# Perancangan Dan Implementasi Pemetaan Lokasi Dalam Ruangan Menggunakan Teknologi Ble Berbasiskan Web *Discover*-U Dengan Algoritma *Advanced Encryption Standard* (AES)

1st Cheril Erlita Zuliarty
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
cherilerlita@student.telkomuniversity.ac.id

2nd Sussi
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
sussiss@telkomuniversity.ac.id

3rd Favian Dewanta
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
favian@telkomuniversity.ac.id

**Abstrak—Teknologi indoor positioning atau indoor localization atau pelacakan dalam ruangan ialah teknologi yang memanfaatkan wireless sensor network. Teknologi ini digunakan untuk mendeteksi lokasi di dalam ruangan dan dianggap lebih akurat dibandingkan menggunakan teknologi GPS. Dalam Tugas Akhir ini, akan membuat desain dan implementasi indoor positioning atau indoor localization berbentuk web application yang bernama "Discover-U". Sistem ini dirancang menggunakan bahasa pemrograman JavaScript untuk memeriksa posisi pengguna alat smart stick yang dihubungkan dengan NodeMCU ESP32 dengan menggunakan teknologi bluetooth low energy (BLE) secara tidak real time. Data pengguna akan dikirmkan ke Firebase yang berasal dari MQTT dan disimpan dalam Local Computer. Pembuatan web application dibuat menggunakan algoritma enkripsi kunci simetris AES 192 yang merupakan blok data 192 bit. Hasil pengukuran *Quality of Service* dari *Server* MQTT ke *Local Computer* memiliki *delay* rata-rata 673 ms, *throughput* 968,1 bps, dan *packet loss* 0%. Untuk hasil pengujian performansi algoritma AES 192-bit memiliki rata-rata waktu enkripsi sebesar 2 s dan tanpa enkripsi yaitu 0 s.**

**Kata Kunci— web application, internet of things, bluetooth low energy, AES, Firebase, indoor localization, MQTT**

***Abstract—Indoor positioning technology or indoor localization or indoor tracking is a technology that utilizes a wireless sensor network. This technology is used to detect indoor location and rate more accurately than using GPS technology. This final project will make design and implement indoor positioning or indoor localization formed web application namely "Discover-U". The system was designed using programming language JavaScript to investigate the position of the smart stick user tool which connected with NodeMCU ESP32 by using Bluetooth low energy (BLE) technology in non-real-time. User data will send to firebase which comes from MQTT and saved into the local computer. A web application is made by using A symmetrical AES 192 encryption algorithm which is data block 192 bit. The measuring result Quality of service from Server MQTT into local computer own delay on the average 673 ms, throughput 968,1 bps, and loss packet amount 0% Besides, the result of Algorithm performance testing AES 192-bit had an encryption time average amount of 2 s and without encryption is 0 s.***

***Key Words— web application, internet of things, bluetooth low energy, AES, firebase, indoor localization, MQTT***

## I. PENDAHULUAN

Saat ini perkembangan teknologi saat ini sudah sangat pesat, sehingga penggunaan internet, mobile device, dan teknologi lain dapat digunakan. Hal yang dapat kita ambil sebagai pengaruh teknologi informasi saat ini yaitu Global Positioning System (GPS). Namun, teknologi GPS memiliki kelemahan yaitu, ketika digunakan di dalam ruangan atau di dalam gedung, kinerjanya tidak maksimal dan tidak dapat membedakan pengguna sedang berada di ruangan mana. Hal ini dikarenakan gelombang radio yang dikirim oleh satelit GPS tidak dapat melewati benda tebal seperti tembok, dll.

Selain teknologi GPS, teknologi indoor positioning atau indoor localization atau pelacakan dalam ruangan yang memanfaatkan wireless sensor network yang kini telah dikembangkan. Teknologi ini digunakan untuk mendeteksi lokasi di dalam ruangan dan dianggap lebih akurat dibandingkan menggunakan

teknologi GPS. Indoor positioning atau indoor localization bisa disebut sebagai teknologi untuk mengatasi kelemahan GPS yang telah disebutkan sebelumnya. [1]

Dengan perkembangan teknologi yang sangat signifikan, *bluetooth* juga tidak mau kalah dengan mengeluarkan inovasi terbarunya yaitu *bluetooth low energy* (BLE). Kelebihan BLE ini ialah menggunakan daya baterai yang kecil dibanding dengan *bluetooth* yang biasa serta perawatan BLE juga lebih murah dan juga jarak yang dekat. Salah satu yang menggunakan teknologi BLE yaitu Beacon. Beacon bekerja sebagai penentu letak lokasi yang terdapat dalam suatu ruangan indoor. [2]

Berdasarkan data Susenas pada 2018, ada 14,2 persen penduduk Indonesia yang menyandang disabilitas atau 30,38 juta jiwa. Dengan adanya permasalahan tersebut dan juga memanfaatkan inovasi yang sedang berkembang, usulan tugas akhir ini adalah berfokus pada membuat sebuah web application bernamakan Discover-U dengan menampilkan data lokasi pengguna tongkat secara tidak real time. Tongkat pintar tersebut memanfaatkan teknologi indoor localization dan menggunakan *bluetooth low energy* (BLE) dalam memaksimalkan alat yang dibuat yang bertujuan untuk membantu pengguna yang membutuhkan tongkat pintar tersebut dalam kebutuhan sehari-harinya. Lalu untuk menyimpan data yang diberikan dari tongkat pintar dibuatkan web application agar pengguna dapat melihat posisi pengguna tongkat berupa map.

Tongkat pintar tersebut namun mungkin saja melakukan pergantian informasi data penting contohnya nama pengguna dan *password*. Hal ini yang mendasari pentingnya authentication dan security data.

## II. KAJIAN TEORI

Pada penelitian sebelumnya digunakan algoritma Diffie-Hellman dan juga AES untuk mengamankan data yang dikirimkan dari alat ke web application dan data yang berada di web application. Penelitian ini mengimplementasikan kriptografi simetrik AES untuk enkripsi data *user* seperti login dan registrasi. [3]

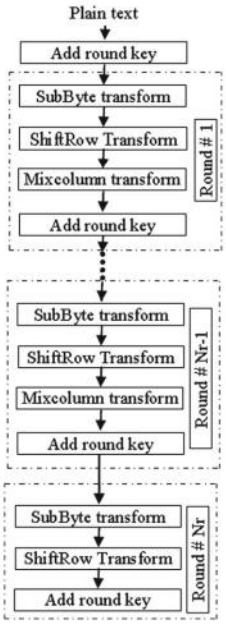
Penelitian lainnya dilakukan oleh Tran Trong Khanh, VanDung Nguyen, Xuan Qui Pham and Eui Nam Huh membahas mengenai penentuan posisi dan navigasi dalam ruangan Wi-Fi menggunakan sistem cloudlet-based cloud computing system. Penelitian ini diuji menggunakan peralatan Raspberry Pi 3 yang dirancang dengan *cloudlets, core cloud*, dan *self-driving cart cloudlet*). Cloudlet dan core cloud dapat melacak navigasi untuk kereta self-driving dalam ruangan serta global positioning dan lokal yang dirancang untuk titik akses referensi dan posisi tertentu dapat menavigasi kereta self-driving ke posisi tertentu secara akurat. [4]

