Rancang Bangun Aplikasi *Discover-U* Berbasis Android dengan Algoritma *Advanced Encryption Standard* (AES) untuk Pemetaan Lokasi Dalam Ruangan Menggunakan *Bluetooth Low Energy*

1st Dikry Ikhwanuddin
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
dikryikhwanuddin@student.telkomuniversity.ac.id

2nd Eng Favian Dewanta
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
favian@telkomuniversity.ac.id

3rd Sussi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sussiss@telkomuniversity.ac.id

Abstrak–Teknologi informasi pelacakan lokasi sangat dibutuhkan pada perkembangan teknologi sekarang, pelacakan lokasi yang digunakan saat ini adalah *Global Positioning System* (GPS). Namun, sinyal GPS sulit untuk melacak dan menangkap sebuah lokasi yang berada di dalam ruangan, oleh karena itu di ciptakanlah teknologi bernama *Indoor Localization System* untuk pelacakan lokasi di dalam ruangan, teknologi yang dipakai untuk *indoor localization* ini menggunakan teknologi *Bluetooth Low Energy* (BLE).Pada penelitian ini, akan membuat desain dan implementasi pemetaan lokasi dalam ruangan berbentuk aplikasi berbasiskan operasi sistem android yang diberi nama "*Discover-U*". Aplikasi *Discover-U* menerapkan algoritma enksripsi data *Advanced Encryption Standard* (AES) untuk menjaga keamanan data pengguna. Hasil pengujian fungsionalitas untuk aplikasi Discover-U menunjukan bahwa aplikasi berjalan dengan baik. Hasil pengujian *Quality of Service* dari aplikasi *Discover-U* didapat dengan rata-rata *delay* 602ms, *throughput* sebesar 1,214 Kbps, dan *packet loss* sebesar 0%. Adapun hasil pengujian hasil *chiptertext* AES-192 dapat bekerja dengan baik, pengujian tingkat keamanan dengan *Avalanche effect* dengan rata-rata 55%, dan rata-rata *running time proses* enkripsi AES-192 adalah 0,002s.

Kata kunci : Android, *Indoor Localization System*, *Bluetooth Low Energy*, *Internet of Things*, AES, MQTT, *Cloud Server*.

Abstract–Location tracking information technology is very much needed in today's technological developments, the location tracking used today is the Global Positioning System (GPS). However, the GPS signal is difficult to track and capture a location that is indoors, therefore a technology called the Indoor Localization System was created for indoor location tracking, the technology used for indoor localization uses Bluetooth Low Energy (BLE) technology.In this final project, we will design and implement an indoor location mapping in the form of an application based on the android operating system, named "Discover-U". The Discover-U application applies the Advanced Encryption Standard (AES) data encryption algorithm to keep user data safe. The results of functionality testing for the Discover-U application show that the application runs well. Quality of Service test results from the Discover-U application are obtained with an average delay of 602ms, throughput of 1.214 Kbps, and packet loss of 0%. The results of testing the results of the AES-192 chipter text can work well, testing the security level with the Avalanche effect with an average of 55%, and the average running time of the AES-192 encryption process is 0.002s.

Keywords: Android, Indoor Localization System, Bluetooth Low Energy, Internet of Things, AES, MQTT, Cloud Server.

I. PENDAHULUAN

Pemberian fisik sempurna merupakan anugrah dari Tuhan yang sangat berharga. Dengan memiliki penglihatan dan tubuh yang masih normal manusia dapat melakukan aktifitasnya dengan lancar. Seseorang yang memiliki fisik kurang sempurna atau mengalami penurunan fungsi tubuh seperti lansia atau orang tua tidak dapat melakukan aktifitasnya secara mandiri. Walaupun mempunyai kekurangan dalam hal tersebut, mereka masih bisa beraktifitas, meskipun terkadang harus dibantu dengan sebuah alat untuk memperlancar pergerakannya yaitu biasanya tongkat.

Teknologi pelacakan lokasi adalah teknologi yang banyak digunakan untuk kebutuhan sehari-hari, seperti dapat mengidentifikasi lokasi saat ini atau mencari alamat[1]. Teknologi yang banyak di gunakan untuk menunjukan lokasi adalah *Global Positioning System* (GPS). Teknologi GPS membuat navigasi pada kasus di luar ruangan saat ini sangat canggih, namun teknologi GPS kurang akurat, terutama untuk pendeteksian posisi dalam ruangan [2].

Pada penelitian sebelumnya yang dilakukan oleh Afzar Fikri Reza telah dilakukan penelitian mengenai teknologi Positioning system dengan konsep *indoor localization* menggukan protokol *bluetooth low energy* (BLE), Dalam penelitiannya dilakukan simulasi navigasi

menggunakan algoritma *trilateration*, serta melakukan pengukuran akurasi dari BLE [3].

Dengan adanya penelitian sebelumnya, penelitian ini dapat dikembangkan sebuah inovasi membuat sebuah aplikasi berbasis android bernama "*Discover-U*" yang dapat menampilkan keberadaan posisi pengguna *smart stick*. Untuk menjamin keamanan data pengguna dapat dilakukan dengan cara enkripsi. Metode enkripsi yang digunakan adalah algoritma AES, digunakan saat pengguna aplikasi android melakukan registrasi akun. Metode AES berlaku untuk layanan aplikasi berbasis android, terutama dalam proses otentikasi dan melindungi

ID password pengguna disimpan di penyimpanan *firebase*.

