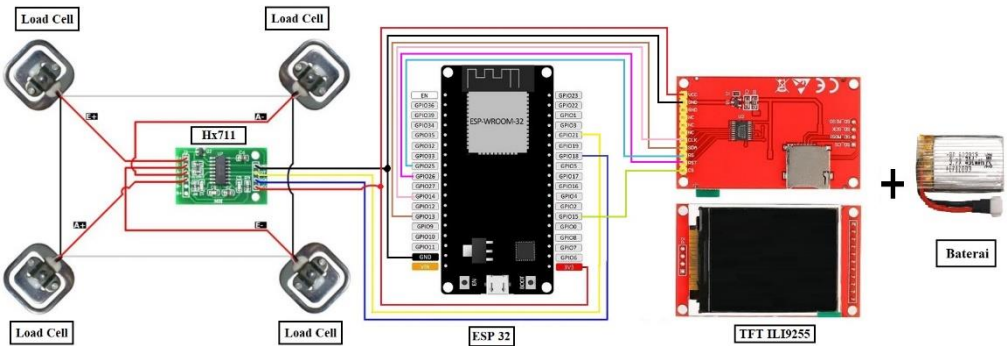
3.1. Desain Sistem



Gambar 3. Diagram Sistem *Telemedicine*.

Gambar 3 menjelaskan bahwa sistem *telemedicine* pemantauan berat badan terdiri tiga bagian utama. Bagian pertama adalah perangkat keras untuk memproses data yang terdiri dari sensor *load cell, ESP32 minimum system*, dan TFT ILI9255. Bagian ini berfungsi untuk mengukur berat badan pengguna, mengaktifkan *BLE* dan modul Wi-Fi sebagai protokol komunikasi antar perangkat keras dengan aplikasi dan *server* serta melakukan proses enkripsi. Bagian kedua adalah *software* aplikasi android berfungsi menampilkan data dari mikrokontroler. Terakhir adalah bagian *cloud server* yang berfungsi untuk menyimpan data rekam medis dari hasil pengukuran. Pada penelitian ini, Penulis berfokus kepada bagian perancangan dan implementasi perangkat keras pada sistem *telemedicine*.