Penelitian lainnya juga dilakukan oleh Bahri Rizaldi, Doni Setio Pambudi, dan Taufiqotul Bariyah membahas mengenai Implementasi Teknologi *Bluetooth Low Energy* dan Metode Trilaterasi Untuk Pencarian Rute Indoor menggunakan teknologi BLE dan triletarion serta menggunakan algoritma Djikstra untuk menentukan lokasi terpendek. Hasil yang didapatkan yaitu memiliki error penentuan lokasi sebesar 0,728 meter dengan jarak antara pengguna dengan beacon kurang dari 10 meter untuk mendapatkan sinyal yang baik dan stabil. [5]

## III. METODE

### A. *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) mempunyai tiga versi, tergantung pada panjang kunci (AES128, AES192 dan AES256). Kunci ini direpresentasikan dalam tabel ukuran 4 × 4, 4 × 6 dan 4 × 8. Dalam AES asli, tergantung pada panjang kunci, empat transformasi status berturut-turut dilakukan dalam 10, 12 atau 14 putaran, lihat Gambar 3.6. Transformasi AES dijelaskan sebagai berikut [6]:




GAMBAR 3.1.
STRUKTUR ALGORITMA AES DIMANA NR =10, 12, OR 14 SEBAGAI PANJANG KUNCI MASING-MASING (128, 192 OR 256 BIT) [6]

1. AddRoundKey

Operasi ARK dilakukan dengan melakukan logic operation X-OR antara state array dan subkey atau disebut dengan round key. Pada AddRoundKey ada proses yang disebut dengan initial round yang diartikan sebagai operasi pada X-OR dilakukan pada masing-masing byte dan array dan menghasilkan nilai baru

dengan ukuran sebesar 4x4 untuk baris dan kolom yang sama dengan array state awal dan array key [6].

2. SubBytes

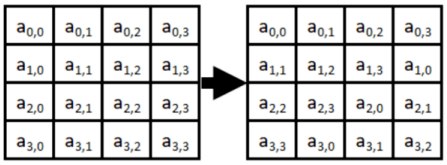
Fase SubBytes menurut AES melibatkan pemisahan input menjadi byte dan masing-masing melewati melalui S-Box. Tidak seperti DES, AES memakai S-Box yang sama untuk seluruh byte. S-Box AES mengimplementasikan perkalian invers pada Galois Field 28 setelahnya diikuti oleh transformasi affine [7]. S-Box AES ditunjukkan dalam Gambar di bawah ini.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0a | 0b | 0c | 0d | 0e | 0f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 1 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 4 | c7 | 23 | c3 | 18 | 96 | 5 | 9a | 7 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 9 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 0 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 2 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 6 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 8 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 3 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

GAMBAR 3.2.
S-BOX [7]

3. ShiftRows

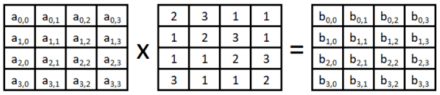
Pada ShiftRows AES, setiap baris dari status internal 128-bit cipher dilakukan pergeseran. Baris dalam tahap ini mengacu pada representasi standar keadaan internal di AES, yang merupakan matriks 4x4 di mana setiap sel berisi satu byte. Dalam operasi ShiftRows, masing-masing baris ini digeser ke kiri dengan jumlah yang ditentukan: nomor barisnya dimulai dari nol. Baris atas tidak dilakukan pergesaran, baris berikutnya digeser satu dan seterusnya. Hal ini diilustrasikan pada Gambar di bawah ini.




GAMBAR 3.3.
OPERASI SHIFTROWS [7]

4. MixColumns

Operasi MixColumns menyediakan difusi dengan mencampurkan input di sekitarnya. Tidak seperti ShiftRows, MixColumns melakukan operasi pemisahan matriks menggunakan kolom, bukan baris.




GAMBAR 3.4.
REPRESENTASI MIXCOLUMNS [7]

Representasi dari operasi MixColumns ditunjukkan di atas. Tidak seperti perkalian matriks yang biasa, MixColumns melakukan perkalian matriks sesuai Galois Field $2^8$ yaitu dengan mengalikan setiap kolom dari array state. Perkalian ini memiliki sifat operasi secara mandiri pada setiap kolom matriks awal.

*B.* Parameter Pengujian performansi

Pengambilan data dari Cloud Server MQTT dengan dengan data pengguna disimpan ke dalam Local Computer lalu pengiriman data dari Cloud Server Firebase ke Web Aplikasi. Pengujian sistem ini dilakukan dengan berbagai skenario yaitu pengujian performansi jaringan dengan Quality of Service (QOS), performansi keamanan, serta fungsionalitas.

1. Pengujian Performansi Jaringan dengan Quality of Service (QoS)

Metode ini mengukur seberapa baik kualitas jaringan dalam sistem web application yang dibuat. Pada pengujian Pengujian kualitas layanan atau Quality of Service memakai skenario yaitu menguji kinerja jaringan dari web application ke *Local Computer*. Adapun parameter yang diuji yaitu [8] :

a. Delay/Latency

Perhitungan delay dilakukan yaitu dengan menghitung waktu yang dibutuhkan data untuk terkirim dari tempat asal ke tempat tujuan.

b. Throughput

Pengukuran dalam Throughput adalah kecepatan (rate) transfer data efektif, yang diukur dalam bps (bit per second) atau bytes per second.

Persamaan perhitungan Throughput :

$$Throughput = \frac{\text{Packet data diterima}}{\text{Lama pengamatan}} \quad (3.1)$$

c. Packet Loss

Packet loss ialah parameter yang menampilkan jumlah total paket hilang yang dapat terjadi akibat tabrakan dan kemacetan pada jaringan.

$$Packet\ loss = \frac{(\text{Paket data dikirim} - \text{Paket data diterima}) \times 100\ \%}{\text{Paket data yang dikirim}} \quad (3.2)$$

2. Pengujian Performansi Keamanan Web Aplikasi

a. Pengujian Performansi Algoritma AES

Perbandingan hasil password sebelum dienkripsi dan sesudah dienkripsi.

b. Pengujian Waktu Pemrosesan Algoritma AES

Perbandingan hasil waktu pemrosesan password menggunakan enkripsi AES dan yang tidak menggunakan enkripsi

c. Pengujian Performa AES-192 berdasarkan Avalanche Effect

d. Pengukuran performansi AES-128 berdasarkan Avalanche Effect menggunakan Cryptool

3. Pengujian Fungsionalitas

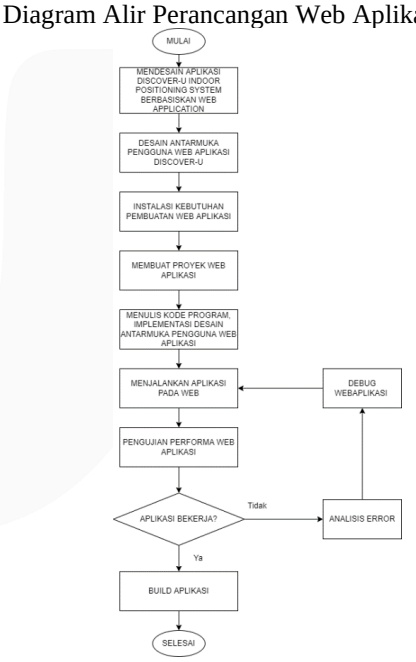
Pengujian ini mengukur kinerja sebuah Web Aplikasi menggunakan metode pengujian *Black Box Testing*. Memastikan semua fitur berjalan dengan lancar dan tidak ada terjadinya *error*.