II. KAJIAN TEORI

A. Aplikasi *Discover-U* Pelacak Lokasi Dalam Ruangan

Aplikasi *Discover-U* merupakan aplikasi berbasis android yang dibuat dapat menyambungkan pengguna *smart stick bluetooth low energy* (BLE) dengan aplikasi ini. Pengguna aplikasi *Discover-U* dapat memantau keberadaan posisi pengguna *smart* stick BLE. Dengan adanya aplikasi ini diharapkan dapat membantu mengurangi kekhawatiran keluarga atau kerabat terdekat pengguna *smart stick* saat mereka sedang berjalan mandiri di dalam ruangan yang besar.

B. Internet of Things

Internet of things (IoT) adalah sebuah sistem perangkat komputasi yang saling terkait, mengidentifikasi berbagai objek seperti hewan, tumbuhan, dan manusia, dengan kemampuan mentransfer data melalui jaringan tanpa memerlukan manusia untuk mentransfer datanya. Menurut Deepak (2020), *Internet of Things* adalah teknologi yang cukup menarik, teknologi ini mengambil semua hal fisik dan semua pemikiran yang ada di dunia dengan menghubungkannya ke internet[4].

C. Indoor Positioning Systems dan Indoor Localization

Indoor Positioning Systems (IPS) adalah seperangkat solusi perangkat keras dan lunak yang memungkinkan mengijinkan pendeteksian lokasi objek atau manusia yang berada di dalam ruangan. *Indoor Localization* merupakan layanan untuk menentukan posisi seseorang atau benda yang berada di dalam sebuah ruangan atau gedung. Secara konsep penerapan sama seperti *indoor positioning*, akan tetapi memiliki perbedaan dalam hal penentuan posisi. *Indoor Localization* menggunakan kordinat relatif sedangkan *indoor Positioning* menggunkan kordinat Global [5][6].

D. Bluetooth Low Energy

Bluetooth adalah suatu teknologi *wireless* berstandar PAN digunakan untuk pertukan data antara perangkat *mobile* atau *fixed* dengan jarak yang cukup dekat. *Bluetooth* beroprasi dalam frekuensi 2.4GHz band, *Bluetoth low Energy* merupakan teknologi hasil dari perkembangan *Bluetooth Classic* yang ditujukan untuk protokol IoT. *Bluetoth low Energy* adalah protokol terbaru yang mengoptimalkan kinerja *bluetooth* dalam aspek efektivitas penggunaan daya pada *device*, kestabilan transfer data, kompatibilitas dengan berbagai perangkat, dan jangkauan sinyal yang jauh daripada bluetooth classic[7][8].

E. Sistem Operasi Android

Sistem Operasi perangkat *mobile* adalah suatu sistem operasi yang bisa mengontrol sistem dan kinerja pada barang elektronik. Sistem Operasi Android merupakan

platform perangkat lunak dan sistem operasi berbasis Linux untuk perangkat seluler seperti *smartphone* dan tablet yang bersifat *open source* dengan Lisensi *Apache*. Kelebihan android dibandingkan dengan OS serupa ialah sistem operasi yang *Open Source, Cloud Storage, Large community, Easier Program Instalation*, *User Friendly* dan lain-lain [9].

F. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi untuk pengamanan data. AES merupakan blok *chipertext* yang dapat mengenkripsi (*encipher*) dan deskripsi (*decipher*) informasi. Enkripsi sendiri merupakan proses penyandian *plaintext* menjadi *chipertext*, atau pengubahan data menjadi bentuk rahasia. Algoritma AES memiliki kunci kriptografi 128, 192, dan 256 bits dengan kunci blok asli 128 bit [10].

G. MQTT

Message Queuing Telemetry Transport (MQTT) adalah protokol pesan berbasis *publish/subscribe* yang ringan dan sederhana, dirancang secara terbuka dan mudah untuk diimplementasikan di berbagai perangkat IoT. MQTT menggunkan *bandwidth* jaringan sedikit dan menggunkan sumber daya perangkat yang sangat kecil.

H. Firebase

Firebase merupakan layanan *web service* dari *Google* dengan menyediakan layanyan *database* dalam pengembangan aplikasi atau *web* dan berfungsi untuk menyimpan data aplikasi atau *device* ke *cloud server*. *Firebase* merupakan platform untuk aplikasi *realtime*. Ketika data berubah, maka aplikasi yang terhubung dengan firebase akan meng-update secara langsung melalui setiap device (perangkat) baik *website* ataupun *mobile* [11].

