ANALISIS ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK SISTEM PEMANTAUAN KONSUMSI DAYA LISTRIK

ANALYSIS OF AES ALGORITHM FOR ELECTRICAL POWER CONSUMPTION MONITORING SYSTEM

Muhammad Rakha Laayu[1], Dr. Ir. Rendy Munadi, M.T.[2], Arif Indra Irawan, S.T., M.T.[3]

[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**rakhalaayu@student.telkomuniversity.ac.id**, [2]**rendymunadi@telkomuniversity.ac.id**,
[3]**arifirawan@telkomuniversity.ac.id**

Abstrak

Penggunaan kriptografi dalam pembuatan proyek *Internet of Things* (IoT) masih terkategori rendah sehingga bisa memunculkan ancaman pribadi untuk penggunanya. Algoritma kriptografi modern digunakan dalam mengamankan lalu lintas data pada sistem pemantauan konsumsi daya listrik. Sistem menggunakan algoritma enkripsi *Advanced Encryption Standard* (AES) mode *Cipher Blocker Chaining* (CBC) dengan panjang kunci 128, 192, dan 256 bit yang terintegrasi dengan layanan *Amazon web server*.

Pengujian performansi dilakukan dan mendapatkan hasil nilai rata-rata *Avalanche effect* untuk setiap panjang kunci 128, 192, dan 256 bit adalah 46% dengan konsumsi listrik sebesar 36 miliAmpere. AES mengalokasikan memori sebesar 128, 192, dan 256 bit untuk tiap-tiap panjang kunci dengan lama waktu proses sebesar 830,11 µs, 850,87 µs, dan 883,26 µs untuk AES-128, AES-192, dan AES-256. Nilai rata-rata QoS mikrokontroler Wemos D1 ESP8266 dari/ke *cloud server* untuk setiap panjang kunci berbeda yaitu *Delay* sebesar 0,34 detik dan *Throughput* sebesar 2244,2 bit/s.

Kata kunci : ***Internet of Things, Advanced Encryption Standard, Amazon webserver, SCT-013-000, Wemos D1 ESP8266.***

Abstract

Lack of cryptography usage in making Internet of Things (IoT) projects cause many privacy threat for the users. Modern cryptographic algorithms are used in electrical power consumption monitoring systems to secure data in electrical power consumption monitoring systems. System uses Advanced Encryption Standard (AES) algorithm with Cipher Blocker Chaining (CBC) mode and using 128, 192, and 256 bit key lengths. System integrated with Amazon web server.

System performance been tested and gets the average Avalanche effect value for each key length of 128, 192, and 256 bits is 46% with an electricity consumption of 36 milliAmpere. AES allocates memory of 128, 192, and 256 bit for each key length with processing times of 830.11 µs, 850.87 µs, and 883.26 µs for AES-128, AES-192, and AES-256. The average QoS value of the Wemos D1 ESP8266 microcontroller from / to the cloud server for each different key length are Delay of 0.34 seconds and Throughput of 2244.2 bits/s.

Key words : Internet of Things, Advanced Encryption Standard, Amazon web server, SCT-013-000, Wemos D1 ESP8266.

1. Pendahuluan

Penggunaan listrik yang tidak efektif pada suatu bangunan ditetapkan dengan menganalisis pola dari beberapa data yang tercipta dari kegiatan pemantauan serta pengukuran listrik. Pendekatan modern untuk mendapatkan informasi konsumsi daya listrik ialah dengan menggunakan instrumen teknologi *Internet of Things* (IoT). Penggunaan modul ESP8266 secara masif pada proyek IoT dikarenakan biayanya yang relatif murah dan kepraktisan yang ditawarkan, namun statistik menunjukkan dalam pengimplementasiannya aspek keamanan masih terkategori rendah[1]. Lalu lintas jaringan IoT rentan terhadap ancaman penyadapan dengan metode serangan *man-in-the-middle* oleh pihak- pihak yang tidak diinginkan. Kegiatan penyadapan pada lalu lintas jaringan yang tidak diproteksi mengarah pada pencurian informasi sensitif yang berujung pada penyalahgunaan informasi.