*C.* Desain Sistem


GAMBAR 3.1.
DESAIN SISTEM

Gambar 3.7 memberikan input yaitu lokasi pengguna smart stick dengan melakukan hubungan komunikasi dengan web application dengan protokol komunikasi smart stick yang terdiri dari *Bluetooth Low Energy*. Ketika pengguna menggunakan web application pendeteksi lokasi, data lokasi akan terlampir pada layar dan data login serta registrasi terintegrasi dengan Firebase yang menggunakan enkripsi AES-192 hingga dapat memantau lokasi setiap harinya.

1. Diagram Alir Perancangan Web Aplikasi



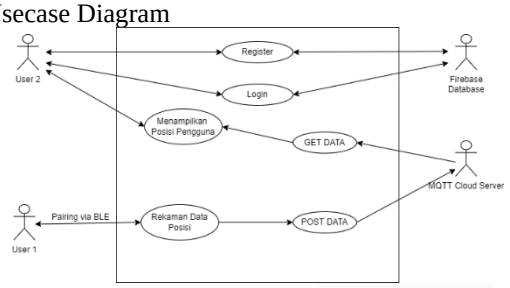

GAMBAR 3.2.
DIAGRAM ALIR PERANCANGAN WEB APLIKASI

Pada gambar 3.8. dijelaskan proses pembuatan aplikasi "Discover-U". Proses pertama yaitu merancang bentuk aplikasi pada sistem web application agar mengetahui proses menghubungkan antara device Smart Stick dengan aplikasi Discover-U berbasis web application dan proses menghubungkan antara web application ke Firebase Server dengan mengambil data

dari MQTT Cloud Server dan disimpan ke dalam Local Computer dan di deploy ke Firebase. Lalu setelah itu dilanjutkan dengan mendesain tampilan antarmuka atau UI/UX pada web aplikasi agar tampilan dapat *user* friendly. Selanjutnya memasukan kebutuhan dalam web aplikasi yang akan digunakan yaitu environment, tools, dependencies, dan libraries. Selanjutnya, pembuatan aplikasi dengan menulis pemrogrograman dan mendesain antarmuka untuk pengguna dalam barisan Source Code. Selanjutnya menjalankan web aplikasi dan menguji performansi untuk mengetahui apakah aplikasi bekerja dengan baik. Dilanjutkan dengan pengecekan apakah aplikasi sudah berjalan dengan baik atau mengalami error dengan dihilangkannya bug dalam log. Jika terdapat error maka melakukan debugging serta melihat performansi aplikasi kembali. Jika aplikasi telah terstruktur berdasarkan Web Application Directory Structure maka web aplikasi siap digunakan oleh pengguna dan dipublikasikan.

D. Perancangan Perangkat Lunak

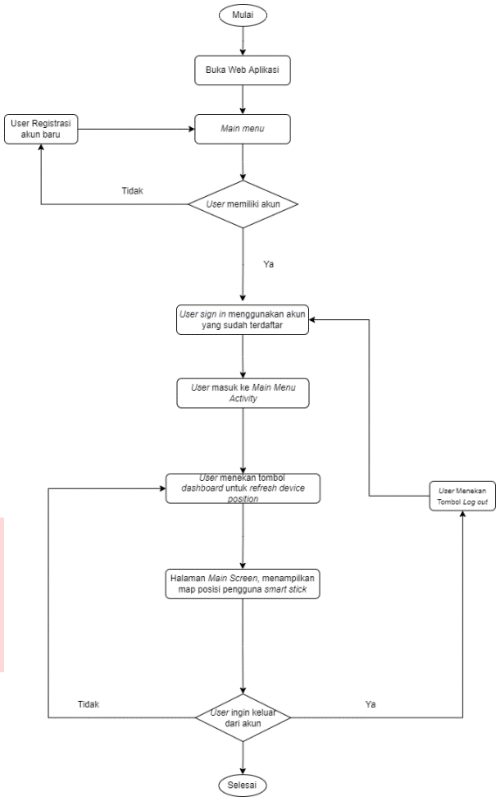
1. Usecase Diagram




GAMBAR 3.3.
USECASE DIAGRAM

Berdasarkan desain sistem pada gambar sebelumnya, diagram usecase pada Gambar 3.9 yang menggambarkan proses mendeteksi lokasi di aplikasi Discover-U memiliki 4 peran yaitu *User* 1, *User* 2, Firebase Database, MQTT *Cloud Server*. *User* 1 melakukan pairing device via *Bluetooth Low Energy* dan data tersebut di post ke dalam MQTT *Cloud server*, lalu data tersebut di ambil dan disimpan ke dalam *Local Computer* yang selanjutnya di deploy ke dalam Firebase. *User* 2 melakukan register dan login untuk melihat tampilan web aplikasi yang terdiri dari posisi pengguna yang data *user* tersebut telah tersimpan ke dalam Firebase.

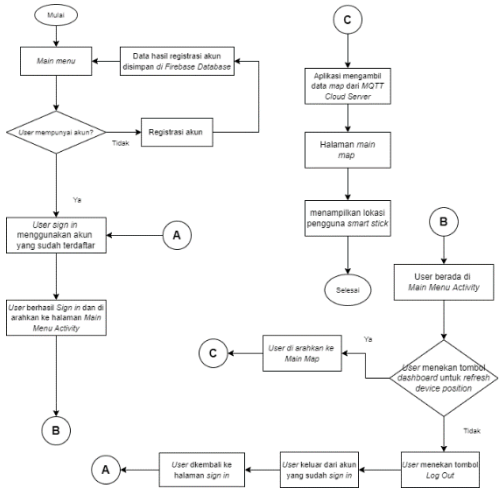
2. Activity Diagram




GAMBAR 3.4.
ACTIVITY DIAGRAM

Gambar 3.4 memperlihatkan bahwa aplikasi dimulai saat aplikasi dibuka pertama kali, Halaman awal akan muncul dengan meminta *user* login dan *user* masuk ke akun yang telah terdaftar. Lalu *user* akan diarahkan ke Main Screen Activity dengan data map yang telah terintegrasi dari MQTT Cloud server. Data tersebut disimpan ke dalam Local Computer dan di deploy ke dalam Firebase maka tampilan map akan muncul sesuai dengan data yang didapatkan dari MQTT Cloud Server.