III. METODE

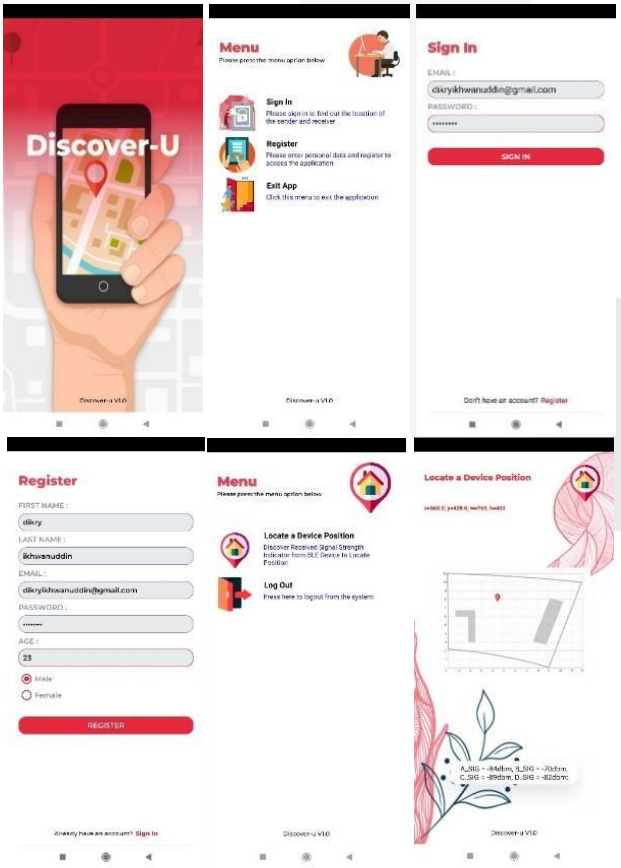
A. Desain Sistem

GAMBAR 1
DESAIN SISTEM APLIKASI ANDROID

Gambar 1 menjelaskan aplikasi *Discover-U* dapat bekerja ketika mikrokontroler ESP32 yang berada di *smart stick* memberikan input data yaitu lokasi pengguna *smart stick* kepada MQTT *server*, proses ini dinamakan *Publish*/*Publisher* data ke server MQTT. Selain input berupa lokasi pengguna *smart stick*, aplikasi *Discover-U* bertindak sebagai *Subscribe* dengan merequest pesan (*topic*) berupa data lokasi pengguna *smart stick* kepada MQTT *Server*. Ketika pengguna menggunakan aplikasi *Discover-U*, data pengguna aplikasi *Discover-U* sudah diamankan oleh algroritma enkripsi AES, data lokasi pengguna *smart stick* akan terlihat pada map di aplikasi *Discover-U*, dan data pengguna aplikasi *Discover-U* akan tersimpan di *Firebase database*.

B. Desain Perangkat Lunak

a. Desain User Interface Aplikasi Android



GAMBAR 2
USER INTERFACE APLIKASI *DISCOVER-U*

Gambar 2 menunjukan hasil desain *user interface* yang di terapkan dalam aplikasi *Discover-U* yang terdiri dari *Splash Screen*, *Main Menu*, *Sign in*, *Register*, *User Menu*, dan *Map Screen*. *Splash Screen* merupakan aktivitas pertama yang muncul setelah user menjalankan aplikasi android *Discover-U*. *sign in screen* merupakan proses untuk autentikasi user dengan memasukan *email* dan *password user*. *Register screen* merupakan proses autentikasi pengguna jika belum mempunyai akun, di *register screen* ini pengguna memasukan nama, *email*, *password*, umur dan gender. Setelah mengisi form *register* di atas maka user menekan tombol Register kemudian menekan tombol *Sign in* untuk pergi ke *screen sign in*.

User Menu merupakan tahapan setelah user melakukan *log in* di aplikasi, kemudian user memilih *Locate Position* untuk pergi ke *map screen* , atau *Log Out* untuk kembali ke *Menu Activity*. *Map Screen* merupakan halaman utama dalam aplikasi android *Discover-U*, pada *map screen* ini user dapat melihat lokasi dari pengguna *smart stick*.

IV. HASIL DAN PEMBAHASAN

A. Hasil pengujian Fungsionalitas

TABEL 1
PENGUJIAN *SPLASH SCREEN ACTIVITY*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian
1	Klik icon aplikasi *Discover-U*	Klik icon aplikasi *Discover-U*	Aplikasi berhasil dimulai dengan *Splash Screen*.	Sesuai harapan

Tabel 1 merupakan pengujian terhadap *Splash Screen Activity* dimulai dari saat user mengklik icon aplikasi *Discover-U* dan melihat hasilnya apakah sesuai dengan yang di harapkan. Dari hasil pengujian *Splash Screen activity* menunjukan hasil yang di dapat sudah sesusi harapan dengan mengklik ikon aplikasi maka aplikasi akan terbuka dan dimalui dengan *Splash Screen*, dengan demikian *user interface* dari *Splash Screen* sudah berfungsi dengan baik.

TABEL 2
PENGUJIAN HALAMAN *MAIN MENU*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian
1	Masuk ke halaman *Sign In*	Menekan tombol *Sign In*	Menuju halaman Sign in	Sesuai harapan
2	Masuk ke halaman *Register*	Menekan tombol *Register*	Menuju halaman Register	Sesuai harapan
3	Keluar dari aplikasi	Menekan tombol *Exit App*	Keluar dari aplikasi	Sesuai harapan

Tabel 2 menunjukan hasil pengujian terhadap *Main Menu Activity* dapat di lihat dari tabel di atas yang menunjukan hasil yang sudah sesuai dengan yang di harapkan pengguna yaitu ketika mengklik *button Sign In* maka pengguna akan di arahkan ke *menu Sign In*, ketika mengklik *button Register* maka pengguna akan di arahkan ke menu *Register*, dan ketika mengklik *button Exit App* maka pengguna akan keluar dari aplikasi *Discover-U*.