Penulis menganjurkan sistem enkripsi pada lalu lintas jaringan IoT menggunakan algoritma *Advanced Encryption Standard* (AES) yang diterapkan dalam sistem pemantauan konsumsi daya listrik. Sistem pemantauan konsumsi daya listrik dibangun menggunakan mikrokontroler Wemos D1 ESP8266, menyajikan data berupa besaran arus listrik yang terbaca oleh sensor SCT-013-00 dan besaran daya yang kemudian ditampilkan pada sebuah LCD. Algoritma enkripsi AES menggunakan mode operasi *Cipher Block Chaining* (CBC). Data berupa arus listrik yang dibaca oleh sensor dilakukan proses enkripsi dan pengkodean dengan algoritma AES dan Base64 sebelum dikirimkan ke aplikasi Node.js pada *cloud server* AWS EC2. Data yang telah ter-*decrypt* oleh aplikasi node.js kemudian ditampilkan oleh aplikasi ReactJS dalam tampilan web sederhana. Protokol HTTP digunakan

dalam komunikasi pengiriman data antara mikrokontroler dan *cloud server*. Analisis algoritma AES pada sistem dilakukan dengan menghitung performansi sistem berupa *Avalanche effect*, konsumsi daya, memori, kecepatan proses, dan *Quality of Service* jaringan berupa *Delay* dan *Throughput* terhadap konfigurasi sistem menggunakan AES dengan panjang kunci 128, 192, dan 256 bit. Diharapkan dengan penggunaan enkripsi pada lalu lintas jaringan IoT dapat meningkatkan aspek keamanan informasi berupa Confidentiality serta Integrity untuk konsumen IoT.

2. Dasar Teori

2.1 Internet of Things

IoT adalah paradigma di mana objek dan elemen dari suatu sistem yang dilengkapi dengan sensor, aktuator, dan prosesor yang dapat saling berkomunikasi untuk memberikan suatu layanan yang bermanfaat[2].

2.2 Sensor SCT-013-000

YHDC SCT-013-000 adalah sensor Current Transformers(CTs) atau trafo arus yang dapat mengukur arus bolak-balik/AC dan berguna untuk mengukur konsumsi atau pembangkitan listrik pada bangunan. Trafo arus memiliki lilitan primer, inti magnetik, dan lilitan sekunder. Arus bolak-balik yang mengalir dalam primer menghasilkan medan magnet dalam inti, yang menginduksi arus dalam rangkaian lilitan sekunder[3]. Arus dalam belitan sekunder sebanding dengan arus yang mengalir dalam belitan primer[3]:

$$Isekunder = CTRasioBelitan \times Iprimer$$
$$CTRasioBelitan = Belitanprimer/Belitansekunder \quad (1)$$

2.3 A*mazon Elastic Compute* Cloud (Amazon EC2)

Amazon EC2 adalah layanan web yang memberikan kapasitas komputasi yang aman dan berukuran fleksibel di cloud[4]. Amazon EC2 digunakan dalam sistem pemantauan konsumsi daya listrik karena memberikan layanan *Virtual Private Server* (VPS) dengan keuntungan fleksibilitas, kontrol, dan penghematan biaya yang baik.

2.4 *Hyper Text Transfer Protocol* (HTTP)

Hyper Text Transfer Protocol (HTTP) merupakan protokol komunikasi yang dapat menghubungkan *client, server* dan perangkat IoT. Protokol HTTP ini berkerja pada TCP/IP yang menyediakan komunikasi yang handal, protokol ini mengirimkan banyak paket kecil ke server agar dapat terhubung.

