OPEN ACCESS
J. OF ICT, VOL. 6, NO. 2, PP.054-069, DES 2024

ISSN : 26861089 (ONLINE)
DOI: 10.52661

Journal of Informatics and Communications Technology (JICT)

Perlindungan Privasi Data Lokasi pada Location Based Services menggunakan Advanced Encryption Standard dan Secure Hash Algorithm-3

Siti Nurrokhimah [#1], Asep Id Hadiana [*2], Fatan Kasyidi [#3]

Program Studi Informatika, Fakultas Sains dan Informatika, Universitas Jenderal Achmad Yani
Jl. Terusan Jend. Sudirman, Cibeber, Kec. Cimahi Sel., Kota Cimahi, Jawa Barat, Indonesia

[1]sitinurrokhimah20@if.unjani.ac.id , [2] asep.hadiana@lecture.unjani.ac.id , [3] fatan.kasyidi@lecture.unjani.ac.id

Abstract

Dalam era transformasi digital, Layanan Berbasis Lokasi (LBS) kini menjadi krusial dalam berbagai platform digital, termasuk website pengiriman untuk pelacakan lokasi paket secara real-time. Namun, penggunaan LBS membawa risiko keamanan data lokasi. Dalam penggunaannya, website ini mengirimkan data ke server dalam bentuk teks biasa, yang menimbulkan kelemahan dalam keamanan data privasi pengguna. Padahal, kerahasiaan data pribadi termasuk data lokasi diatur dalam Pasal 26 UU ITE Revisi 2016 yang mengatur tentang privasi data pengguna. Berdasar hal tersebut, pada penelitian ini diterapkan algoritma AES dan SHA-3 untuk mengenkripsi dan *hashing* data lokasi pengguna sebelum dikirimkan ke server. Penelitian ini menunjukkan bahwa proses enkripsi dan *hashing* data lokasi dengan menggunakan kombinasi dua algoritma dapat diterapkan pada *database* sistem LBS. Pengujian dilakukan dengan melihat waktu tempuh pengiriman data pada seluruh sistem sebanyak 10 kali dengan variasi jumlah input data berbeda, yang menunjukkan adanya peningkatan waktu proses setelah implementasi Algoritma AES dan SHA-3. Selanjutnya, dari hasil pengujian *avalanche effect* menunjukkan hasil yang kurang baik sehingga tidak memberikan tingkat keamanan yang maksimal. Pengujian integritas juga dilakukan, dengan memeriksa hasil *hashing* data menggunakan SHA-3. Dari hasil pengujian tersebut, menunjukkan bahawa aspek integritas data lokasi pengguna terpenuhi sesuai dengan hasil pengujian integritas yang dilakukan.

Keywords: AES, data lokasi, LBS, pengiriman, privasi, SHA-3

I. PENDAHULUAN

Dalam era transformasi digital, layanan berbasis lokasi (*Location Based Services*) telah menjadi bagian integral dari aplikasi sehari-hari, seperti peta digital, media sosial, layanan transportasi, dan berbagai aplikasi lainnya, yang memanfaatkan informasi lokasi pengguna [1]. LBS sendiri merupakan istilah yang umumnya digunakan untuk merujuk pada teknologi yang digunakan untuk menentukan dan mengakses lokasi suatu perangkat atau objek tertentu dengan menggunakan informasi lokasi geografis [2]. Dengan LBS, pengguna dapat secara langsung menunjukkan lokasi atau arah yang sedang dicari, sehingga memudahkan mereka dalam menemukan tujuan atau arah perjalanan dengan mudah secara real time [3]. Suatu contoh penerapan teknologi layanan berbasis lokasi (LBS) dapat ditemukan pada sebuah aplikasi pengiriman yang memanfaatkan LBS untuk memonitor dan melacak perjalanan paket dari lokasi awal (pengirim) hingga ke tujuan (penerima).

Meskipun memberikan kemudahan dan kegunaan yang besar, penggunaan data lokasi ini dapat mengancam privasi individu [4]. Kekhawatiran terhadap privasi dan keamanan data pengguna khususnya data lokasi dalam konteks LBS semakin meningkat seiring dengan perkembangan teknologi LBS, karena pengguna harus berbagi lokasi, dan memberikan izin kepada aplikasi serta layanan untuk mengakses informasi lokasi fisik. Isu-isu terkini seperti pelacakan tanpa izin, akses tidak sah, dan potensi penyalahgunaan data pribadi menyoroti urgensi perlindungan privasi pada LBS [5]. Data lokasi pada LBS memiliki signifikansi yang besar karena data lokasi yang bersifat rahasia dapat dimanfaatkan untuk berbagai keperluan dan membawa risiko tinggi jika jatuh ke pihak yang tidak sah.

Penggunaan layanan berbasis lokasi rentan terhadap pelanggaran privasi [4]. Ancaman tersebut meliputi penyalahgunaan data, penyusupan privasi, dan bahaya keamanan terkait lokasi yang mengarah pada potensi risiko bagi pengguna [6]. Oleh karena memiliki konsekuensi yang serius jika jatuh ke tangan yang tidak seharusnya, maka menjaga kerahasiaan informasi lokasi geografis menjadi sangat penting. Dalam situasi ini, menjaga keamanan data lokasi pada aplikasi pengiriman menjadi krusial untuk mencegah potensi pencurian informasi yang dapat dimanfaatkan oleh pihak yang tidak sah. Selain itu, upaya perlindungan data juga diperlukan untuk menghindari kemungkinan modifikasi dan manipulasi data lokasi pelanggan. Algoritma enkripsi seperti *Advanced Encryption Standard* (AES) dan algoritma *hashing* seperti *Secure Hash Algorithm* (SHA) telah menjadi standar dalam bidang keamanan data. AES menggunakan pendekatan kunci simetris yang efisien untuk mengenkripsi data dengan cepat, sementara SHA-3 menawarkan keamanan tambahan dalam hal integritas data karena sangat sulit untuk menghasilkan nilai *hash* yang sama dari data input yang berbeda [7]. Kombinasi kedua algoritma ini dapat memberikan perlindungan yang lebih kuat terhadap berbagai ancaman keamanan. Dengan demikian, informasi lokasi asli pengguna tidak akan dapat dibaca oleh pihak-pihak yang tidak bertanggung jawab.