3. Diagram Alir Proses Kerja Web Aplikasi

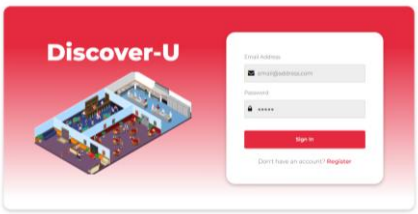



GAMBAR 3.5.
DIAGRAM ALIR PROSES KERJA WEB APLIKASI

Pada Gambar 3.11 dapat dilihat untuk proses kerja web aplikasi pertama dimulai saat *user* memiliki akun yang akan diarahkan ke proses Sign In dan jika tidak maka diarahkan untuk membuat akun terlebih dahulu yaitu ke kolom registrasi. Jika berhasil maka *user* akan diarahkan ke home screen aplikasi yang menjadi menu utama. *User* menekan tombol dashboard untuk me-refresh tampilan Web Aplikasi agar map dapat terlihat. Web Aplikasi mengambil data dari MQTT *Cloud Server* dan menempatkan data tersebut ke *Local Computer* dan data tersebut di deploy ke dalam Firebase. *User* juga dapat melakukan log out maka aktifitas dalam aplikasi akan terhenti saat user berhasil melakukan log out.

E. Desain *User Interface* (UI) Web Aplikasi

1. Login activity




GAMBAR 3.6.
LOGIN ACTIVITY

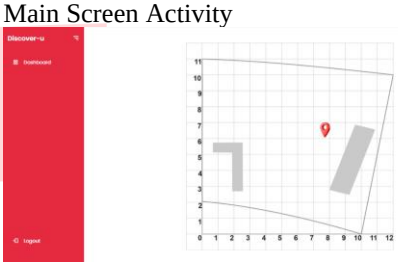
Login Activity merupakan proses ketika user memasukan email dan password dan melakukan otentikasi.

2. Register Activity


GAMBAR 3.7.
REGISTER ACTIVITY

Register Activity merupakan otentikasi jika user belum memiliki akun. Disini memasukan Nama, Email, dan Password, Age, Gender, dan Statement agree all agreement.

3. Main Screen Activity



GAMBAR 3.8.
MAIN SCREEN ACTIVITY

Main Screen Activity merupakan halaman utama dalam web aplikasi Discover-U, pada laman ini dapat terlihat lokasi dari pengguna *Smart Stick Indoor Localization* dengan teknologi BLE. Terdapat beberapa *icon* yaitu *Dashboard* yang bertujuan untuk me-*refresh* halaman dan juga Log Out

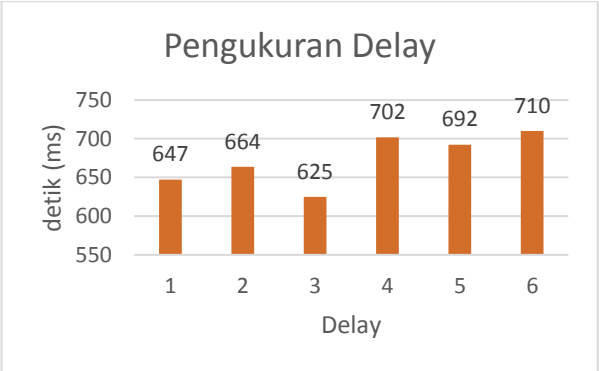
## IV. HASIL DAN PEMBAHASAN

Bab ini berisi hasil pengujian sistem yang telah dilakukan pada web aplikasi.

A. Hasil Pengujian Performansi Jaringan dengan Quality of Service

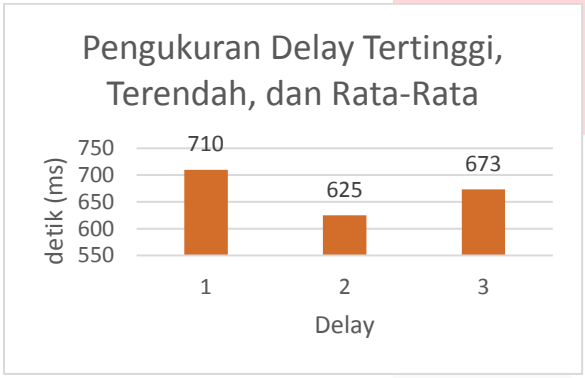
1. Hasil Pengujian Delay

a. Delay dari Server MQTT ke Local Computer



GAMBAR 4.1.
DELAY DARI SERVER MQTT KE LOCAL COMPUTER

Pengukuran delay dari Cloud Server ke Local Computer menggunakan software Wireshark. Jumlah pengujian 30 kali dengan dibagi menjadi 6 sesi dan 1 sesi terdiri dari 5 kali percobaan. Gambar 4.1 menunjukkan delay dari Cloud Server ke Local Computer. Dengan nilai pada sesi pertama, kedua, ketiga, keempat, kelima, dan keenam secara berurutan yaitu, 647 ms, 664 ms, 625 ms, 702 ms, 692 ms, dan 710 ms. Hasil pengujian 6 sesi ini terlihat tidak berbeda jauh dikarenakan waktu pengujian yang dilakukan sekitar pukul 21:00 WIB sampai 22:00 WIB dengan persesi memakan waktu kurang lebih 10 menit.

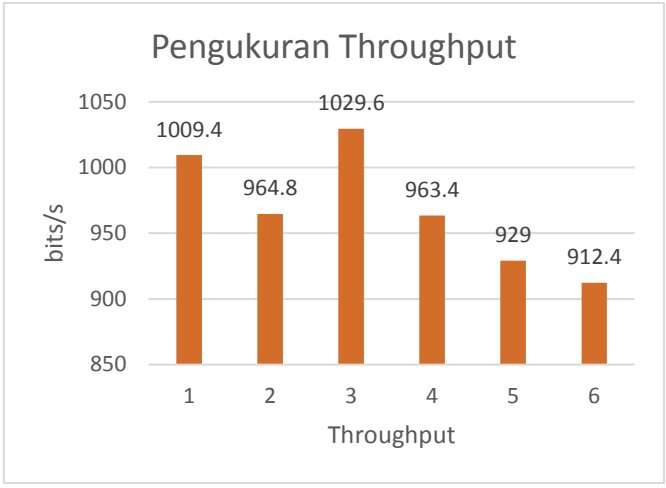



GAMBAR 4.2.
RATA-RATA DELAY DARI SERVER MQTT KE LOCAL COMPUTER

Pada gambar diatas hasil delay tertinggi, terendah, dan rata-rata secara berurutan bernilai 710 ms, 625 ms, dan 673 ms dan dapat diberi kesimpulan rata-rata delay yang diperoleh buruk dikarenakan banyak faktor seperti *storage delay* atau propagasi yaitu waktu yang diperlukan paket untuk mencapai tujuan.