2.5 Daya AC

Daya listrik adalah besarnya laju hantaran energi listrik yang terjadi pada suatu rangkaian listrik. Dalam satuan internasional daya listrik adalah Watt (W) yang menyatakan besarnya usaha yang dilakukan oleh sumber tegangan untuk mengalirkan arus listrik tiap satuan waktu Joule/detik (J/s). Pada sistem pemantauan konsumsi daya listrik, beban yang diukur sensor bersifat resistif murni, sehingga daya semu (S) adalah hasil perkalian antara tegangan efektif (*rootmean-square/RMS*) dengan arus efektif (*root-mean-square*/RMS)[3]:

$$S = Tegangan\ rms \times Arus\ rms \quad (2)$$

2.6 Liquid Crystal Display (LCD)

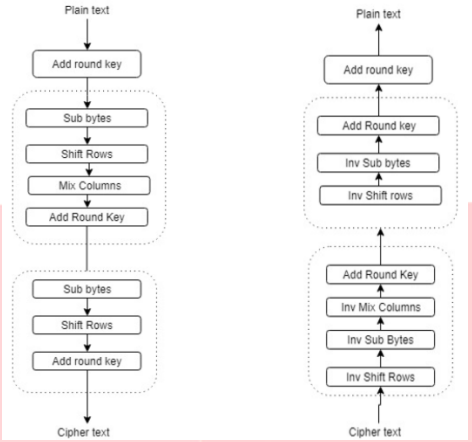
LCD merupakan media tampilan yang dapat penampilkan informasi keluaran dari program sebuah alat, pada sistem pemantauan konsumsi daya listrik menggunakan LCD 2 x 16 sebagai media tampilan.

2.7 *Man-in-the-Middle Attack* (MITM)

MITM adalah istilah umum ketika penyerang memposisikan dirinya ditengah-tengah percakapan antara pengguna dan aplikasi. Secara umum, serangan MITM pada sistem pemantauan konsumsi daya listrik terjadi jika penyerang berhasil masuk kedalam jaringan lokal yang menghubungkan mikrokontroler dengan *cloud server*. Kemudian penyerang melakukan pemantauan pada setiap paket yang melintasi jaringan dan melakukan *capture* data ataupun mengubah data asli korban yang kemudian diteruskan ke *cloud server*.

2.8 Advanced Encryption Standard (AES)

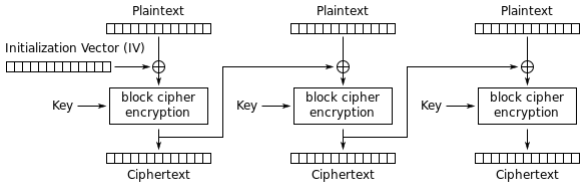
AES adalah sistem kriptografi simetris bertipe *block cipher* dengan spesifikasi panjang blok 128 bit. Istilah *Plain text* adalah data atau pesan awal sebelum dilakukannya proses enkripsi dan hasil dari data terenkripsi disebut sebagai *Cipher text*. Proses operasi AES dilakukan menggunakan satuan penyimpanan data *byte*/bita.



Gambar 2.1 Diagram Proses Enkripsi AES

2.9 *Cipher Block Chainning* (CBC)

CBC merupakan salah satu mode operasi *block cipher* yang menggunakan *initialitation vector* (IV) dengan ukuran yang sama dengan satu blok *plain text*. Pada mode operasi ini *plain text* dibagi menjadi beberapa blok. Sebelum dienkripsi, *plain text* di-XOR dengan IV. Lalu, hasil XOR tersebut dienkripsi hingga menghasilkan *cipher text*. Selanjutnya, *cipher text* tersebut digunakan sebagai IV untuk proses penyandian blok *plain text* selanjutnya. Dengan cara ini, tiap cipher text dari masing-masing blok akan tergantung pada seluruh hasil cipher teks dari blok-blok sebelumnya dan membuat tiap pesan menjadi unik[5].



Gambar 2.2 Skema mode CBC

2.10 Base64

Transformasi Base64 merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan *encoding* (penyandian) terhadap data *binary*.

2.11 Node.js

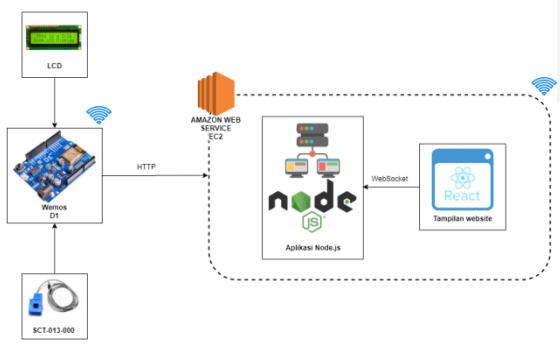
Node.JS adalah sistem perangkat lunak yang didesain untuk pengembangan aplikasi web dan diimplementasikan di *server*. Pada sistem pemantauan konsumsi daya listrik Node.js digunakan sebagai *back-end server* pada *cloud server* yang melakukan proses dekripsi dan *decode* data yang diterima dari mikrokontroler.