TABEL 3
PENGUJIAN HALAMAN REGISTRASI

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	Sesuai harapan
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	Sesuai harapan
3	Menggunakan alamat email yang tidak sesuai format	Memasukkan alamat email yang tidak sesuai dengan format *e-mail*	Sistem akan menolak dan memberikan pesan untuk memasukkan format *e-mail* yang benar	Sesuai harapan
4	Memasukkan seluruh data dengan benar	Memasukkan seluruh data sesuai yang diminta dengan benar	Sistem menerima registrasi dan kemudian menampi	Sesuai harapan

			lkan halaman *Menu Utama*	
5	Masuk ke halaman *Sign In*	Menekan tombol *Sign In*	Menuju halaman *Sign in*	Sesuai harapan

Tabel 3 merupakan hasil pengujian fungsionalitas terhadap *Register Activity*, Pengujian halaman *Register Activity* ini dilakukan dengan 5 skenario pengujian, skenario pengujian ini diberikan skenario Register berhasil dan skenario Register gagal. Skenario berhasil jika pengguna memasukan seluruh data sesuai yang di minta dengan benar, dan skenario gagal ketika pengguna mengosongkan data yang di minta dan memasukan data yang tidak sesuai format. Dari pengujian diatas dilihat dari setiap skenario pengujian berhasil maupun gagal menunjukan hasil yang sudah sesui dengan apa yang di harapkan. Hal ini menunjukan bahwa *user interface* dari *Register Activity* sudah berfungsi dengan baik.

TABEL 4
PENGUJIAN HALAMAN *SIGN IN*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian
1	E-mail dan Password tidak diisi kemudian klik tombol masuk	*-E-mail:* (kosong) *-Password:* (kosong)	Sistem akan menolak dan memberikan pesan user dan password tidak terdaftar di sistem	Sesuai harapan
2	Mengetikkan email dan password tidak di isi atau kosong kemudian klik tombol masuk	*-E-mail:* Dikry@gmail.com *-Password:* (kosong)	Sistem akan menolak dan memberikan pesan user dan password tidak terdaftar di sistem	Sesuai harapan
3	Mengetikkan email dan/atau password tidak sesuai, kemudian klik tombol masuk	*-E-mail:* Dikry@gmail.com *-Password:* 123454321	Sistem akan menolak dan memberikan pesan user dan password tidak terdaftar di sistem	Sesuai harapan
4	Mengetikkan email dan password yang sesuai, kemudian klik tombol masuk	*-E-mail:* Dikry@gmail.com *-Password:* 12345Dikri	Sistem menerima Sign in dan kemudian menampilkan halaman user menu	Sesuai harapan
5	Masuk ke halaman *Sign In*	Menekan tombol *Sign In*	Menuju halaman *User*	Sesuai harapan

			Menu Activity	

Tabel 4 menunjukan hasil pengujian dari fungsionalitas terhadap *Sign In Activity*, Pengujian halaman *Sign In Activity* ini dilakukan dengan 5 skenario pengujian, skenario pengujian ini diberikan skenario *Sign In* berhasil dan skenario *Sign In* gagal. Skenario berhasil jika pengguna memasukan seluruh data sesuai yang di minta dengan benar, dan skenario gagal ketika pengguna mengosongkan data yang di minta dan memasukan data yang tidak sesuai format. Dari pengujian diatas dilihat dari setiap skenario pengujian berhasil maupun gagal menunjukan hasil yang sudah sesui dengan apa yang di harapkan. Hal ini menunjukan bahwa user interface dari *Sign In Activity* sudah berfungsi dengan baik.

TABEL 5
PENGUJIAN HALAMAN *USER MENU*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian
1	Masuk ke halaman pemetaan lokasi	Menekan tombol *Locate a Device Position*	Menuju halaman pemetaan lokasi	Sesuai harapan
2	Keluar dari akun yang sudah *Sign In*	Menekan tombol *Log out*	Kembali ke halaman *Sign In*	Sesuai harapan

Tabel 5 menunjukan hasil pengujian fungsionalitas terhadap *User Menu* dapat di lihat dari tabel di atas yang menunjukan hasil yang sudah sesuai dengan yang di harapkan pengguna yaitu ketika mengklik button *Locate a Device Position* maka pengguna akan di arahkan ke menu *Map Screen* untuk melihat lokasi pengguna *smart stick*, ketika mengklik *button Log out* maka pengguna akan di arahkan kembali ke halaman Sign in.

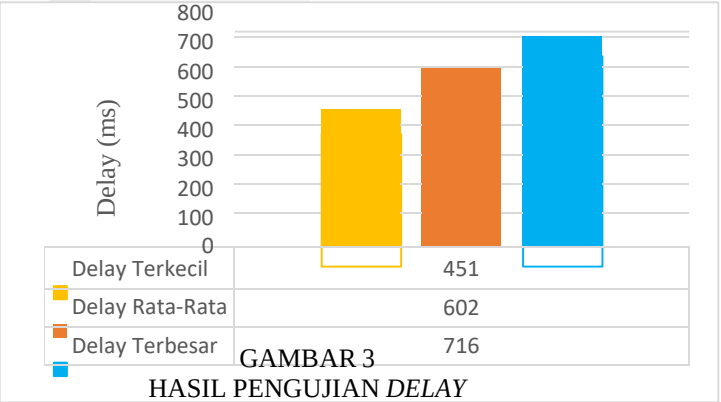
TABEL 6
PENGUJIAN HALAMAN *MAP SCREEN*

No.	Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian
1	Menampilkan hasil dari pemetaan lokasi	Menampilkan map dan menggerakan titik lokasi	Titik lokasi dalam map berpindah-pindah	Sesuai harapan