Dalam penelitian [8] sebelumnya, digunakan algoritma algoritma AES-128 dan SHA-256 untuk mengamankan file dokumen, yang menunjukkan bahwa kombinasi tersebut dapat digunakan untuk membangun aplikasi pengamanan file dokumen yang efektif. Algoritma AES-128 digunakan untuk mengenkripsi file dokumen, sedangkan SHA-256 digunakan untuk menghasilkan *hash* file yang kemudian diverifikasi untuk memastikan integritas file. Hasil penelitian menunjukkan bahwa aplikasi yang dibangun dapat mengenkripsi dan dekripsi file dokumen dengan cepat dan aman, serta dapat mendeteksi perubahan pada file dokumen dengan akurat. Selain itu, pada penelitian [9] menggunakan algoritma SHA-3 dan AES untuk meningkatkan keamanan proses pensinyalan Mobile IPv6. Algoritma SHA-3 digunakan untuk menghasilkan *hash* dari pesan pensinyalan, dan *hash* tersebut kemudian dienkripsi dengan AES untuk melindungi integritas dan kerahasiaan data. Hasil penelitian menunjukkan bahwa kombinasi SHA-3 dan AES dapat memberikan keamanan yang lebih baik dibandingkan dengan algoritma yang digunakan saat ini, seperti MD5 dan 3DES, tanpa menyebabkan overhead kinerja yang signifikan. Penelitian tersebut, menunjukkan bahwa dengan pengujian Brute Force, untuk melakukan cracking pada berkas yang telah dienkripsi algoritma AES diperlukan waktu komputasi dengan estimasi 2.7 x 10^25 tahun. Sementara itu, dilakukan juga pengujian Collision Attack untuk SHA-3 dan hasilnya menunjukkan bahwa SHA-3 tidak memiliki celah keamanan collision attack berapapun variasi bit yang dimilikinya. Selanjutnya pada penelitian [7], digunakan algoritma Grain dan SHA-3 untuk mengamankan data lokasi, yang menunjukkan bahwa kombinasi tersebut dapat digunakan untuk mengamankan data lokasi secara efektif. Algoritma Grain digunakan untuk mengenkripsi data lokasi, dan SHA-3 digunakan untuk menghasilkan *hash* dari data terenkripsi. Hasil penelitian menunjukkan bahwa kombinasi ini mampu melindungi data lokasi dari berbagai serangan. Pada penelitian ini didapatkan hasil pengukuran menggunakan t-test menunjukkan bahwa waktu tempuh sebelum diterapkannya Algoritme Grain dan SHA-3 pada aplikasi Ambulan Online yakni 3,768366667 s dan setelah diterapkan yakni 5,629166667 s, sehingga nilai t adalah -2.018, dengan nilai probabilitas (Sig.) masing-masing adalah 0.048 dan 0.049. Hal ini mengindikasikan adanya perbedaan signifikan dalam waktu tempuh sebelum dan setelah implementasi Aplikasi Ambulan Online menggunakan Algoritma Grain dan SHA-3. Selain itu, dilakukan juga pengujian integritas untuk memastikan hasing data yang dihasilkan valid, dimana dapat disimpulkan jika aspek integritas terpenuhi dan Algoritma SHA-3 yang

digunakan bersifat valid, karena digest text yang terbentuk sesuai dengan percobaan digest pertama. Hal ini menunjukkan bahwa kombinasi ini dapat digunakan dalam aplikasi yang membutuhkan keamanan data lokasi dan kinerja yang baik.

Berdasarkan studi terdahulu tersebut, maka penerapan algoritma AES dan SHA-3 untuk menjaga keamanan data lokasi dalam konteks Layanan Berbasis Lokasi sangat relevan, mengingat semakin banyaknya aplikasi yang bergantung pada data lokasi dan risiko terkait kebocoran data tersebut. Penelitian ini mengidentifikasi kinerja algoritma AES dan SHA-3 jika diterapkan pada layanan berbasis lokasi berbentuk website responsive yang bisa diakses melalui desktop dan mobile. Proses enkripsi pada data lokasi melibatkan transformasi informasi geografis seperti longitude (sumbu x) dan latitude (sumbu y) ke dalam format yang tidak dapat diakses, dengan menggunakan kunci enkripsi yang hanya diketahui oleh pihak yang berwenang. Sementara proses *hashing* digunakan untuk memeriksa integritas data lokasi yang telah dienkripsi karena sangat sulit untuk menghasilkan nilai *hash* yang sama dari data input yang berbeda. Diharapkan bahwa penelitian ini menghasilkan strategi yang dapat meningkatkan keamanan dan privasi data lokasi pengguna dalam layanan berbasis lokasi.