2.12 ReactJS

ReactJs adalah sebuah library JavaScript yang di buat oleh Facebook. React adalah library yang bersifat *composable user interface*, yang artinya kita dapat membuat berbagai *user interface* yang bisa kita bagi menjadi beberapa komponen[6].

3. Pembahasan

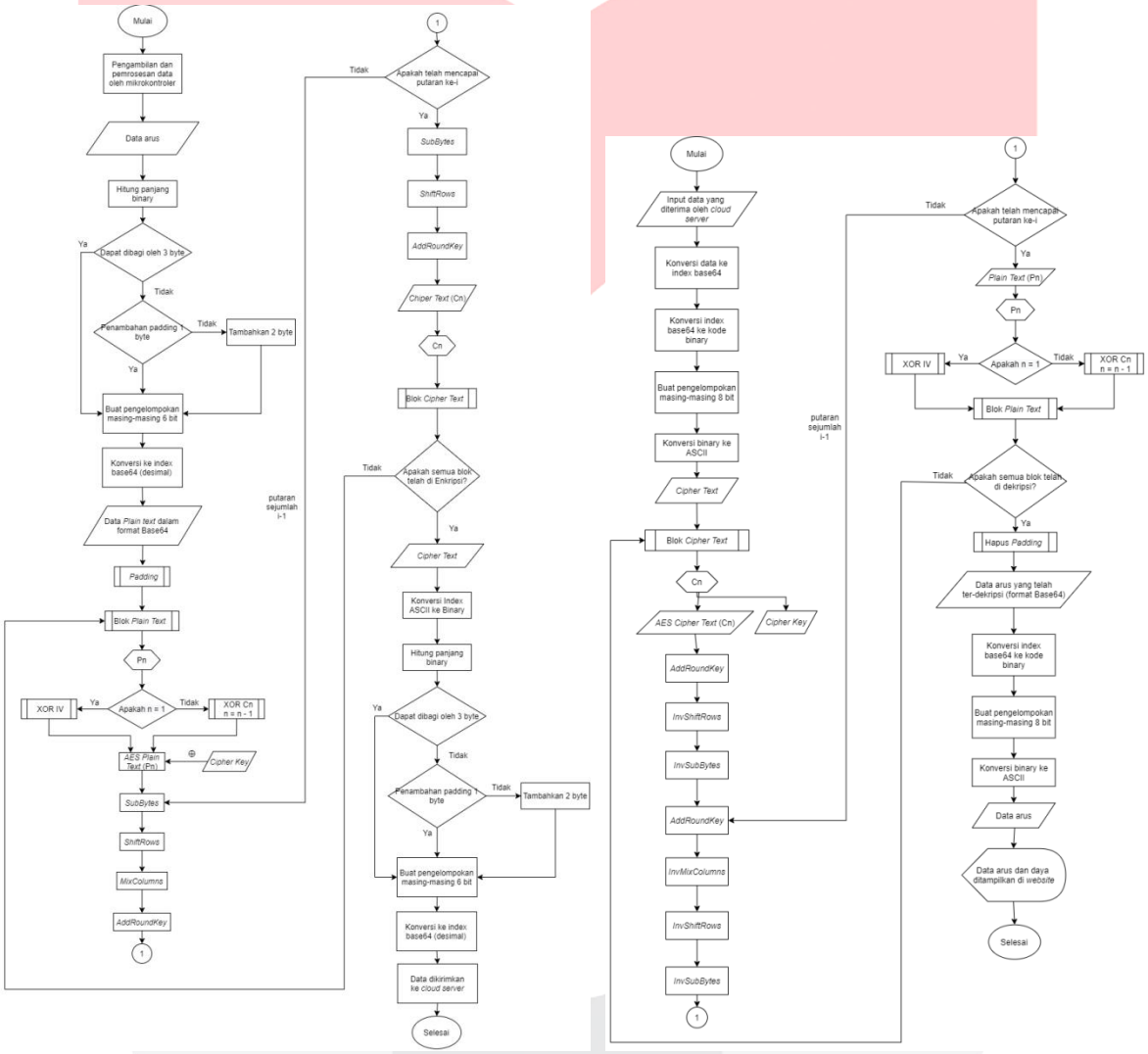
3.1 Desain Sistem



Gambar 3.1 Diagram sistem pemantauan konsumsi daya listrik

Komponen pertama adalah bagian *hardware* yaitu terdiri dari mikrokontroler, sensor, dan rangkaian resistor beban. Bagian ini berfungsi sebagai alat yang dapat membaca arus listrik, pengontrol rangkaian elektronik, menyimpan program dan melakukan proses enkripsi dan pengkodean data. Komponen kedua adalah bagian *software* yaitu berupa aplikasi Node.js yang berfungsi sebagai *back-end* dari *server* yang dapat mengolah data yang diterima dari mikrokontroler. Komponen terakhir adalah bagian khusus untuk *brainware* yaitu berupa LCD dan tampilan grafis berupa *website* yang dibangun menggunakan *framework front-end* ReactJS.

3.2 Flowchart



(a) **(b)**

Gambar 3.2 Diagram Alir Sistem Pemantauan Konsumsi Daya Listrik, (a) pada sisi mikrokontroler dan (b) pada sisi *cloud server*

3.3 Pengujian Sistem

3.4.1 *Avalanche Effect* (AE)

AE adalah perubahan kecil bit (misalnya, satu bit) baik pada *plain text* maupun *key*/kunci yang akan menyebabkan perubahan signifikan terhadap hasil dari *cipher text*. AE dapat digunakan sebagai metrik untuk menganalisis kinerja dan keamanan dari suatu algoritma enkripsi kriptografi [7]. Pada skenario ini dilakukan analisis kinerja dan keamanan enkripsi AES berupa besar AE terhadap panjang kunci enkripsi yaitu 128, 192, dan 256 bit.