Tabel 6 menunjukan hasil dari pengujian *Map Screen*. Dapat disimpulkan bahwa pada halaman *Map Screen* ini dapat berjalan sesuai dengan apa yang diharapkan dan aplikasi dapat menampilkan map lokasi dari pengguna *smart stick*. Berdasarkan tabel pengujian *black box* di atas. Dapat disimpulkan bahwa aplikasi yang dibuat dapat berjalan sesuai dengan apa yang diharapkan dan dapat digunakan dengan baik.

B. Hasil Pengujian Performansi Jaringan dengan Quality of Service

a. Hasil Pengujian Delay

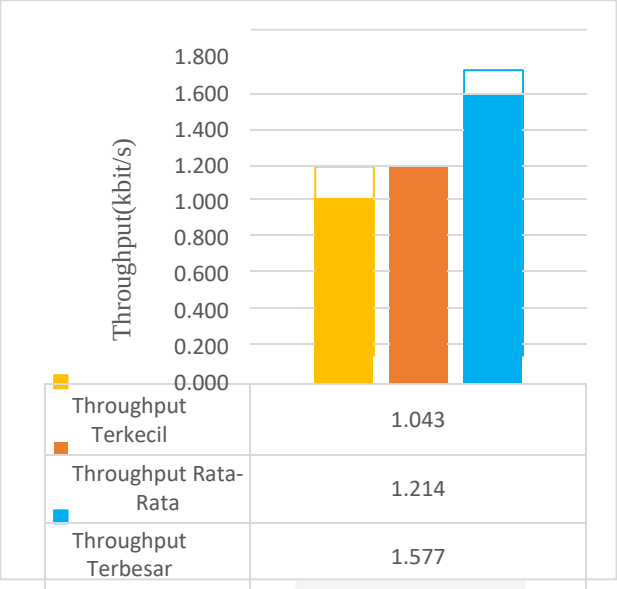


GAMBAR 3
HASIL PENGUJIAN *DELAY*

Gambar 3 merupakan hasil pengujian *delay* dengan skenario pengiriman data dari aplikasi android ke server menggunakan *software* Wireshark dengan mem-filter paket data dari Aplikasi Android dan Server. Jumlah pengujian *delay* ini dilakukan sebanyak 60 kali. Dapat

dilihat dari Gambar 3 untuk nilai *delay* pengiriman data dari aplikasi *Android* ke *Server* dari nilai *delay* terkecil, nilai *delay* rata-rata, dan nilai *delay* terbesar secara berurutan 451ms, 602ms, dan 716ms. Pengujian delay ini menggunakan sistem 2 sesi, dimana sesi pengujian ke 1 dilakukan malam hari pada jam 22.00-02.00 WIB dilakukan pengujian sebanyak 30x, dan sesi pengujian ke 2 dilakukan sore hari pada jam 16.00-19.00 WIB dilakukan pengujian sebanyak 30x total pengujian keseluruhan adalah 60x.

b. Hasil Pengujian Throughput

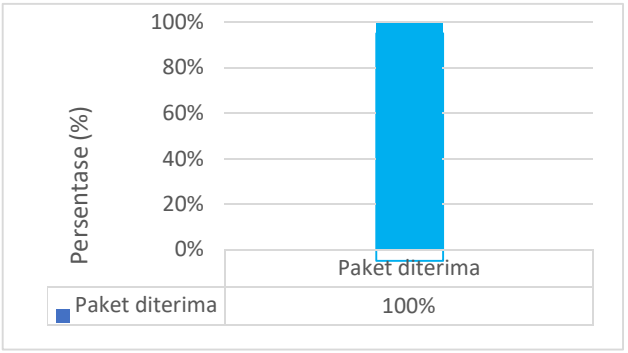


GAMBAR 4

HASIL PENGUJIAN *THROUGHPUT*

Gambar 4 merupakan hasil pengujian *throughput* menggunakan *software* Wireshark dengan mem-filter paket data dari Aplikasi Android dan Server. Jumlah pengujian *throughput* ini dilakukan sebanyak 60 kali. Dapat dilihat dari Gambar 4 untuk nilai *throughput* Aplikasi Android ke server MQTT dari nilai *throughput* terkecil, nilai *throughput* rata-rata, dan nilai *throughput* terbesar secara berurutan 1,043Kbps, 1,214Kbps, dan 1,577Kbps. Pengujian *throughput* ini menggunakan sistem 2 sesi, dimana sesi pengujian ke 1 dilakukan malam hari pada jam 22.00-02.00 WIB dilakukan pengujian sebanyak 30x, dan sesi pengujian ke 2 dilakukan sore hari pada jam 16.00-19.00 WIB dilakukan pengujian sebanyak 30x total pengujian keseluruhan adalah 60x.