3.2. Desain Perangkat Keras

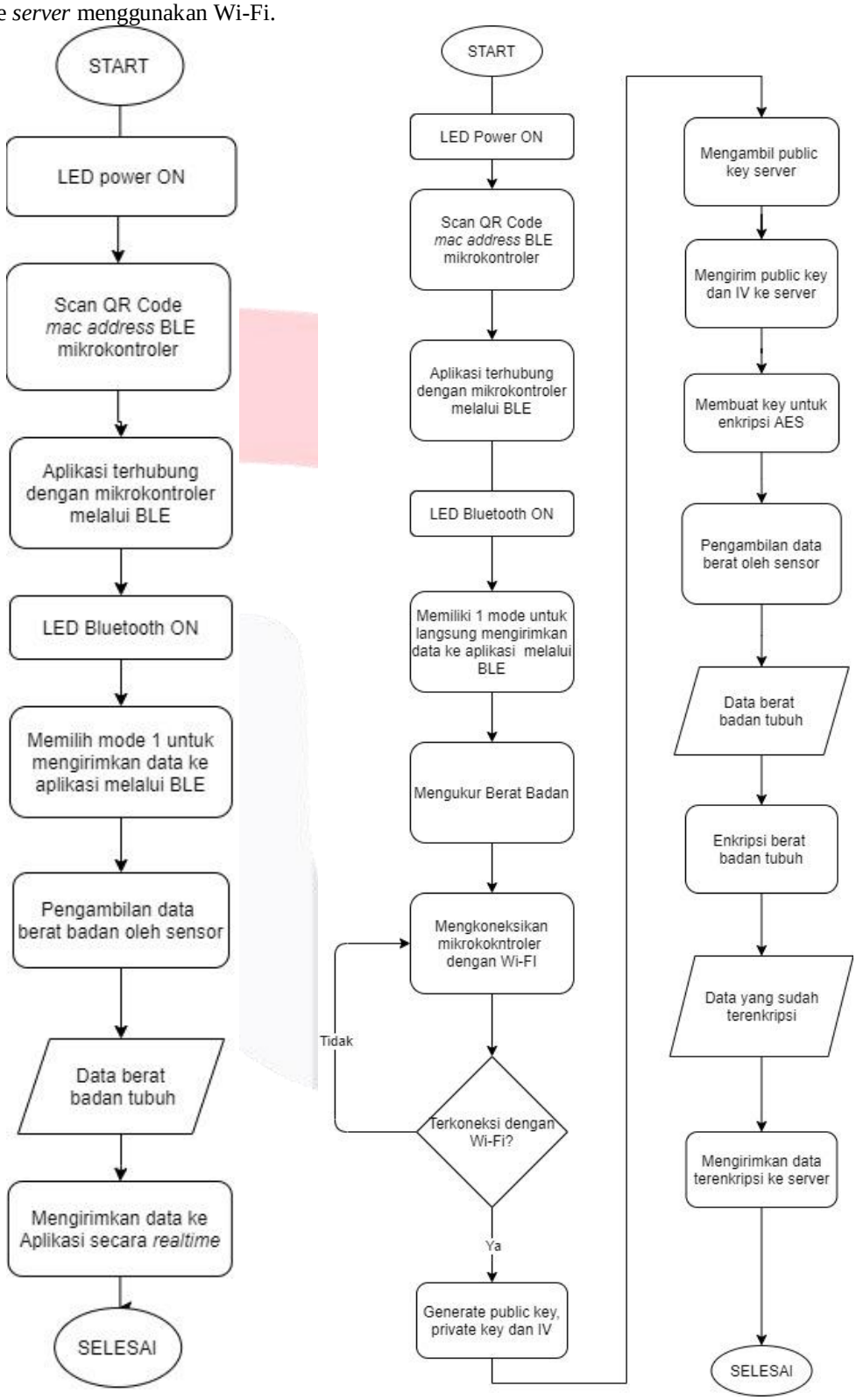


Gambar 4. Desain Perangkat Keras.

Desain perangkat keras terdiri dari empat sensor l*oad cell half bridge 50 kg* yang disusun ke dalam konfigurasi Jembatan *Wheatstone* sesuai dengan Gambar 4. Rangkaian sensor berat terhubung dengan modul HX711 untuk mengkonversi perubahan resistansi menjadi besaran tegangan. Rangkaian sensor dihubungkan dengan mikrokontroler ESP32 Minimum System yang telah terhubung dengan baterai Li-Po untuk menampilkan hasil pengukuran pada LCD TFT ILI 9255, proses enkripsi AES dan pengiriman data ke aplikasi dan *server*.

3.2. Diagram Aliran Pengiriman Data

Pada penelitian ini, Penulis membuat dua skema aliran pengiriman data. Mode satu mengirimkan data dari mikrokontroler ke aplikasi menggunakan *BLE* dan mode dua mengirimkan data ke *server* menggunakan Wi-Fi.



Gambar 5. Diagram Aliran Pengiriman Data (a) Mode 1 dan (b) Mode 2.

3.3 Skenario Pengujian

Pengujian sistem dilakukan untuk mengetahui performansi sistem. Adapun skenario pengujian sistem sebagai berikut:

1. Rancangan Alat
   Pengujian dilakukan dengan mengaktifkan timbangan dan melakukan pengukuran berat badan untuk mengetahui apakah setiap komponen dapat bekerja sesuai dengan fungsinya.
2. Akurasi Alat
   Pengujian akurasi timbangan digital, dilakukan perbandingan antara data hasil pengukuran timbangan digital rancangan (A) dengan data aktual dari timbangan digital asli (B). Kemudian dilakukan perhitungan *Root Mean Squared Error* (RMSE) untuk menentukan besar *error* pengukuran untuk mendapatkan nilai akurasi alat. Untuk persamaan RMSE dan akurasi alat dapat dilihat pada persamaan (1) dan (2).

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(A-B)^2}{n}} \quad (1)$$

$$Akurasi = 100\% - RMSE \quad (2)$$

3. Kecepatan Proses Data
   Pengujian dilakukan dengan mengirim data menggunakan kunci 128 bit dan 256 bit serta memproses program berdasarkan fungsinya dengan menambahkan fungsi *micros ()* pada setiap program yang ingin diukur dalam satuan mikrodetik.
4. Konsumsi Daya
   Pengujian dilakukan dengan dua skema, pertama menyalakan timbangan tanpa mengirimkan data dan yang kedua menyalakan timbangan dengan melakukan pengiriman data dari baterai terisi penuh hingga daya dari baterai habis.
5. Lalu Lintas Data
   Pengujian lalu lintas data dilakukan untuk mengetahui apakah enkripsi AES telah berhasil diimplementasikan proses pengiriman data.
6. *Quality of Service*
   Pengujian *Quality of Service (QoS)* dilakukan untuk menganalisa performansi jaringan pada sistem dengan parameter yang diukur adalah *delay* dan *throughput* menggunakan bantuan *software* Wireshark versi 3.4.2.