$$Avalanche\ effect = \frac{jumlah\ perubahan\ bit}{jumlah\ seluruh\ bit\ cipher\ text} \times 100\% \quad \textbf{(3)}$$

3.4.2 Konsumsi Daya

Pengukuran dilakukan menggunakan multimeter untuk mengetahui besar arus yang dikonsumsi mikrokontroler dalam pengimplementasian AES dengan panjang kunci enkripsi 128, 192, dan 256 bit. Alasan untuk menghitung nilai konsumsi daya pada projek IoT adalah untuk mengetahui *power supply* yang sesuai dengan kebutuhan perangkat dan berapa lama *runtime* perangkat jika menggunakan baterai.

$$Runtime\ (jam) \frac{Kapasitas\ baterai\ (mAh)}{Konsumsi\ arus\ mikrokontroler\ (mA)} \quad \textbf{(4)}$$

3.4.3 Memori

Pengukuran nilai memori berupa *Flash* yang digunakan untuk menjalankan program mikrokontroler berdasarkan konfigurasi panjang kunci enkripsi yang digunakan yaitu 128, 192, dan 256 bit. Pengujian dilakukan membandingkan nilai memori yang digunakan secara bergantian untuk tiap panjang kunci yang digunakan.

3.4.4 Kecepatan Proses

Pengujian ini bertujuan untuk menghitung lama waktu yang dibutuhkan sistem untuk menjalankan proses enkripsi dan pengkodean data serta lama waktu yang dibutuhkan sistem untuk menjalankan keseluruhan program pada sistem yang menggunakan panjang kunci 128, 192, dan 256 bit. Analisa dilakukan dengan melakukan program arduino menggunakan fungsi *micros*() yang melakukan perhitungan berdasarkan *string* per data.