II. STUDI LITERATUR

Dalam penelitian [8] sebelumnya, digunakan algoritma algoritma AES-128 dan SHA-256 untuk mengamankan file dokumen, yang menunjukkan bahwa kombinasi tersebut dapat digunakan untuk membangun aplikasi pengamanan file dokumen yang efektif. Algoritma AES-128 digunakan untuk mengenkripsi file dokumen, sedangkan SHA-256 digunakan untuk menghasilkan *hash* file yang kemudian diverifikasi untuk memastikan integritas file. Persamaan penelitian tersebut adalah dari segi penggunaan algoritma AES-128 untuk ekripsi data dari file. Perbedaan dari penelitian tersebut adalah, pada penelitian ini menerapkan algoritma AES-128 untuk data tracking dengan jumlah data yang terus bertambah secara signifikan untuk tiap waktu tertentu. Selain itu, pada penelitian [9] menggunakan algoritma SHA-3 dan AES untuk meningkatkan keamanan proses pensinyalan Mobile IPv6. Algoritma SHA-3 digunakan untuk menghasilkan *hash* dari pesan pensinyalan, dan *hash* tersebut kemudian dienkripsi dengan AES untuk melindungi integritas dan kerahasiaan data. Hasil penelitian menunjukkan bahwa kombinasi SHA-3 dan AES dapat memberikan keamanan yang lebih baik dibandingkan dengan MD5 dan 3DES, tanpa menyebabkan overhead kinerja yang signifikan. Persamaan dari penelitian tersebut terletak pada penggunaan algoritma AES dan SHA3 untuk meningkatkan keamanan. Sementara perbedaannya, terletak pada jenis data yang dienkripsi, dimana dalam penelitian ini, data yang dienkripsi adalah data lokasi pengguna yang diinputkan oleh klien ke server dan dapat berubah setiap waktu. Selanjutnya pada penelitian [7], digunakan algoritma Grain dan SHA-3 untuk mengamankan data lokasi, yang menunjukkan bahwa kombinasi tersebut dapat digunakan untuk mengamankan data lokasi secara efektif. Algoritma Grain digunakan untuk mengenkripsi data lokasi, dan SHA-3 digunakan untuk menghasilkan *hash* dari data terenkripsi. Hasil penelitian menunjukkan bahwa kombinasi ini mampu melindungi data lokasi dari berbagai serangan. Isi dari penelitian inilah yang menjadi dasar untuk penulis membuat penelitian terkait dengan algoritma SHA-3. Pada penelitian ini dijelaskan mengenai algoritma SHA-3, yang mana aspek integritas pada user dapat dipenuhi dari penerapan SHA-3 dibuktikan dengan adanya pengujian integritas. Digest text yang dihasilkan pada beberapa percobaan dengan inputan sama terbukti menghasilkan digest text yang sama dan tidak bisa diubah menjadi plain text.

A. *Layanan Berbasis Lokasi* (LBS)

Location Based Service (LBS) atau Layanan Berbasis Lokasi adalah layanan yang memanfaatkan informasi lokasi pengguna untuk memberikan layanan yang relevan dengan lokasi tersebut [3]. LBS memanfaatkan perangkat seluler, teknologi pemosisian, dan internet seluler untuk memberikan informasi atau layanan relevan terkait dengan lokasi pengguna yang dapat digunakan untuk berbagai keperluan, seperti navigasi, pencarian informasi, dan pemasaran [10]. LBS dapat diimplementasikan dengan berbagai teknologi, seperti GPS, Wi-Fi, dan Bluetooth, yang memungkinkan komunikasi dua arah antara pengguna dan penyedia layanan, dimana pengguna dapat memberikan informasi lokasi kepada penyedia layanan, dan penyedia layanan dapat memberikan informasi yang relevan dengan lokasi pengguna [2].

B. *Data Lokasi*

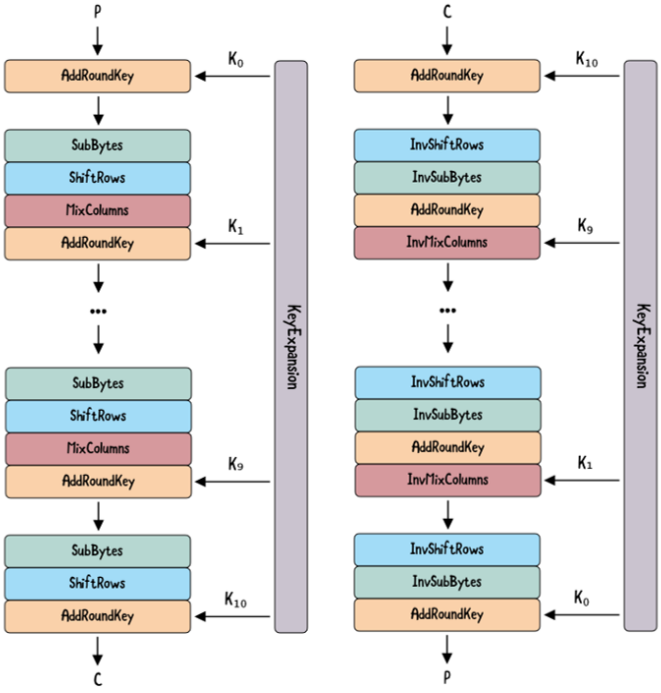
Data lokasi adalah informasi yang menunjukkan posisi suatu objek atau perangkat di permukaan bumi. Informasi ini mencakup koordinat geografis, seperti latitude dan longitude [6]. Latitude adalah jarak suatu titik dari garis khatulistiwa, sedangkan longitude adalah jarak suatu titik dari meridian primer [5]. Data lokasi adalah komponen penting dalam banyak aplikasi dan teknologi, terutama dalam layanan berbasis lokasi, yang digunakan untuk memberikan informasi atau layanan yang relevan dengan lokasi pengguna. Data lokasi dapat digunakan untuk berbagai tujuan, seperti navigasi, pemasaran, dan keamanan [6]. Oleh karena itu, data lokasi memainkan peran penting dalam berbagai aplikasi dan teknologi.

C. *Kebutuhan Perlindungan Privasi pada Layanan Berbasis Lokasi*

Data pribadi yang sensitif menjadi bagian penting dari kehidupan setiap individu. Oleh karena itu, dalam penggunaan aplikasi berbasis internet, data pribadi menjadi titik fokus utama [11]. Kebutuhan untuk melindungi privasi data pribadi dalam Layanan Berbasis Lokasi (LBS) telah menjadi semakin penting seiring dengan meningkatnya penggunaan teknologi yang mengumpulkan data lokasi pengguna. Pengguna LBS harus memiliki kejelasan tentang bagaimana data mereka dikumpulkan, diproses, dan digunakan, serta diberikan kontrol penuh atas informasi pribadi mereka [4]. Kerahasiaan data pribadi termasuk data lokasi diatur dalam Pasal 26 UU ITE Revisi 2016 yang mengatur tentang privasi data pengguna, sehingga perusahaan atau layanan yang menggunakan data lokasi pengguna dalam layanan itu wajib menjaga kerahasiaan informasi lokasi tersebut.