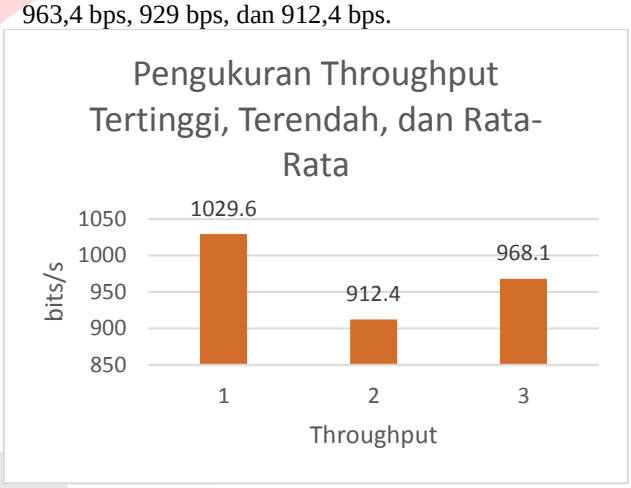
2. Hasil Pengujian Throughput

   a. Throughput dari Server MQTT ke Local Computer




GAMBAR 4.3.
THROUGHPUT DARI SERVER MQTT KE LOCAL COMPUTER

Pada gambar diatas menunjukan throughput dari MQTT ke Local Computer diperoleh nilai secara berurutan yaitu 1009,4 bps, 964,8 bps, 1029,6 bps, 963,4 bps, 929 bps, dan 912,4 bps.




GAMBAR 4.4.
RATA-RATA THROUGHPUT DARI SERVER MQTT KE LOCAL COMPUTER

Pengukuran Throughput juga dapat dilihat untuk nilai tertinggi, terendah, serta rata-rata yang diperoleh yaitu secara berurutan 1029,6 bits/s, 912,4 bits/s, dan 968,1 bits/s. Yang dapat disimpulkan bahwa nilai throughput dapat dikatakan baik karena packet yang dikirimkan juga hanya sedikit.

3. Hasil Pengujian Packet Loss

   a. Packet Loss dari Server MQTT ke Local Computer


GAMBAR 4.5.
PACKET LOSS DARI SERVER MQTT KE LOCAL COMPUTER

Dapat dilihat di gambar 4.9 bahwa paket yang diterima dari Server MQTT ke Local Computer mendapatkan hasil sebesar 100% dan tidak terjadi kehilangan paket pada proses pengiriman data tersebut.

B. Pengujian Performansi Keamanan dari Web Aplikasi

1. Hasil Pengujian Performansi Enkripsi AES

Pengujian performansi keamanan web aplikasi dilakukan dengan menguji *password* pada saat pengirimannya ke Firebase sudah terenkripsi dengan baik.

```
ciphertext: "hzxCnlrUFq2hw/V5TBwhTg=="
duration: 1
email: "cece@gmail.com"
method: "AES192"
plaintext: "CECE11"
```

GAMBAR 4.6.
PENGUJIAN MENGGUNAKAN AES-192

Hasil skenario pertama menggunakan enkripsi AES dapat dilihat pada gambar 4.6. Pengujian dengan enkripsi AES dengan memasukan email cece@gmail.com dan password CECE11 menghasilkan ciphertext yaitu hzxCnlrUFq2hw/V5TBwhTg==.

```
ciphertext: "CECE11"
duration: 0.10000014305114746
email: "cece@gmail.com"
method: "No Encryption"
plaintext: "CECE11"
```

GAMBAR 4.7.
PENGUJIAN TANPA MENGGUNAKAN ENKRIPSI

Dapat dilihat pada gambar 4.7 hasil skenario kedua tanpa menggunakan enkripsi AES dengan email dan password yang sama, setelah dikirimkan masih berupa plain text yaitu CECE11.

Penulis melakukan pengujian kebenaran hasil enkripsi AES-192 pada kalkulator AES online www.javainuse.com/aesgenerator dengan secret key 6CYYqT8cbFcWj7QW2VhjN37c dan initialization vector 7299238835873542.

TABEL 4.1.
HASIL ENKRIPSI YANG TERDAPAT PADA FIREBASE

| ***Secret Key*** | ***Initialization Vector*** | ***Plain Text*** | ***Cipher Text*** | ***Method*** |
|---|---|---|---|---|
| 6CYYqT8cbFcWj7QW2VhjN37c | 7299238835873540 | sFau7zrva | 8Y/qkOvNKU1qisHjHQOK2g== | AES 192 |
| | | YgkJGa22yDU | x/8sMEY2KWb+ZjaXsVVVKw== | AES 192 |
| | | eEcSsH84JJdvMMTVS | 8lVIiAXOfSxNP4iPaviltp9YVpfGcUHvX0hVSdy8jGE= | AES 192 |
| | | VkJQ9L4TTXpNbQV7j | Bl5Ldkfdme8r/Et3t+IqjdeA1n4GwX | AES 192 |

| | | | | |
|---|---|---|---|---|
| | | | 1+L4jtN Aykm2I = | |
| | | s4emwk 789e3rF LY2N MH5 | kapX3p6 ymS/l4+ ZzbfzU5l NrQ5N3 Abby+c RfN8Fvs q4= | AES 192 |

TABEL 4.2.
HASIL ENKRIPSI MENGGUNAKAN AES CALCULATOR

| *Secret Key* | *Initialization Vector* | *Plain Text* | *AES Calculator* | *Method* |
|---|---|---|---|---|
| 6CYYqT8 cbFcWj7Q W2VhjN3 7c | 72992 38835 87354 0 | sFau7zrv a | 8Y/qkO vNKU1q isHjHQ OK2g== | AES 192 |
| | | YgkJGa2 2yDU | x/8sME Y2KWb +ZjaXs VVVKw == | AES 192 |
| | | eEcSsH8 4JJdvM MTVS | 8lVIiAX OfSxNP 4iPaviltp 9YVpfG cUHvX0 hVSdy8j GE= | AES 192 |
| | | VkJQ9L 4TTXpN bQV7j | Bl5Ldkfd me8r/Et3t +IqjdeA1n 4GwX1+L 4jtNAykm 2I= | AES 192 |
| | | s4emwk 789e3rF LY2NM H5 | kapX3p6y mS/l4+Zz bfzU5lNr Q5N3Abb y+cRfN8F vsq4= | AES 192 |

Dari kedua tabel diatas tabel yaitu 4.1 dan 4.2 mempunyai kecocokan yang sama, maka dapat dibuktikan bahwa enkripsi yang dilakukan berhasil.

Lalu, penulis melakukan pengujian durasi dimana pengujian kali ini dilakukan sebanyak 20 kali pada setiap skenario yang dapat dilihat hasilnya pada tabel 4.3 dan 4.4