4 Hasil Pengujian

Berikut hasil pengujian yang telah dilakukan untuk mengetahui performasi dari sistem yang telah dirancang.

1. Hasil Rancangan Alat

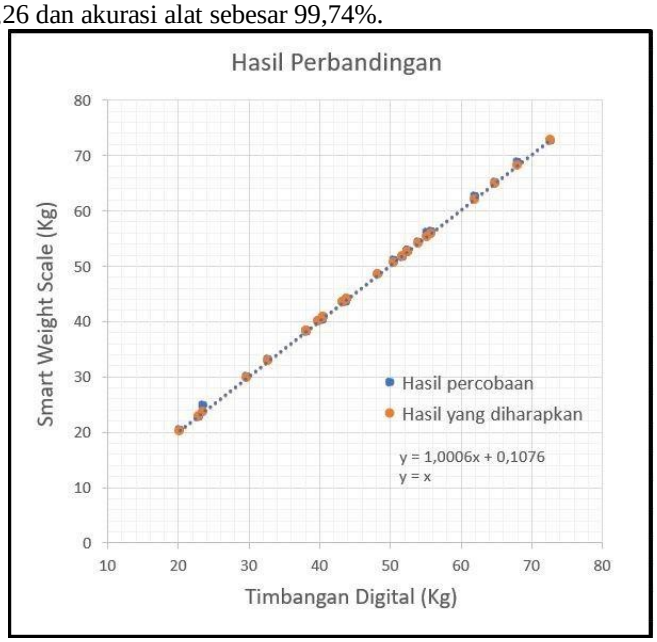
(a) (b)

Gambar 6 (a) Bagian Dalam Alat (b) Pengujian Alat.

Alat 100% telah sesuai dengan perancangan dan hasil perancangan bagian dalam dapat dilihat pada Gambar 6 (a). Setiap komponen mampu bekerja, ditandai dapat digunakan untuk mengukur berat badan serta menampilkan hasil pengukuran pada layar LCD terlihat pada Gambar 6 (b).

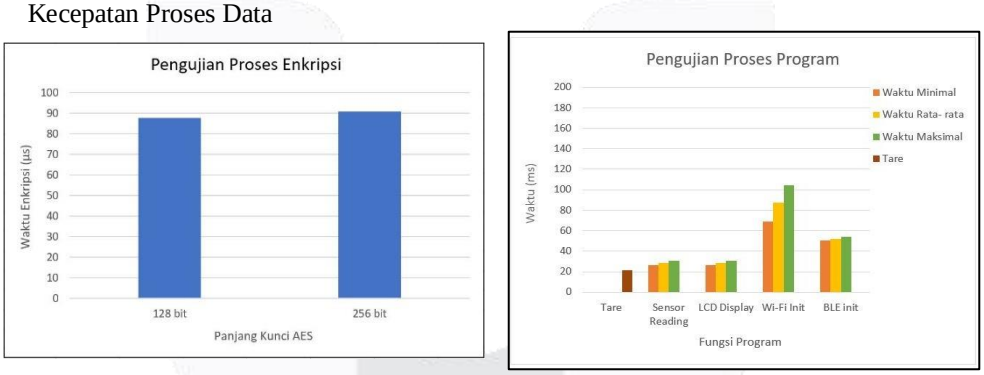
2. Akurasi Alat

Setelah dilakukan pengujian dengan mengukur berat badan 30 orang diperoleh nilai RMSE sebesar 0,26 dan akurasi alat sebesar 99,74%.



Gambar 7. Hasil Pengujian Akurasi Alat.

3. Kecepatan Proses Data



(a) (b)

Gambar 8. Kecepatan Proses Data (a) Enkripsi (b) Proses Program.

Pengujian kecepatan proses enkripsi diperoleh waktu 87,68 µs untuk panjang kunci 128 bit dan 90,64 µs untuk panjang kunci 256 bit. Semakin besar kunci maka semakin banyak *round key* sehingga waktu enkripsi juga semakin lama. Gambar 8 (b) menunjukan bahwa proses Wi-Fi init dan BLE init membutuhkan waktu lebih lama dengan waktu rata rata 87.31 ms dan 52.17 ms karena dipengaruhi oleh jaringan yang digunakan. Sedangkan proses Tare, Sensor Reading dan LCD Display lebih cepat karena tidak dipengaruhi oleh kualitas jaringan dan diperoleh waktu 21.32 ms 28.51 ms dan 28.52 ms.