c. Hasil Pengujian Packet Loss



GAMBAR 5
HASIL PENGUJIAN *PACKET LOSS*

Dapat dilihat dari Gambar 5 bahwa jumlah paket yang berhasil dikirim dari sisi *Server* ke Aplikasi Android memiliki nilai sebesar 100%. Hal ini menandakan banyaknya paket yang hilang (*packet loss*) selama proses pengiriman data ke tujuan sebesar 0%. Jumlah *packet loss* 0% dalam sistem yang dibuat memiliki performansi yang sangat baik dengan menggunkan jaringan Wi-Fi. Pengujian *packet loss* ini menggunakan sistem 2 sesi, dimana sesi pengujian ke 1 dilakukan malam hari pada jam 22.00-02.00 WIB dilakukan pengujian sebanyak 30x, dan sesi pengujian ke 2 dilakukan sore hari pada jam 16.00-19.00 WIB dilakukan pengujian sebanyak 30x total pengujian keseluruhan adalah 60x. Berdasarkan nilai standar pada ITU-TG nilai *packet loss* sudah sesuai dengan standar yaitu 0% *packet loss*[12].

C. Pengujian Hasil Ciphertext

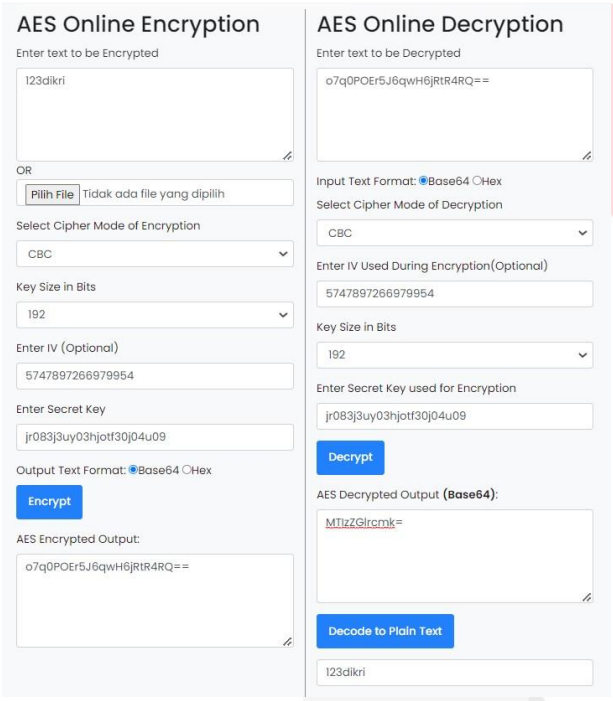
TABEL 7
HASIL ENKRIPSI PASSWORD MENJADI *CIPHERTEXT*

E-mail	Password	Hasil enkripsi
DikryId@gmail.com	123dikri	o7q0POEr5J6qwH6jRtR4RQ==
Dikry01@gmail.com	6a)F[f	ClYVQ2fbYtYrlEOwTMYkDQ==
Dikry02@gmail.com	"7X:w0	sgXPoomDEGMpP2/qKFOcfw==
Dikry05@gmail.com	h6.%Dl	VwCC22elaR373zuu7dRZJQ==
Dikry07@gmail.com	-_Z3eG	sEdBwoBqFcmPuLiOskdubg==

Dikry08@gmail.com	^jxF2	FwpVwzpzTtqWCzlolvL8FA==

Tabel 7 menjelaskan jika enkripsi data yang dilakukan AES berjalan dengan baik. Hal ini terlihat bahwa *password user* yang sebelumnya berbentuk plain text, berubah menjadi *cipher text*. Selain itu setiap cipher text tidak memiliki kemiripan antara satu user dengan user yang lainnya.

a. Pengujian Hasil Ciphertext menggunakan kalkulator AES



GAMBAR 6 GAMBAR HASIL PENGUJIAN MENGGUNAKAN KALKULATOR AES

Gambar 6 menunjukan hasil pengujian menggunakan kalkulator AES berjalan dengan baik dan benar, dengan memasukan *plaintext* dengan *secret key* yang sama dengan aplikasi *Discover-U*. Hasil *Ciphertext* yang di dapat sudah sesuai dengan hasil *Ciphertext* dari aplikasi android. Dapat disimpulkan bahwa hasil algoritma AES dalam aplikasi *Discover-U* sudah sesuai dan berjalan dengan baik.

D. Hasil Pengujian Tingkat Keamanan AES

TABEL 8
HASIL PENGUJIAN *AVALANCHE EFFECT* AES-192

	Plain Text	AES key (hex)	Avalanche effect
Plaintext 1 “6a)F[f”	**36** 61 **29 46**	6A 72 30 38 33 6A 33 75	54,70%
	5B **66** 00 **00** 00 00 00 00 00 00 00 00	79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	
Modified key AES (hex) ““4a+D[b”	**34** 61 **28 44** 5B **62** 00 **04** 00 00 00 00 00 00 00 00		
Plaintext 2 “"7X:w0”	**22** 37 **58 3A** 77 **30** 00 **00** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	53,10%
Modified key AES (hex) “7Z8w4”	**20** 37 **5A 38** 77 **34** 00 **04** 00 00 00 00 00 00 00 00		
Plaintext 3 “h6.%Dl”	**68** 36 **2E 25** 44 **6C** 00 **00** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	53,90%
Modified key AES (hex)	**6A** 36 **2C 27**		