TABEL 4.1.
PENGUJIAN MENGGUNAKAN AES-192

| **Plain Text** | **Cipher Text** | **Method** | **Pass Length** | **Email** | **Duration** |
|---|---|---|---|---|---|
| 7QT 9t8q by | a3f81869 f43936a3 3be7a7f8 45a127d3 | AES 192 | 9 | cherilez1@gmail.com | 1.7999 999821 186066 |
| Lp9 AW Mrv p | 12e39ea6 f2b50080 dec4decf 0e999689 | AES 192 | 9 | cherilez2@gmail.com | 1.6999 999880 79071 |
| spYs wG6 Kk | c0090b71 2f9fa6d3 298d0eee 9ebad7cd | AES 192 | 9 | cherilez3@gmail.com | 2.6000 000238 41858 |
| 4Uz EYV dHN | ff6d0d14 556c8889 0d69942 b09721c1 a | AES 192 | 9 | cherilez4@gmail.com | 1.7999 999523 162842 |
| sFau 7zrv a | a8f1a03b 1e67eb97 69dbcaf0 47ff0f13 | AES 192 | 9 | cherilez9@gmail.com | 1.7000 000476 837158 |
| Fj6p hDA j59n | 1647033 475c6f25 d1f57aef 8e6d7336 b | AES 192 | 11 | cececici6@gmail.com | 1.8000 000119 20929 |
| 2crv Cy7d R2m | 0dc41a64 0a822276 36a108ca 9b35474 b | AES 192 | 11 | cececici7@gmail.com | 1.8000 000119 20929 |
| spD whR Lyj3 d | 9ec0d3ce dc43aa51 81eed2cd 58ebf57a | AES 192 | 11 | cececici8@gmail.com | 2 |
| YgkJ Ga22 yDU | d77cde17 7ec05229 923e1e9b 4abe5705 | AES 192 | 11 | cececici9@gmail.com | 1.6999 999880 79071 |
| Wyz eSR9 FE5g | 228a9e00 15b7237 37cfa0b2 5e99bdb4 9 | AES 192 | 11 | cececici10@gmail.com | 1.7999 999523 162842 |
| eEcS sH84 JJdv MM TVS | f78da101 c875e446 989071c1 68e555ac fde0346d b9b4ceff 20ad88bd 6a31a4a2 | AES 192 | 17 | ceceril6@gmail.com | 2.5 |
| 7zpG 9Vq 3VP Ec5e QbY | dfc153c7 7d1be02d ec7fb3e4 0142f02b c575222a e44f5182 8130e8e9 5ca4dc7c | AES 192 | 17 | ceceril7@gmail.com | 1.7000 000476 837158 |

| | | | | | |
|---|---|---|---|---|---|
| tb6BPEQk5PJdznrH2 | cbd3fadd9785536cf9061deb4bbe76cbc49e37849b52e643f8448a1bee26063d | AES 192 | 17 | ceceril8@gmail.com | 2.399999976158142 |
| a54FtPTRtmRGjUDZG | f97ce8c65ca4f4feef53fb0fdb1ae14958140d88ee484e1509cf4a81f4b4a039 | AES 192 | 17 | ceceril9@gmail.com | 1.800000011920929 |
| VkJQ9L4TTXpNbQV7j | 4d888b0d2881e6a7572400086355ae6d492ffb3f16a12b9b9cf74f23837dfc96 | AES 192 | 17 | ceceril10@gmail.com | 1.699999988079071 |
| s4emwk789e3rFLY2NMH5 | 6924d90f5f5ae0d9b717cef86084eb10e19bfb228adfdd01bb1253d656629930 | AES 192 | 20 | erlitacece6@gmail.com | 2.8 |
| bxBCvWWSW5a3VYUuegUc | 40a5fb43736db2cbd47e192c09dee1a4dcbb4e5932469f8600b4aacd734f9197 | AES 192 | 20 | erlitacece7@gmail.com | 1.699999988079071 |
| NmgwPrZ625Lg7SAGqDdk | 638b2d8f2e86872a12877060820cd45a49a266189f55d433ffc9e1d160b9a0f9 | AES 192 | 20 | erlitacece8@gmail.com | 1.899999976158142 |
| CQWGAM2cMmj2pZcN6Gqr | a222e49d64fe050abf208747ef3a70dcf5c36b7313eb6f0072d6ce4f1c40bb14 | AES 192 | 20 | erlitacece9@gmail.com | 1.900000035762786 9 |
| VxttvgfDNQeNPUc7hCuz | 2e5245b1984c140a91a156a4c1cd18071c93ec16b0a994633c25bc57af2c7a4b | AES 192 | 20 | erlitacece10@gmail.com | 1.899999976158142 |

TABEL 4.2
PENGUJIAN TANPA MENGGUNAKAN ENKRIPSI

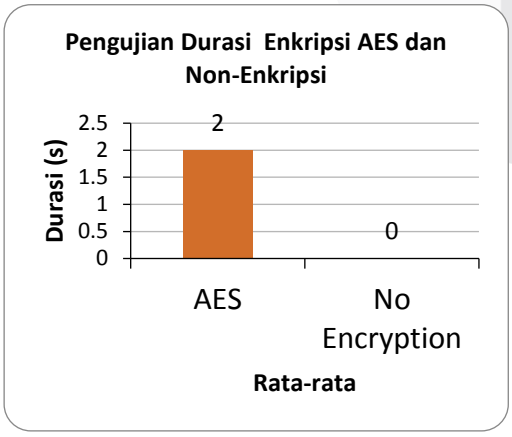
| Plain Text | Cipher Text | Method | Pass Length | Email | Duration |
|---|---|---|---|---|---|
| 7QT9t8qby | 7QT9t8qby | No Encryption | 9 | cherilez1@gmail.com | 0.10000002384185791 |
| Lp9AWMrvp | Lp9AWMrvp | No Encryption | 9 | cherilez2@gmail.com | 0.10000002384185791 |
| spYswG6Kk | spYswG6Kk | No Encryption | 9 | cherilez3@gmail.com | 0.19999998807907104 |
| 4UzEYVdHN | 4UzEYVdHN | No Encryption | 9 | cherilez4@gmail.com | 0 |
| sFau7zrva | sFau7zrva | No Encryption | 9 | cherilez9@gmail.com | 0 |
| Fj6phDAj59n | Fj6phDAj59n | No Encryption | 11 | cececici6@gmail.com | 0.10000002384185791 |
| 2crvCy7dR2m | 2crvCy7dR2m | No Encryption | 11 | cececici7@gmail.com | 0.29999995231628424 |
| spDwhRLyj3d | spDwhRLyj3d | No Encryption | 11 | cececici8@gmail.com | 0.19999998807907104 |
| YgkJGa22yDU | YgkJGa22yDU | No Encryption | 11 | cececici9@gmail.com | 0 |
| WyzeSR9FE5g | WyzeSR9FE5g | No Encryption | 11 | cececici10@gmail.com | 0.09999996423721313 |
| eEcSsH84JJdvMMTVS | eEcSsH84JJdvMMTVS | No Encryption | 17 | ceceril6@gmail.com | 0.09999996423721313 |
| 7zpG9Vq3VPEc5eQbY | 7zpG9Vq3VPEc5eQbY | No Encryption | 17 | ceceril7@gmail.com | 0 |
| tb6BPEQk5PJdznrH2 | tb6BPEQk5PJdznrH2 | No Encryption | 17 | ceceril8@gmail.com | 0.09999996423721313 |
| a54FtPTRtmRGjUDZG | a54FtPTRtmRGjUDZG | No Encryption | 17 | ceceril9@gmail.com | 0.09999996423721313 |
| VkJQ9L4TTXpNbQV7j | VkJQ9L4TTXpNbQV7j | No Encryption | 17 | ceceril10@gmail.com | 0.10 |
| s4emwk789e3rFLY2NMH5 | s4emwk789e3rFLY2NMH5 | No Encryption | 20 | erlitacece6@gmail.com | 0.10000002384185791 |
| bxBCvWWSW5a3VYUuegUc | bxBCvWWSW5a3VYUuegUc | No Encryption | 20 | erlitacece7@gmail.com | 0 |

| | | | | | |
|---|---|---|---|---|---|
| NmgwPrZ625Lg7SAGqDdk | NmgwPrZ625Lg7SAGqDdk | No Encryption | 20 | erlitacece8@gmail.com | 0.1000000238418579 1 |
| CQWGAM2cMmj2pZcN6Gqr | CQWGAM2cMmj2pZcN6Gqr | No Encryption | 20 | erlitacece9@gmail.com | 0.1000000238418579 1 |
| VxttvgfDNQeNPUc7hCuz | VxttvgfDNQeNPUc7hCuz | No Encryption | 20 | erlitacece10@gmail.com | 0.1999999880790710 4 |

Dapat diambil kesimpulan bahwa enkripsi AES sangat dibutuhkan untuk melindungi data *password* pengguna untuk mencegah terjadi pencurian atau pembobolan data.