D. *Algoritma Advenced Encyption Standard*

Advanced Encryption Standard (AES) adalah algoritma enkripsi yang menggunakan kunci yang sama untuk enkripsi dan dekripsi (kunci simetris) yang dikembangkan oleh NIST pada tahun 2001 [12]. AES memiliki tiga jenis, yaitu AES-128, AES-192, dan AES-256 [13]. Perbedaan ketiga jenis AES terletak pada panjang bit kunci yang digunakan dan jumlah putaran yang dilakukan [14]. Pada penelitian ini digunakan AES-128 untuk proses enkripsi data, dimana menggunakan kunci 128 bit dan melakukan 10 putaran. AES-128 dipilih karena memiliki panjang bit kunci yang cukup untuk memberikan keamanan yang memadai, namun tetap memiliki performa yang baik.

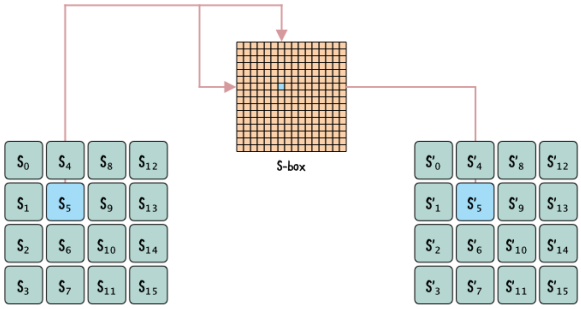


Gambar. 1. Tahapan Enkripsi dan Dekripsi AES

terdapat 4 tahapan transformasi byte untuk proses enkripsi pada AES, yakni sebagai berikut [14]:

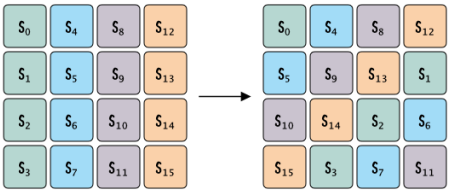
1) Putaran AddRoundKey: dimana setiap putaran melibatkan proses XOR antara status kerja dan kunci putaran. Proses XOR ini menggunakan tabel RCON untuk menghasilkan nilai kolom pertama pada setiap putaran. Tabel RCON ini berisi nilai-nilai khusus yang digunakan dalam proses tersebut.

2) SubBytes: proses menggantikan atau mengubah setiap byte pada state dengan byte yang sesuai dari S-box. S'[r, c] = xy adalah elemen dalam tabel S-Box, di mana S'[r, c] adalah perpotongan baris (x) dengan kolom (y), dan xy adalah digit hexadecimal.



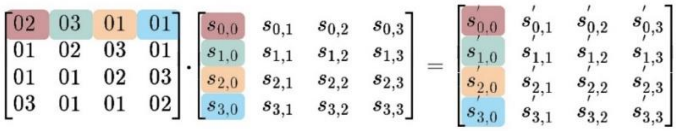
Gambar. 2. Transformasi SubBytes

3) ShiftRows: proses menyusun byte-byte di setiap baris dengan menggesernya ke kiri sejumlah posisi tertentu sehingga enkripsi dan dekripsi dapat dilakukan.



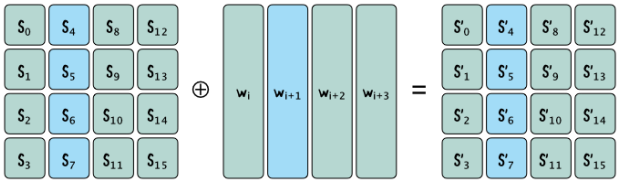
Gambar. 3. Transformasi ShiftRows

4) MixColumns: proses memperkenalkan tingkat difusi yang lebih tinggi dimana kolom-kolom state diubah dengan menggunakan Matriks Penggandaan Galois (Galois Field Multiplication).



Gambar. 4. Transformasi MixColumns

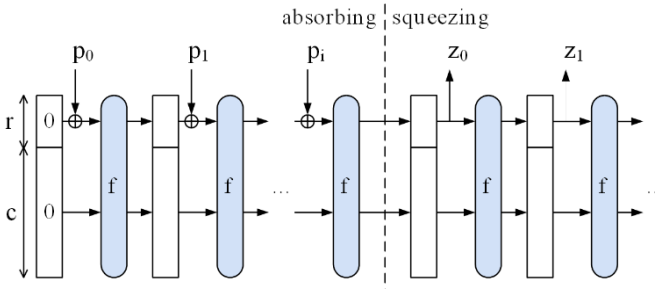
5) AddRoundKey: proses melakukan operasi XOR antara matriks state yang baru dengan round key.



Gambar. 5. Transformasi AddRoundKey

E. *Teknik Hashing dengan Secure Hash Algorithm-3*

Secure Hash Algorithm-3 merupakan fungsi *hash* kriptografis untuk mengubah data menjadi format yang bersifat unik (*hash*), yang sangat sulit untuk diubah kembali ke bentuk semula [7]. SHA-3 dikembangkan oleh National Institute of Standards and Technology (NIST) sebagai bagian dari proses seleksi untuk mengganti SHA-2 yang sebelumnya ada [15]. Kelebihan utama SHA-3 (Keccak) adalah desain yang berbeda dan lebih aman dibandingkan dengan SHA-2 pendahulunya karena menggunakan pendekatan yang berbeda dalam strukturnya [9]. Karena keamanannya dan pendekatannya yang berbeda, SHA-3 menawarkan variasi *hash* yang berbeda, seperti SHA3-224, SHA3-256, SHA3-384, SHA3-512, dan SHAKE128/256. Rancangan SHA-3 menggunakan pendekatan konstruksi spons, di mana data diserap ke dalam struktur spons. Pada fase ini, blok pesan di-XOR-kan ke dalam status, dan seluruhnya mengalami transformasi menggunakan fungsi permutasi f. Hasilnya kemudian diperas, di mana blok keluaran dibaca dari subset yang sama dari status dengan bantuan fungsi transformasi keadaan f [7].