3.4.5 Throughput

Throughput adalah kemampuan jaringan dalam melakukan pengiriman data yang terukur dalam satuan bit per second (bps). Throughput merupakan jumlah total kedatangan paket yang sukses sampai pada tujuan selama interval waktu tertentu kemudian dibagi dengan durasi interval waktu tersebut [8].

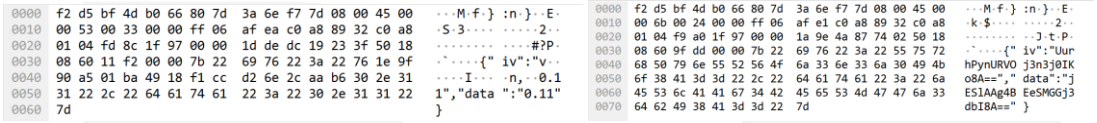
3.4.6 Delay

Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama.

4. Hasil dan Analisis

4.1 Hasil Pengujian Alat

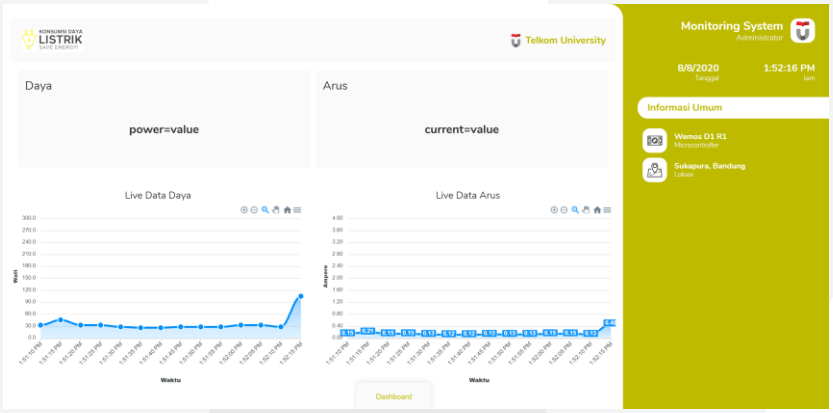
4.1.1 Lalu Lintas Data



(a) **(b)**

Gambar 4.1 Hasil pemantauan lalu lintas data sistem, (a) *payload* sistem tanpa penggunaan AES dan Base64 dan (b) *payload* sistem dengan penggunaan AES dan Base64

4.1.2 Aplikasi Web



Gambar 4.2 Hasil pembacaan konsumsi daya listrik pada aplikasi web

4.2.1 Analisis
4.2.2 Analisis *Avalanche Effect*

Tabel 4.1 Avalanche Effect (rata-rata).

Panjang Kunci	Nilai Avalanche Effect
AES 128 bit	46,1%
AES 192 bit	46%
AES 256 bit	46,1%

Pada pengujian yang telah dilakukan, **Tabel 4.1** menunjukkan nilai rata-rata *Avalanche Effect* untuk tiap-tiap panjang kunci. Nilai *Avalanche effect* yang didapatkan tidak sepenuhnya berbanding lurus dengan panjang kunci yang digunakan, hal ini dikarenakan beberapa faktor seperti *plain text* yang digunakan ataupun pemilihan karakter yang diubah dalam menghitung perubahan bit pada pengujian.