2. Hasil Pengujian Waktu Pemrosesan Algoritma AES

Pada gambar 4.13 menunjukan data yang menggunakan enkripsi AES memiliki waktu yang lebih lama daripada yang tidak menggunakan enkripsi AES, hal ini disebabkan ketika memakai enkripsi AES terjadinya pemroresan putaran atau round, dalam pengujian kali ini penulis menggunakan AES-192 dengan memiliki 12 *round.* Semakin banyak bit yang dipakai maka semakin banyak *round* yang berlangsung, dan semakin lama juga waktu pemroresan data.




GAMBAR 4.8.
PENGUJIAN DIRASI ENKRIPSI AES DAN NON-ENKRIPSI

3. Hasil Analisis Performa AES-192 berdasarkan Avalanche Effect

Hasil analisis AES-192 untuk melihat tingkat keamanan ciphertext pada AES-192 menggunakan *Avalanche Effect*. Nilai-nilai yang didapatkan menggunakan aplikasi *Cryptool*.

TABEL 4.3
PENGUJIAN AVALANCHE EFFECT AES

| *Password* | | *AES Plaintext (in hex)* | *AES Key (in hex)* | *Nilai Avalanche Effect* |
|---|---|---|---|---|
| 4UzEYVdHN | *Plaintext 1* | **34 55 7A 45** 59 56 64 48 4E 00 00 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 47,70% |
| | *Modified plaintext 1* | 26 41 76 51 59 56 64 48 4E 00 00 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |
| sFau7zrva | *Plaintext 2* | **73 46 61 75 37 7A 72 76** 61 00 00 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 52,30% |
| | *Modified plaintext 2* | 7F 44 70 77 23 78 53 64 61 00 00 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |
| YgkJGa22yDU | *Plaintext 3* | **59 67 6B** 4A 47 61 32 32 79 44 55 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 50,80% |
| | *Modified plaintext 3* | 09 F7 43 4A 47 61 32 32 79 44 55 00 00 00 00 00 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |
| eEcSsH84JJdvMMTVS | *Plaintext 4* | **65 45 63 53 73 48 38 34 4A 4A 64 76** 4D 4D 54 56 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 46,10% |
| | *Modified plaintext 4* | 41 61 41 77 5B 6D 2C 3A 6C 5E 76 5E 4D 4D 54 56 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |
| VkJQ9L4TTXpNbQV7j | *Plaintext 5* | **56 6B 4A 51 39 4C** 34 54 54 58 70 4E 62 51 56 37 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 50% |

| | | | | |
|---|---|---|---|---|
| | *Modified plaintext 5* | 53 55 7B 15 1B 0E 34 54 54 58 70 4E 62 51 56 37 | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |
| s4emwk7 89e3rFL Y2NMH 5 | *Plaintext 6* | **73 34 65 6D 77 6B 37 38 39 65 33 72 46 4C 59 32** | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | 52,30% |
| | *Modified plaintext 6* | 5F 20 7D 7F 5F E3 13 08 11 77 7B 6A 0E 68 4D 1A | 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 | |

Dari tabel diatas dapat disimpulkan bahwa untuk pengujian AES-192 memiliki performa yang baik dari segi keamanan data karena nilai yang diperoleh berada di nilai yang baik yang itu sekitar 49,20% - 51,60%.

C. Hasil Pengujian Fungsionalitas Web Aplikasi

1. Pengujian User Experience

Pengujian User Experience pada Web Aplikasi dilakukan sebanyak 20 kali menggunakan metode *black-box testing*. Metode pengujian dimaksudkan untuk melihat fitur yang terdapat pada web aplikasi berjalan dengan baik agar *user* dapat merasakan *experience* yang baik dari sisi pengguna.

a. Dashboard Screen Activity

TABEL 4.4.
PENGUJIAN HALAMAN DASHBOARD MENU

| No. | Skenario Pengujian | Test Case | Hasil yang diharapkan | Hasil Pengujian |
|---|---|---|---|---|
| 1 | Menekan tombol Sign In | User masuk ke halaman utama | User berhasil menuju halaman Sign in | Berhasil |
| 2 | Menekan tombol Register | User masuk ke halaman register | User berhasil menuju halaman Register | Berhasil |

Tabel 4.4 merupakan hasil pengujian terhadap Dashboard Screen Activity yang memiliki 3 skenario pengujian diantaranya terdiri darimenekan tombol *sign in, register*. Pada skenario pengujian pertma yaitu menekan tombol *sign in* hasil pengujian menunjukan bahwa user dapat menuju halaman *sign in* serta dapat dikatakan pengujian skenario pertama berhasil. Skenario kedua yaitu menekan tombol *register* juga dapat dikatakan berhasil dikarenakan *user* mampu masuk ke halaman *register*.

b. Login Screen Activity

TABEL 4.5.
PENGUJIAN HALAMAN SIGN IN

| No. | Skenario Pengujian | Test Case | Hasil yang diharapkan | Hasil Pengujian |
|---|---|---|---|---|
| 1 | E-mail dan Password tidak diisi kemudian klik tombol *sign in* | -E-mail: (kosong) -Password: (kosong) | User tidak dapat masuk | Berhasil, Muncul *Please fill in this field* pada kotak yang kosong |
| 2 | Mengetikkan email dan password tidak di isi atau kosong kemudian klik tombol *sign in* | -E-mail: Cece@gmail.com -Password: (kosong) | User tidak dapat masuk | Berhasil, Muncul *Please fill in this field* pada kotak yang kosong |
| 3 | Mengetikkan password tidak sesuai, kemudian klik tombol *sign in* | -E-mail: Cece@gmail.com -Password: 12345678 | User tidak dapat masuk | Berhasil, muncul *the password is invalid or the user does not have a password.* |
| 4 | Mengetikkan Email tidak sesuai, kemudian klik tombol *sign in* | -E-mail: ceril@gmail.com -Password: cece11 | User tidak dapat masuk | Berhasil, muncul *there is no user record corresponding to this identifier. The user may have* |

| | | | | |
|---|---|---|---|---|
| | | | | *been deleted.* |
| 5 | Mengetikkan email dan password yang sesuai, kemudian klik tombol *sign in* | -E-mail: Cece@gmail.com -Password: cece11 | User berhasil masuk | Berhasil |

Tabel 4.5 merupakan hasil pengujian terhadap Login Screen Activity yang memiliki 5 skenario pengujian diantaranya terdiri dari dengan *E-mail* dan *Password* tidak diisi, mengetikkan *Email* dan *Password* tidak di isi atau kosong kemudian klik tombol *sign in*, mengetikkan *password* tidak sesuai, kemudian klik tombol *sign in*, mengetikkan *Email* tidak sesuai, kemudian klik tombol *sign in*, mengetikkan *email* dan *password* yang sesuai, kemudian klik tombol *sign in*.