Gambar. 6. Tahapan hashing SHA-3

Dalam pembangunan fungsi *hash* menggunakan konstruksi spons, masukan diberi label Pi dan keluaran *hash* disebut Zi. "Kapasitas" c, yang tidak dimanfaatkan, harus setara dengan dua kali lipat dari tingkat keamanan yang diinginkan terhadap benturan atau serangan preimage. Secara umum, konstruksi spons terdiri dari dua tahap, yaitu [7]:

1) Fase absorbing: tahap dimana pecahan-pecahan masukan diolah melalui operasi XOR, lalu input masukan dialirkan ke dalam fase ini untuk diteruskan ke fungsi f pada bitrate dari state yang sedang digunakan.

2) Fase squeezing: tahap yang bertujuan untuk mendapatkan hasil keluaran, yang selanjutnya digabungkan dengan sejumlah bit tertentu dari hasil fungsi f. Tujuannya adalah agar jumlah bit yang digabungkan sama dengan jumlah bit yang diinginkan dalam proses ini.

F. *Pengujian t-test*

Pengujian t-test adalah sebuah metode statistik yang digunakan untuk membandingkan rata-rata antara dua kelompok atau sampel yang independen. Tujuan dari pengujian t-test yakni untuk menentukan apakah ada perbedaan yang signifikan antara rata-rata dari dua kelompok data secara statistik ataukah hanya terjadi karena kebetulan. Dengan menggunakan t-test, dapat dievaluasi efektivitas suatu intervensi, membandingkan hasil sebelum dan sesudah suatu perubahan atau menguji efek dari suatu variabel independen terhadap variabel dependen dalam sebuah eksperimen [16]. Selain itu, pengujian t-test juga dapat digunakan dalam pengambilan keputusan bisnis, seperti mengevaluasi strategi pemasaran atau kebijakan harga. Dalam konteks mengukur perbedaan waktu tempuh, pengujian t-test dapat digunakan untuk membandingkan waktu tempuh sebelum dan sesudah pengujian pada dua kelompok yang sama atau berbeda. Pengujian ini digunakan untuk mengevaluasi perbedaan dalam waktu tempuh sistem sebelum dan sesudah diterapkan algoritma enkripsi [7].

Perhitungan nilai t dilakukan secara sequensial ketika algoritma telah diterapkan pada sistem dengan menggunakan rumus yang memperhitungkan perbedaan antara rata-rata dua sampel, deviasi standar masing-masing sampel, serta ukuran sampel, yakni sebagai berikut:

$$t = \frac{X_1 - X_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}} \quad (1)$$

Keterangan :
X_1 dan X_2 : rata-rata dari dua sampel
S_1 dan S_2 : deviasi standar masing-masing sampel
n_1 dan n_2 : ukuran sampel masing-masing

Proses perhitungan ini memberikan nilai t yang akan dibandingkan dengan nilai kritis untuk menentukan apakah perbedaan antara rata-rata kedua sampel tersebut signifikan secara statistik atau tidak.

G. *Pengujian Avalanche Effect*

Avalanche Effect adalah pengujian yang mengevaluasi bagaimana perubahan kecil dalam input memengaruhi hasil enkripsi. Pengujian ini menunjukkan dampak perubahan susunan kunci enkripsi terhadap susunan bit data terenkripsi [17]. Dengan kata lain, sedikit perubahan pada teks dapat menyebabkan perubahan besar pada hasil enkripsi. Semakin tinggi nilai *avalanche effect*, semakin aman algoritma kriptografi tersebut[18]. Dalam penelitian ini, hasil enkripsi dan pengujian *avalanche effect* dilakukan secara berurutan setelah proses enkripsi dan dekripsi selesai. Perhitungan *Avalanche Effect* dapat dilakukan menggunakan rumus berikut:

$$\text{Avalanche Effect} = \frac{Jumlah\ bit\ yang\ berbeda}{total\ bit} \times 100 \quad (2)$$

Pada pengujian *avalanche effect* ini, target ideal adalah sekitar 50% perubahan bit pada output. Hal ini menunjukkan bahwa algoritma sangat sensitif terhadap perubahan kecil pada input, yang merupakan karakteristik keamanan yang diinginkan. Namun, rentang antara 45% hingga 60% masih dianggap sangat baik dan menunjukkan properti keamanan yang kuat [19].