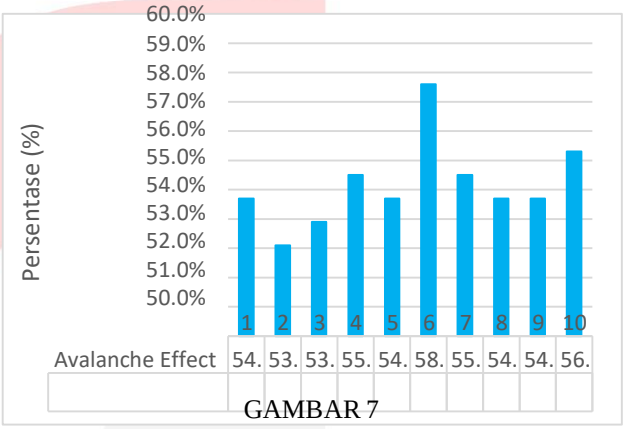
“j6,'Dh”	44 **68** 00 **04** 00 00 00 00 00 00 00 00		
Plaintext 4 “-_Z3eG”	**2D** 5F **5A 33** 65 **47** 00 **00** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	55,50%
Modified key AES (hex) “/_X1eC”	**2F** 5F **58 31** 65 **43** 00 **04** 00 00 00 00 00 00 00 00		
Plaintext 5 “^jxF2_”	**5E** 6A **78 46** 32 **5F** 00 **00** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	54,70%
Modified key AES (hex) “\jzD2[”	**5C** 6A **7A 44** 32 **5B** 00 **04** 00 00 00 00 00 00 00 00		

Plaintext 6 “pN{_4&”	**70** 4E **78 5F** 34 **26** 00 **00** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	58,60%
Modified key AES (hex) “`rNy]4"”	**72** 4E **79 5D** 34 **22** 00 **04** 00 00 00 00 00 00 00 00		
Plaintext 7 “~gI(B7|h”	**7E** 67 **49 28** 42 **37** 7C **68** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	55,50%
Modified key AES (hex) “|gK*B3|l”	**7C** 67 **48 2A** 42 **33** 7C **6C** 00 00 00 00 00 00 00 00		
Plaintext 8 “$2%oX&=b”	**24** 32 **25 6F** 58 **26** 30 **62** 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	54,70%

	00 00 00 00		
Modified key AES (hex) “&2'mX"=f”	**24** 32 **25 6F** 58 **26** 30 **62** 00 00 00 00 00 00 00 00		
Plaintext 9 “V8&ptIq#”	**56** 38 **26 70** 74 **49** 71 **23** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	54,70%
Modified key AES (hex) “T8$rtMq'”	**54** 38 **24 73** 74 **4D** 71 **27** 00 00 00 00 00 00 00 00		
Plaintext 10 “t>0'Ij{/”	**74** 3E **30 27** 49 **6A** 78 **2F** 00 00 00 00 00 00 00 00	6A 72 30 38 33 6A 33 75 79 30 33 68 6A 6F 74 66 33 30 6A 30 34 75 30 39	56,30%
Modified key AES (hex) “v>2%In{+”	**76** 3E **32 25** 49 **6E** 78 **28** 00 00 00 00		

	00 00 00 00		

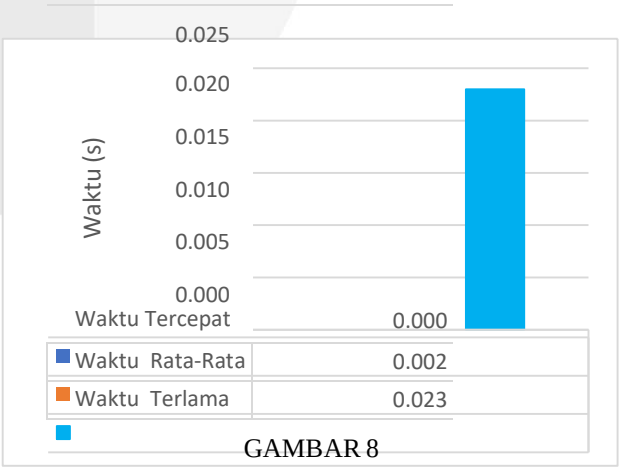
Tabel 8 menunjukan hasil pengukuran keamanan AES 192 ini dilakukan dengan menguji 10x *password* yang berbeda dan penguji melakukan pengacakan *password* untuk melihat tingkat keamanan atau *Avalanche effect* dari algoritma AES 192. Hasil dari pengujian *Avalanche effect* ini masuk kedalam tingkatan normal *Avalanche effect* yaitu dari 40%-60%. Dari 10 kali pengujian dapat kita lihat di atas bahwa semua hasil pengujian *Avalanche effect* berada di atas 50% .



GAMBAR 7
HASIL PENGUJIAN *AVALANCHE EFFECT*

Gambar 7 menunjukan hasil 10x hasil pengujian *Avalanche effect*, nilai *Avalanche effect* terendah terdapat pada pengujian ke-2 yaitu sebesar 53,9%, nilai tertinggi terdapat pada pengujian ke-6 yaitu sebesar 58,6%, dan nilai rata rata *Avalanche effect* dari 10x pengujian adalah 55%.