TABEL 4.6.
PENGUJIAN HALAMAN REGISTER

| No. | Skenario Pengujian | Test Case | Hasil yang diharapkan | Hasil Pengujian |
|---|---|---|---|---|
| 1 | Tidak mengisi salah satu atau seluruh data | Mengosongkan salah satu atau seluruh data yang diminta | Sistem akan menolak dan memberikan pesan untuk mengisi data yang kosong | Berhasil, Muncul *Please fill in this field* pada kotak yang kosong |
| 2 | Menggunakan alamat e-mail yang telah terdaftar | Memasukkan e-mail yang telah didaftarkan sebelumnya pada kolom e-mail | Sistem akan menolak dan memberikan pesan bahwa e-mail tersebut telah digunakan | Berhasil, muncul *the email address is already in use by another account.*. |
| 3 | Menggunakan alamat email yang tidak sesuai format | Memasukkan alamat email yang tidak sesuai dengan format email dengan tidak menggunakan format '@' | Sistem akan menolak dan memberikan pesan untuk memasukkan format email yang benar | Berhasil |
| 4 | Memasukkan seluruh data dengan benar | Memasukkan seluruh data sesuai yang diminta dengan benar | Sistem menerima registrasi dan kemudian menampilkan halaman login | Berhasil |

Tabel 4.6 merupakan hasil pengujian terhadap *Register Screen Activity* yang memiliki 4 skenario pengujian diantaranya terdiri dari dengan skenario pertama yaitu tidak mengisi salah satu atau seluruh data, skenario kedua menggunakan alamat e-mail yang telah terdaftar, skenario ketiga enggunakan alamat email yang tidak sesuai format, dan skenario keempat memasukkan seluruh data dengan benar.

c. Main Screen Activity

TABEL 4.7.
PENGUJIAN MAIN SCREEN

| No. | Skenario Pengujian | Test Case | Hasil yang diharapkan | Hasil Pengujian |
|---|---|---|---|---|
| 1 | Menekan tombol Dashboard | Menekan tombol Dashboard | Halaman ter-refresh | Berhasil |

| | | | | |
|---|---|---|---|---|
| 2 | Menekan tombol Log out | Menekan tombol Log out | Halaman kembali ke menu Log In | Berhasil |

Tabel 4.7 merupakan hasil pengujian terhadap *Main Screen Activity* yang memiliki 2 skenario pengujian diantaranya terdiri dari dengan skenario pertama yaitu menekan tombol *dashboard* dan menekan tombol *log out*. Skenario pertama didapatkan hasil yang sesuai dengan halaman berhasil ter-refresh ketika menekan tombol *dashboard* serta pengujian kedua juga menunjukan hasil yang baik saat user *user* menekan tombol *Log Out* maka halaman kembali ke halaman awal yaitu *Log In Screen.*

## V. KESIMPULAN

Berdasarkan pada hasil pengujian dan analisis pada perancangan sistem Web Aplikasi Discover-U yang telah dilakukan dapat ditarik kesimpulan sebagai berikut:

1. Penelitian tugas akhir mendesain dan mengimplementasikan pemetaan lokasi pada web aplikasi Discover-U dengan menampilkan posisi pengguna smart stick dengan datanya disimpan ke dalam Local Computer yang diambil dari MQTT Cloud Server dan di deploy ke dalam Firebase untuk menjadi Web Aplikasi.
2. Waktu Enkripsi data user yaitu password menggunakan AES-192 bit dan waktu yang diperlukan jika tidak menggunakan enkripsi apapun pada web aplikasi berhasil dilakukan dengan rata-rata waktu 2 s untuk yang menggunakan enkripsi dan 0 s untuk yang tidak menggunakan enkripsi.
3. Hasil pengukuran Quality of Service dari Cloud Server MQTT ke Local Computer memiliki delay rata-rata 673 ms, throughput 968,1 bps, dan packet loss 0% serta dari Cloud Server Firebase ke Web Aplikasi memiliki delay rata-rata 37 ms, throughput 190 bits/s dan packet loss 0%
4. Web Aplikasi berhasil mengenkripsi data user dan enkripsi yang digunakan yaitu AES-192 dapat dikatakan baik menurut penguian Avalanche Effect
5. Fungsionalitas web aplikasi melalui pengujian user experience dengan metode black-box telah memenuhi hasil yang diharapkan dengan hasil yang memenuhi standar pengujian yaitu 100%.

## REFERENSI

[1] A. Aryaseno, R. H. Ginardi dan F. Baskoro, “Perancangan Indoor Localization Menggunakan Bluetooth Untuk Pelacakan Posisi Benda di Dalam Ruangan,” JURNAL TEKNIK ITS, vol. V, pp. A326-A330, 2016.

[2] R. Faragher and R. Harle, "An Analysis of the Accuracy of Bluetooth Low Energy for Indoor Positioning Applications," Proc. 27th Int. Tech. Meet. Satell. Div. Inst. Navig. (ION GNSS+ 2014), pp. 201-210, 9 April 2014.

[3] Y. Yusfrizal, A. Meizar, H. Kurniawan and F. Agustin, "Key Management Using Combination of Diffie–Hellman Key Exchange with AES Encryption," The 6th International Conference on Cyber and IT Service Management (CITSM 2018), 2018.

[4] T. T. Khanh, . V. Nguyen, X. Pham and E. Huh, "Wi Fi indoor positioning and navigation: a cloudlet based cloud computing approach," Khanh et al. Hum. Cent. Comput. Inf. Sci, vol. 10:32, pp. 1-26, 2020.

[5] B. Rizaldi, D. S. Pambudi and T. Bariyah, "IMPLEMENTASI TEKNOLOGI BLUETOOTH LOW ENERGY DAN METODE TRILATERASI UNTUK PENCARIAN RUTE INDOOR," Jurnal Ilmiah Teknologi Informasi, vol. 18, no. 2, pp. 57-67, 2020.

[6] W.-J. Li, C. Yen, Y.-S. Lin, S.-C. Tung and S. Huang, "JustIoT Internet of Things based on the Firebase Real-time Database," in IEEE International Conference on Smart Manufacturing, Industrial & Logistics Engineering (SMILE) , Hsinchu, 2018.

[7] S. M. Wadi and N. Zainal, "High Definition Image Encryption Algorithm Based on AES Modification," Wireless Pers Commun, no. 79, p. 811–829, 2014.

[8] H. Poston and K. Dhandhania, "The Advanced Encryption Standard (AES) Algorithm," Learn Cryptography: From Beginner to Expert, 2016. [Online]. Available: https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5. [Accessed 9 November 2021].

[9] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET (STUDI KASUS : UPT LOKA UJI TEKNIK PENAMBANGAN JAMPANG KULON – LIPI)," Jurnal Teknik Informatika dan Sistem Informasi, vol. II, no. 2, pp. 162-172, 2016.