H. *Pengujian Integritas*

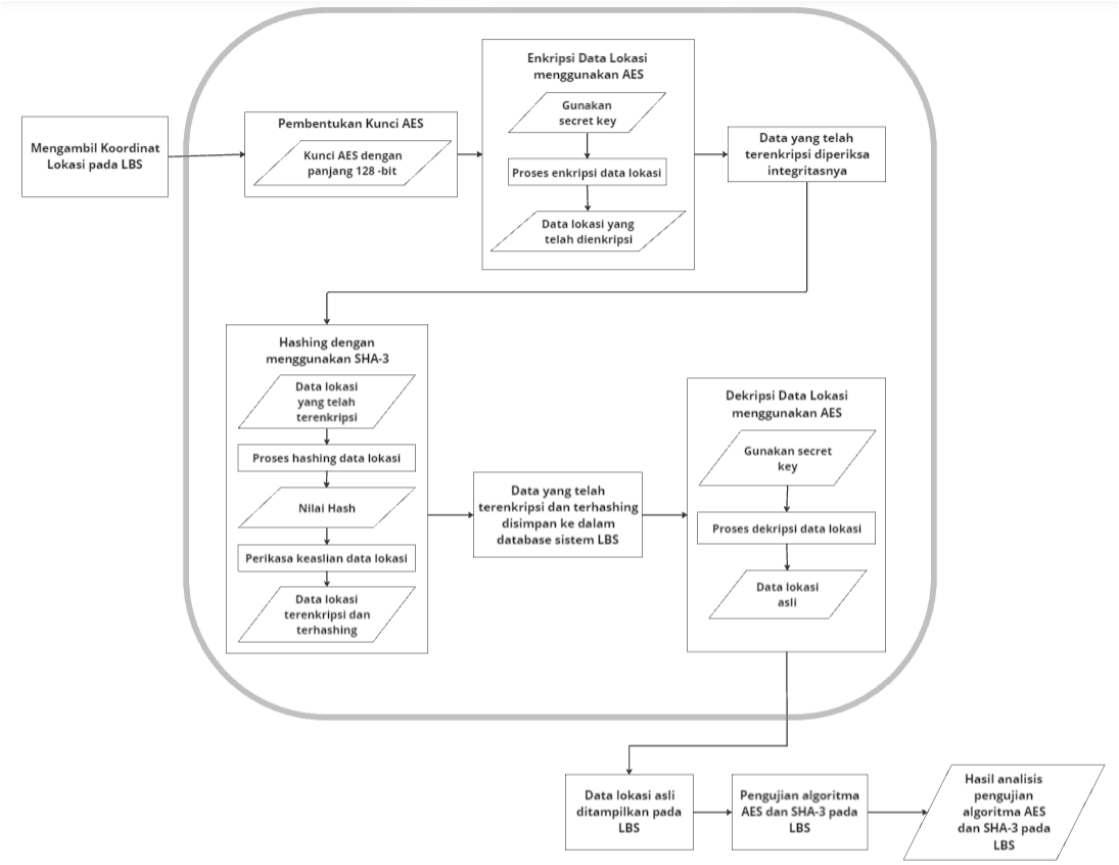
Pengujian integritas adalah proses verifikasi yang digunakan untuk memastikan bahwa hasil *hashing* data yang dihasilkan oleh algoritma tertentu valid dan tidak mengalami perubahan yang tidak diinginkan [7]. Langkah-langkah dalam pengujian integritas biasanya melibatkan pembentukan *hash* dari dua input yang sama, kemudian membandingkan hasil *hash* tersebut. Jika kedua hasil *hashing* tersebut sama, maka dapat disimpulkan bahwa algoritma yang digunakan dalam proses *hashing* tersebut valid dan integritas data tersebut dianggap terjamin [9]. Pengujian integritas ini dilakukan secara sequensial ketika ketika algoritma telah diterapkan pada sistem. Rumus yang digunakan dalam pengujian integritas adalah membandingkan hash dari dua input yang sama, seperti.

$$H\ (m_1) = H\ (m_2) \quad (3)$$

Keterangan :
H : fungsi *hash*
m_1 dan m_2 : dua pesan yang sama.

III. METODE PENELITIAN

Pada penelitian ini dilakukan implementasi algoritma AES dan SHA-3 pada lingkungan simulasi LBS untuk melindungi privasi data lokasi, dengan alur metode penelitian dengan tahapan-tahapan yang dapat dilihat pada Gambar 7 berikut ini.



Gambar. 7. Metodologi Penelitian

A. *Pengambilan Koordinat Lokasi*

Pada tahap pengambilan data lokasi atau koordinat, dilakukan melalui layanan berbasis lokasi (LBS) dengan memanfaatkan antarmuka pemrograman aplikasi (API) dari Google Maps API. Proses ini dimulai dengan memperoleh kunci API yang diperlukan dari Google Maps API, yang nantinya digunakan untuk mendapatkan izin akses terhadap informasi lokasi. Setelah mendapatkan kunci API, langkah berikutnya yakni penggunaan Software Development Kit (SDK) atau Endpoint API untuk mengambil data lokasi dalam bentuk koordinat geografis, berupa longitude dan latitude. Selanjutnya, memperoleh izin lokasi dari pengguna agar dapat mengakses informasi lokasi dengan lebih akurat. Contoh data lokasi yang akan dienkripsi pada sistem Pengiriman berbasis LBS, yakni seperti pada Tabel I berikut:

TABEL I
CONTOH DATA LOKASI

No	Titik Lokasi	Latitude	Longitude
1	Jalan MH Thamrin, Jakarta	-6.1751	106.8272
2	Jalan Asia Afrika, Bandung	-6.9039	107.6098
3	Jalan Malioboro, Yogyakarta	-7.7956	110.4256
4	Jalan Raya Kuta, Bali	-8.4095	115.1628
…			
30	Jalan Kapten A Rivai, Palembang	-2.9167	104.7458

B. *Implementasi Algoritma AES dan SHA-3*

Tahap selanjutnya yaitu mengimplementasikan algoritma AES dan SHA-3 ke dalam sistem Pengiriman berbasis LBS yang telah dibangun untuk perlindungan privasi data lokasi.

1) Pembentukan Kunci AES: dimana kunci AES yang terdiri dari 128-bit dan dihasilkan secara acak, diorganisir ke suatu state (matriks 4x4 byte). Kunci tersebut kemudian mengalami proses key expansion, menghasilkan kunci putaran tambahan untuk setiap langkah enkripsi. Setiap byte dalam state mengalami substitusi dengan byte lain berdasarkan tabel S-Box. Lalu, dilakukan serangkaian transformasi termasuk shiftrows, mixcolumns, dan addroundkey, dimana seluruh proses ini diulang sebanyak 10 putaran.

2) Enkripsi data Lokasi menggunakan AES: dilakukan dengan menggunakan kunci simetri AES yang telah dibentuk sebelumnya. Proses ini menghasilkan data lokasi yang telah terenkripsi yang selanjutnya disimpan dalam database sistem LBS, juga diperiksa integritasnya menggunakan algoritma *hashing*.

3) Hashing dengan SHA-3: dilakukan untuk men-*hash* data lokasi yang telah dienkripsi menggunakan algoritma SHA-3. Nilai *hash* yang dihasilkan kemudian disimpan dalam database sistem LBS. Nilai *hash* ini digunakan untuk memeriksa integritas data lokasi yang telah dienkripsi.