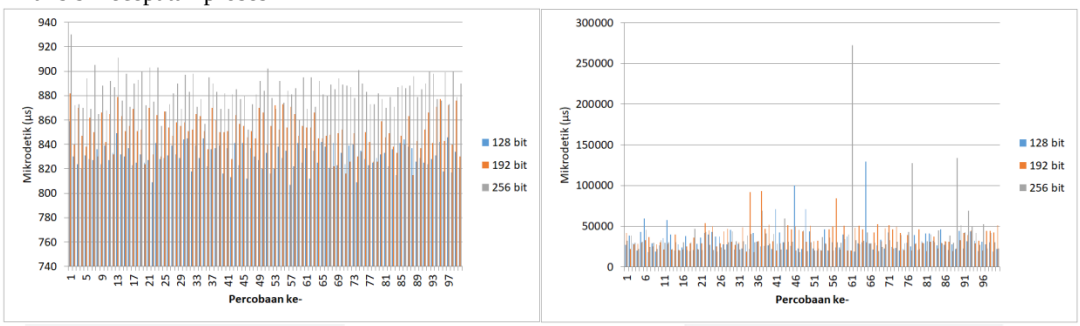
4.2.3 Analisis Konsumsi Daya

Pengukuran konsumsi daya pada sistem yang menjalankan enkripsi dengan panjang kunci berbeda mendapatkan hasil yang relatif sama yaitu rata-rata sebesar 36 miliAmpere. Perbedaan nilai arus yang didapatkan pada pengujian sistem terjadi karena konsumsi listrik yang bekerja pada mikrokontroler bersifat acak dan sulit ditebak yang mana bergantung pada kualitas dan kondisi prosesor yang sedang berlangsung ataupun kondisi memori mikrokontroler yang digunakan.

4.2.4 Analisis Memori

Nilai besaran *flash* yang digunakan untuk sistem IoT bergantung pada panjang kunci yang digunakan, semakin besar panjang kunci yang digunakan maka semakin banyak memori yang dibutuhkan. Algoritma AES mengalokasikan variabel yang harus disimpan pada memori mikrokontroler sebesar panjang kunci yang digunakan yaitu 128, 192, dan 256 bit.

4.2.5 Analisis Kecepatan proses

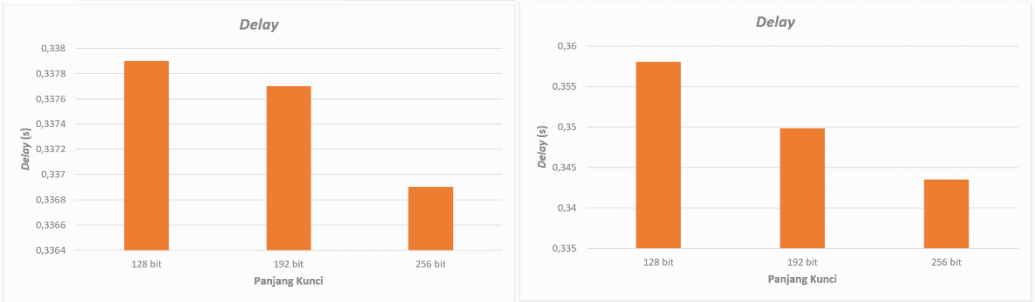


(a) **(b)**

Gambar 4.3 Hasil pengujian kecepatan proses. (a) kecepatan enkripsi dan pengkodean data, (b) kecepatan sistem untuk memproses seluruh *script.*

Lama waktu proses enkripsi dan pengkodean data untuk panjang kunci 128, 192, dan 256 bit adalah 830,11 µs, 850,87 µs, dan 883,26 µs. Lama waktu proses seluruh *script* untuk panjang kunci 128, 192, dan 256 bit adalah 32406,26 µs, 36338,68 µs, dan 36546,41 µs. Rata-rata nilai selisih kenaikan lama waktu proses enkripsi dari panjang kunci 128, ke 192, dan ke 256 bit sebesar 3,15%. Hal ini dikarenakan dalam memproses data algoritma AES melakukan proses enkripsi dengan putaran (*round*) yang berbeda untuk tiap panjang kunci.