E. Hasil Pengujian *Running Time* Proses Enkripsi AES 192



GAMBAR 8
HASIL PENGUJIAN *RUNNING TIME*

Gambar 8 menunjukan hasil pengujian *running time* proses enkripsi AES pada aplikasi android menggunakan

fungsi *System.currentTimeMillis*, untuk menguji hasil durasi enkripsi AES 192 pada aplikasi android *Discover-U*. Grafik di atas menunjukan hasil *running time* proses enkripsi AES, dapat dilihat bahwa proses enkripsi AES memiliki rata-rata waktu pengujian 0,002s dengan waktu tercepat 0s dan waktu telama sekitar 0,023s. Pengujian ini dilakukan dengan menggunakan 60 sampel *password* dari weak dengan 6-8 karakter sampai *strong* dengan 18-20 karakter *password*.

V. KESIMPULAN

A. Kesimpulan

Setelah dilakukannya pengujian aplikasi dan hasil enkripsi, dapat disimpulkan bahwa:

a. Aplikasi *Discover-U* menggunakan algoritma *Advanced Encryption Standard* (AES), mampu melakukan pemetaan lokasi dalam ruangan dan dapat melakukan penyimpanan data user pengguna.
b. Aplikasi *Discover-U* dapat melakukan enkripsi dengan menggunakan kriptografi AES pada data *user id password* saat proges registrasi.
c. Pengimplementasian pemetaan lokasi dalam ruangan dengan cara mengambil data RSSI dari *smart stick* menggunkan protokol komunikasi MQTT, Data RSSI di ambil lalu dirubah menjadi sebuah *pixel* dan di visualisasikan ke map yang sudah di buat.
d. Hasil pengujian fungsionalitas dengan menggunakan metode black box, berjalan dengan lancar dan sudah sesuai dengan yang di harapkan. Hasil *Quality of Service* dari aplikasi *Discover-U* ke *server* MQTT memiliki *delay* rata-rata 602 ms, rata-rata *throughput* 1,214 Kbps, dan packet loss 0%..

B. Saran

Peneliti menyadari hasil dari implementasi, pengujian, dan penulisan jurnal ini masih jauh dari kata sempurna. Diharapkan dengan adanya penelitian ini, pengembangan aplikasi dan implementasi pemetaan lokasi dalam ruangan dapat terus di tingkatkan. Selain itu, diharapkan adanya penelitian lanjutan sebagai pengembang dari jurnal ini, dengan meningkatkan keamanan data dan menggunakan enkripsi data untuk lokasi pengguna *smart stick* yang diharapkan lebih aman untuk menjaga data-data pengguna dan memberikan user interface yang lebih menarik pada aplikasi sehingga lebih banyak masyarakat yang menggunakannya. Selain itu pengujian *Quality of Service* harus di dalam kondisi jaringan internet yang stabil sehingga hasil peujian lebih maksimal.

REFERENSI

[1] E. D. K. C. J. Hegarty, *Understanding GPS*. 2018.
[2] A. Muhdhor, “Efektivitas Penggunaan Aolikasi GPS (Global Positioning System) Dalam Menjangkau Lokasi Tujuan,” 2020.
[3] A. F. Reza, “Simulasi Sistem Indoor Localization Di Laboratorium Telekomunikasi FTI UII Dengan Algoritma Trilateration Menggunakan Bluetooth Low Energy,” Yogyakarta, 2018.
[4] K. K. Kamlesh Lakhwani, Hemant Kumar, Joseph Kofi, *IoT Internet Of Things “Principles, Paradigms and Applications of IoT.”* 2020.
[5] J. Mier, A. Jaramillo-Alcázar, and J. J. Freire, “At a Glance: Indoor Positioning Systems Technologies and Their Applications Areas,” *Adv. Intell. Syst. Comput.*, vol. 918, no. February, pp. 483–493, 2019, doi: 10.1007/978-3-030-11890-7_47.
[6] S. Chan and G. Sohn, “Indoor Localization Using Wi-Fi Based Fingerprinting and Trilateration Techiques for Lbs Applications,” *Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.*, vol. XXXVIII-4/, no. June, pp. 1–5, 2012, doi: 10.5194/isprsarchives-xxxviii-4-c26-1-2012.
[7] M. H. Vargas, “Indoor Navigation Using Bluetooth Low Energy (BLE) Beacons,” p. 54, 2016.
[8] C. Gomez, J. Oller, and J. Paradells, “Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology,” *Sensors (Switzerland)*, vol. 12, no. 9, pp. 11734–11753, 2012, doi: 10.3390/s120911734.
[9] E. Budiman, *Mobile Programming For Student*. 2019.
[10] S. K. s.frankel, R.Glenn, NIST, “The AES-CBC Cipher Algorithm and its use with IPsec,” *2003*. https://www.ietf.org/rfc/rfc3602.txt (accessed Dec. 01, 2021).
[11] M. C. Wadkar and P. P. Patil, “Traditional Infrastructure vs. Firebase Infrastructure,” *Int. J. Trend Sci. Res. Dev.*, vol. Volume-2, no. Issue-4, pp. 2050–2053, 2018, doi: 10.31142/ijtsrd14550.
[12] ITU-T, “G.1010: End-user multimedia QoS categories,” *Int. Telecommun. Union*, vol. 1010, 2001, [Online]. Available: http://scholar.google.com.au/scholar?hl=en&q=ITU-T+Recommendation+G.1010&btnG=&as_sdt=1,5&as_sdtp=#7.