4) Dekripsi Data Lokasi menggunakan AES: dilakukan menggunakan kunci simetri AES yang sebelumnya digunakan untuk mengenkripsi data lokasi. Hasil dekripsi ini menampilkan data lokasi asli, yang nantinya dapat ditampilkan pada Layanan Berbasis Lokasi (LBS) sesuai dengan hak akses yang dimiliki oleh pengguna.

C. *Pengujian dan Analisis*

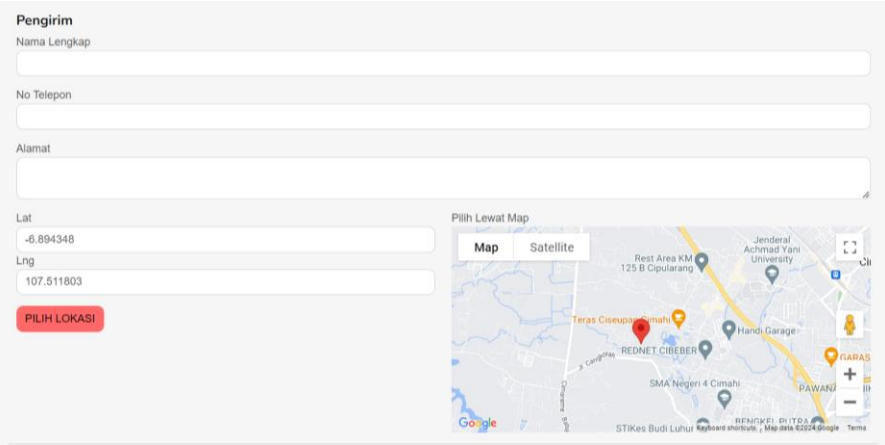
Pada tahap ini, dilakukan serangkaian pengujian dengan mengukur lamanya waktu respon website ketika sebelum dan sesudah diterapkannya algoritma AES dan SHA-3, juga mengukur *avalanche effect* dari algoritma AES, serta menguji integritas dari algoritma dan SHA-3. Pada tahapan ini juga, dihasilkan data hasil pengujian serta analisisnya untuk menilai tingkat keamanan, kinerja, serta integritas dari enkripsi dan *hashing* dalam melindungi privasi data lokasi.

IV. HASIL DAN PEMBAHASAN

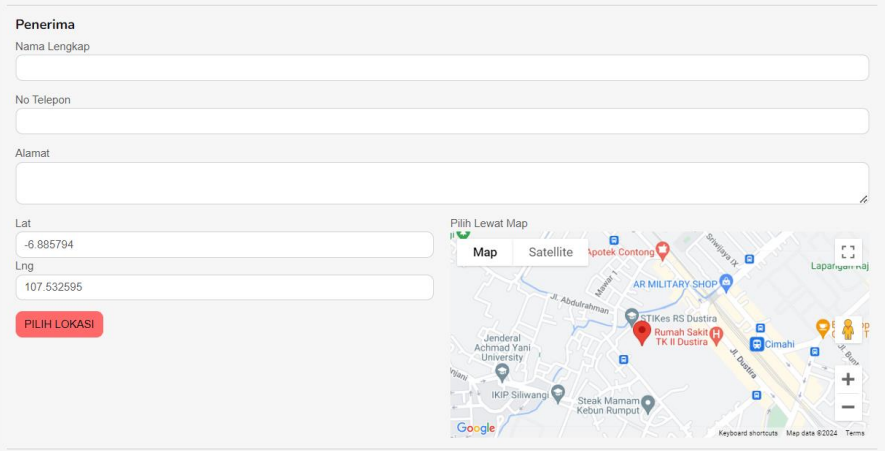
Penelitian ini menghasilkan informasi mengenai langkah-langkah enkripsi, *hashing*, dekripsi, pengujian performa sistem, pengujian *avalanche effect* pada ciphertext yang diperoleh, serta pengujian integritas pada data lokasi terenkripsi yang telah diamankan dengan AES dan SHA-3.

A. *Proses Pengambilan Koordinat Lokasi*

Proses pengambilan data lokasi atau koordinat, dilakukan melalui website pengiriman saat pelanggan akan melakukan pemesanan pengiriman dengan terlebih dahulu memperoleh izin lokasi dari pelanggan agar dapat mengakses informasi lokasi dengan lebih akurat. Pengambilan data lokasi ini dilakukan dengan menentukan titik lokasi pengirim dan penerima paket, antar muka proses pengambilan data lokasi pengirim dapat dilihat pada Gambar 8, dan antar muka proses pengambilan data lokasi penerima dapat dilihat pada Gambar 9 berikut ini.



Gambar. 8. Proses pengambilan data lokasi pengirim (pelanggan)



Gambar. 9. Proses pengambilan data lokasi penerima (pelanggan)

B. *Implementasi Algoritma AES (enkripsi)*

Setelah berhasil mengambil data lokasi dari sistem LBS, tahap selanjutnya yaitu mengimplementasikan algoritma AES ke dalam sistem LBS Pengiriman yang telah dibangun untuk mengenkripsi data lokasi, maka data yang tersimpan pada database sistem yakni data yang telah terenkripsi oleh AES-128.

TABEL II
DATA LOKASI TERENKRIPSI PADA DATABASE

No	lat_kurir	lang_kurir	lat_pengirim	long_pengirim	lat_penerima	long_penerima
1	uPoLU6mFNPj8h/McoDEYhA==	p+XUaAUbJriETjVeYaO1Qg==	bdTKYHz7MiCNiLpshm9Ofg==	FtN+KViDs3ZD797cnGICGQ==	VxWOz2vUhfZBNIJBWo+khQ==	a2CZ198l+psc3bHiwehZYg==
2	I4cHvAJnljgmOslIqqx7nA==	BK1o2/W3+f/MSbkHadHV1A==	c5e2Q64oaDeJZld8yBumLw==	wBV53YZJXkzl+NQ4963Mtw==	+4fdgJdHHihsSRWqBahOtg==	DkGT3e3EnMyv8HJtRsobOw==
3	peDqhYNeEEtcFTXJxYInAA==	/f/tp2Bn2qpkZwHbdCo/lg==	Ia3R5U939BVks8qFoK1cTg==	v2PCP6PQDK9Lw7ldFWAGzQ==	9dWDjmA9zHSJVH25O/sh7A==	o+fTscjX/2DcDSEHjo9rEQ==
…	…	…	…	…	…	…
30	I4cHvAJnljgmOslIqqx7nA==	BK1o2/W3+f/MSbkHadHV1A==	uqzZKtVEQJAuJbwTahaXZg==	4GPTUAe8RL49U5ZsVTM09w==	scu2VbgAKWtD0OwqPNOiCA==	X2gv3xIQhAKizh2DkAsIVg==