4. Konsumsi Daya

Tabel 1. Hasil Pengujian Konsumsi Daya

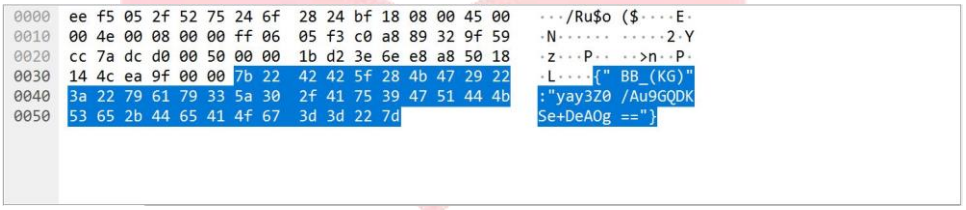
Percobaan	**Keadaan**	***Uptime* (sekon)**	***Downtime* (sekon)**
1	Hidup tanpa mengirim data	14.400	5.400
2	Hidup dengan mengirim data	9.000	5.400

Sistem memberikan tegangan untuk mikrokontroler, LCD dan HX711 saat pengujian tanpa mengirimkan data. Jika sistem hidup serta mengirimkan data, baterai juga memberikan tegangan untuk proses koneksi *BLE* dan Wi-Fi serta proses enkripsi AES. Sistem akan bekerja lebih lama jika tanpa mengirimkan data.

5. Lalu Lintas Data

Gambar 9. Data Sebelum Enkripsi AES

Gambar 9 menunjukan hasil pemantauan lalu lintas data tanpa menggunakan enkripsi AES sehingga hasil pengukuran langsung terlihat saat dikirimkan sebesar 0,94.



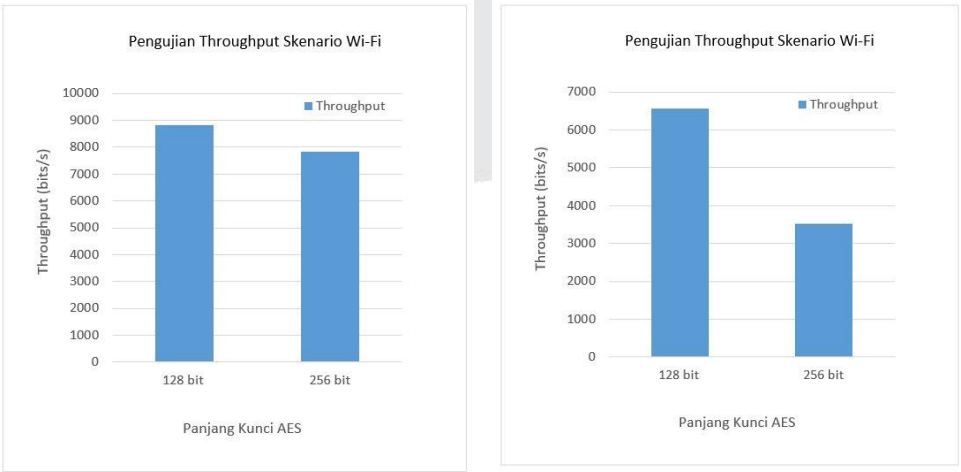
Gambar 10. Data Setelah Enkripsi AES

Gambar 10 menunjukan bahwa data dikirimkan dalam bentuk pengkodean oleh Base64 yaitu ”yay3z0/Au9GQDKSe+DeAOg==” dan algoritma AES telah berhasil diimplementasikan pada sistem *telemedicine*.

6. *Quality of Service*

Gambar 11. *Delay* (a) Skenario *Bluetooth* dan (b) Skenario Wi-Fi.

Pada pengujian *delay* skenario *Bluetooth* panjang kunci 128 bit dan 256 bit memiliki *delay* rata-rata sebesar 85.428 ms dan 88.522 ms. Sedangkan untuk skenario Wi-Fi diperoleh 311.173 ms dan 323.980 ms. Nilai *delay* untuk setiap kunci tidak terlalu jauh karena panjang kunci tidak mempengaruhi proses pengiriman data. Perubahan nilai *delay* dipengaruhi oleh jaringan yang digunakan. Menggunakan *BLE*, data akan langsung dikirim ke aplikasi sehingga lebih cepat dibandingkan dengan menggunakan Wi-Fi ke *server* yang dipengaruhi oleh kualitas dan kecepatan internet yang digunakan.



(a) (b)

Gambar 12. *Throughput* (a) Skenario *Bluetooth* dan (b) Skenario Wi-Fi.