4.2.6 Analisis *Delay*

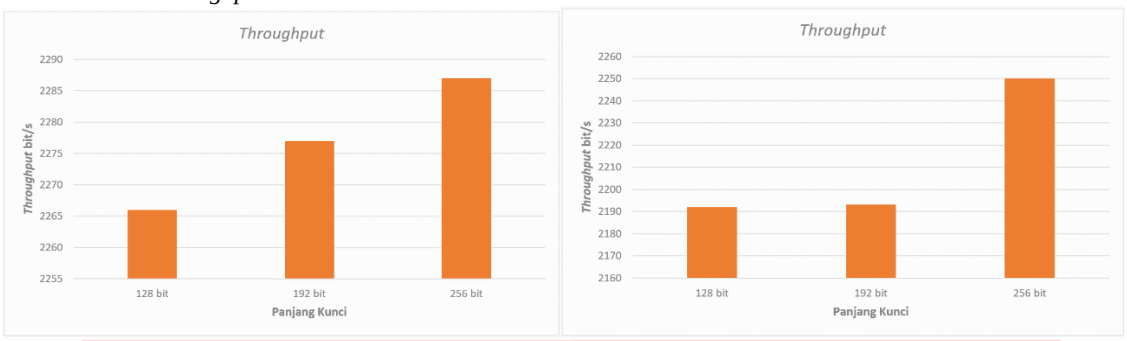


(a) **(b)**

Gambar 4.4 Diagram rata-rata *Delay* jaringan Wemos D1 ESP8266 dari/ke *cloud server.* (a) menggunakan jaringan Wi-fi serat optik, (b) menggunaka jaringan Wi-Fi 4G

Hasil *delay* bersifat tidak konsisten pada tiap-tiap sistem dengan panjang kunci yang berbeda. Hal tersebut dikarenakan oleh kualitas koneksi internet yang tidak dapat diprediksi.

4.2.7 Analisis *Throughput*



(a) **(b)**

Gambar 4.4 Diagram rata-rata *Delay* jaringan Wemos D1 ESP8266 dari/ke *cloud server*. (a) menggunakan jaringan Wi-fi serat optik, (b) menggunaka jaringan Wi-Fi 4G

Hasil *Throughput* bersifat tidak konsisten pada tiap-tiap sistem dengan panjang kunci yang berbeda. Hal tersebut dikarenakan oleh kualitas koneksi internet yang tidak dapat diprediksi.

5. Kesimpulan

Berdasarkan hasil pengujian sekaligus analisis performansi algoritma *Advance Encryption Standard* (AES) yang telah dilakukan pada sistem pemantauan konsumsi daya listrik, penulis bisa mengambil kesimpulan yaitu sebagai berikut:

1) Algoritma enkripsi yang digunakan pada sistem pemantauan konsumsi daya listrik berjalan dengan baik.
2) Sistem AES-CBC dengan menggunakan panjang kunci 126 bit dirasa cukup aman untuk diterapkan pada lalu lintas jaringan IoT, menimbang nilai *Avalanche effect* yang relatif sama untuk tiap panjang kunci.
3) Nilai rata-rata konsumsi daya dengan konfigurasi tiga jenis panjang kunci enkripsi adalah 36 miliAmpere, dapat dijalankan menggunakan baterai 9 Volt kapasitas 550mAh selama lebih kurang 15 jam.
4) Besar penggunaan memori dan kecepatan proses berbanding lurus dengan panjang kunci yang digunakan, nilai selisih kenaikan lama waktu proses enkripsi dari panjang kunci 128, ke 192, dan ke 256 bit sebesar 3,15%.
5) Nilai rata-rata QoS mikrokontroler Wemos D1 ESP8266 dari/ke *cloud server* dengan konfigurasi tiga jenis panjang kunci berbeda yaitu *Delay* sebesar 0,34 detik dan *Throughput* sebesar 2244,2 bit/s.

Daftar Pustaka:

[1] "Nodemcu custom build." [Online]. Available: https://nodemcu-build.com/stats.php
[2] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of things (iot) and the energy sector," Energies, vol. 13, no. 2, p. 494, 2020.
[3] Openenergymonitor, "openenergymonitor/learn." [Online]. Available: https://github.com/openenergymonitor/learn/blob/master/view/ electricity-monitoring/ct-sensors/introduction.md
[4] ——, "Amazon ec2," 2001. [Online]. Available: https://aws.amazon.com/id/ec2/
[5] R. Munir, "Pengantar kriptografi," Informatika, Bandung, 2006.
[6] "Getting started." [Online]. Available: https://reactjs.org/docs/getting-started.html
[7] D. Dafid, "Kriptografi kunci simetris dengan menggunakan algoritma crypton," @ lgoritma, vol. 2, no. 3, pp. 20–27, 2006.
[8] P. Wulandari, S. Soim, and M. Rose, "Monitoring dan analisis qos (quality ofservice) jaringan internet pada gedung kpa politeknik negeri sriwijaya denganmetode drive test," Prosiding SNATIF, pp. 341–347, 2017.