Pada pengujian *throughput* skenario *Bluetooth* dengan panjang kunci 128 bit dan 256 bit diperoleh nilai sebesar 2.074 bits/s dan 1.532 bits/s. Sedangkan untuk skenario Wi-Fi diperoleh 8.832 bits/s dan 7.819 bits/s. Menggunakan skenario Wi-Fi memiliki nilai *throughput* yang lebih besar dibandingkan menggunakan *Bluetooth*. Hal tersebut karena saat pengujian, data yang dikirim melalui Wi-Fi lebih banyak dibandingkan dengan data yang dikirim menggunakan *BLE*. Nilai *throughput* dapat berubah setiap saat tergantung dengan besar jumlah data yang berhasil dikirim oleh mikokontroler persatuan waktu. Semakin banyak data yang berhasil dikirim maka nilai *throughput* akan semakin besar. Semakin bagus jaringan yang digunakan, maka *throughput* semakin besar dikarenakan semakin banyak paket data yang dapat dikirim oleh mikrokontroler.

4. Kesimpulan

Berdasarkan pada hasil pengujian dan analisis hasil perancangan *smart weight scale* menggunakan algoritma *Advanced Encryption Standard* (AES) 100% telah sesuai dengan rancangan yang memiliki tingkat akurasi sebesar 99,74%. Proses enkripsi menggunakan kunci 128 bit membutuhkan waktu 87,68 µs lebih cepat dibandingkan menggunakan kunci 256 bit sebesar 90,64 µs. Sistem dapat bekerja lebih lama jika tanpa mengirimkan data. Data dari mikrokontroler dikirimkan secara *realtime* ke aplikasi dan pengiriman ke *server* merupakan data yang telah ter-enkripsi menggunakan algoritma AES-CBC yang ter-*encode* dengan algoritma Base64. Pengiriman data menggunakan *Bluetooth Low Energy* ke aplikasi memiliki *delay* lebih kecil dengan nilai rata-rata untuk kunci 128 bit dan 256 bit sebesar 85.428 ms dan 88.522 ms dengan *throughput* sebesar 2.074 bits/s dan 1.532 bits/s. Sedangkan untuk skenario Wi-Fi ke *server* nilai *delay* sebesar 311.173 ms dan 323.980 ms dengan nilai *throughput* 8.832 bits/s dan 7.819 bits/s.

Referensi:

[1] H. F. L. Muhammad, “Prevention of weight gain during self-isolation in COVID-19 pandemic era: a narrative review,” *J. Community Empower. Heal.*, vol. 3, no. 2, p. 123, 2020, doi: 10.22146/jcoemph.55976.

[2] D. Culica, J. Rohrer, M. Ward, P. Hilsenrath, and P. Pomrehn, “Medical checkups: who does not get them?,” *Am. J. Public Health*, vol. 92, no. 1, pp. 88–91, Jan. 2002, doi: 10.2105/ajph.92.1.88.

[3] C. M. Peterson, D. M. Thomas, G. L. Blackburn, and S. B. Heymsfield, “Universal equation for estimating ideal body weight and body weight at any BMI,” *Am. J. Clin. Nutr.*, vol. 103, no. 5, pp. 1197–1203, 2016, doi: 10.3945/ajcn.115.121178.

[4] C. Combi, G. Pozzani, and G. Pozzi, “Telemedicine for Developing Countries. A Survey and Some Design Issues,” *Appl. Clin. Inform.*, vol. 7, no. 4, pp. 1025–1050, Nov. 2016, doi: 10.4338/ACI-2016-06-R-0089.

[5] K. K. Patel, S. M. Patel, and P. G. Scholar, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges,” *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 1–10, 2016, doi: 10.4010/2016.1482.

[6] W. WAHYUDI, A. RAHMAN, and M. NAWAWI, “Perbandingan Nilai Ukur Sensor Load Cell pada Alat Penyortir Buah Otomatis terhadap Timbangan Manual,” *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 5, no. 2, p. 207, Feb. 2018, doi: 10.26760/elkomika.v5i2.207.

[7] A. Setiawan and A. I. Purnamasari, “Pengembangan Smart Home Dengan Microcontrollers ESP32 Dan MC-38 Door Magnetic Switch Sensor Berbasis Internet of Things (IoT) Untuk Meningkatkan Deteksi Dini Keamanan Perumahan,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 3 SE-Artikel Teknologi Informasi, Dec. 2019, doi: 10.29207/resti.v3i3.1238.

[8] G. Bhaudhayana and I. Widiartha, “Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap,” *J. Ilmu Komput.*, vol. 8, no. 2, pp. 15–25, 2015.