C. *Implementasi Algoritma SHA-3*

Setelah itu, data yang sudah terenkripsi dilanjutkan ke tahap berikutnya dengan menerapkan algoritma SHA-3 pada data lokasi yang telah dienkripsi. Hal ini memungkinkan pengecekan integritas data lokasi terenkripsi sebelum data tersebut didekripsi. Hasil *hash* dari SHA-3 kemudian disimpan di database sistem. Ketika data lokasi dipanggil oleh klien, terlebih dahulu dilakukan perbandingan dengan nilai *hash* yang tersimpan untuk memastikan integritasnya. Proses ini melibatkan *hashing* ulang data lokasi terenkripsi dan membandingkannya dengan nilai *hash* yang tersimpan sebelumnya di database untuk menguji apakah ada perubahan, karena fungsi *hash* akan menghasilkan output yang sama jika inputnya tidak berubah.

TABEL III
HASH DATA LOKASI (KURIR) TERENKRIPSI PADA DATABASE

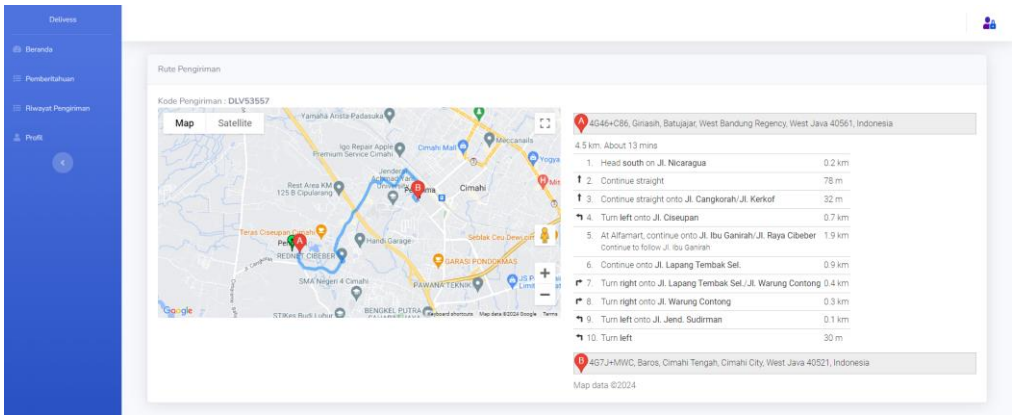
No	hash_lat_kurir	hash_lang_kurir
1	a29073b08538bfd3933c5a5f7c637232b4b4ebb6c3d5f703f752db78a1b972e2	3b3bc718e9f5c5cc0e64eee7f14822eec1527733d609030cc23de1e68f8ecb11
2	3937a47279bf2a182c5ea5ffd124cb9de38ffdcfd6ccb9c0192b1f71970f171f	217a2a35f7fd09e832ecc674b0a1ad5b740223662f1dd2fc275848860db79554
3	98cd10c69a8c69f2122c9bdc1d043898d33436de50c6d9f524f6e085409b87de	bc98c76d9544035b89fc299c4719d897a932d88dace1b50b36486efcc13c15d0
…	…	…
30	3937a47279bf2a182c5ea5ffd124cb9de38ffdcfd6ccb9c0192b1f71970f171f	217a2a35f7fd09e832ecc674b0a1ad5b740223662f1dd2fc275848860db79554

TABEL IV
HASH DATA LOKASI (PENGIRIM DAN PENERIMA) TERENKRIPSI PADA DATA DATABASE

No	hash_lat_pengirim	hash_long_pengirim	hash_lat_penerima	hash_long_penerima
1	e648cc512e479bce8acd02d88a20137f9308653aea3374d44bc4e2308426f18b	5b009aa23ae83e78a1c874784b44c0d087644f881ee129e012e435cf0d6e0471	38f4a185178ba56f00f7f439dea127cfe27bd643ff445cebb49d2825f5cd1b03	ff01aec9ea6ac4cad7f57c8b2be88b51814d3ad6b4a18d26b46e1a5e8c315f3b
2	54882d18f3288e710c47753a43bcf2dabfc7acbf1eff7f0a2569d5a7f6341d28	7aae8d57ee83284e15ee6e3cbf7d09d15e195c7923fc32e17f4ddb59eed9a878	dd5f55e4f2756a8bcb0033de11d92464488f7d82069f4b3b55c17052be7c0351	1d31ef6f79ef45ae9caf962566dee4771e1da3ede416bfd7a6e439b71b4d468b
3	734a645a478b2574f8d1b41a37fda4ae3c8ea9b90bd112b85e9a539082157245	775cb4dddb41175486fe09a3c6ece56332dab8ea8bf051fa159cacb0d625bf99	e27c432b98f1dbe90b3a32722fd12836532711c232ea0bd0ff1b6994b3a76a14	533df8669dd7119f715a23ad11f777e69ca0396dc66eb25bda77abd51dd07ec3
…	…	…	…	…
30	a5bdc4d85603bc7702e7901a307be5a4ab5f4fcdaf8681f8d4f873d85bd83378	8a1b225d01b6d9d7542085e6af4de6ce23b86af2977e1b15698e4297accaf875	4ff1be8699e092bff58444d217c7f71aea649675039d8e4c35d8d6a049c03b94	9e6b283d60e6f65e42ed50c113f5cf9214c3349ae2a25bd1bfa35e383597fec9

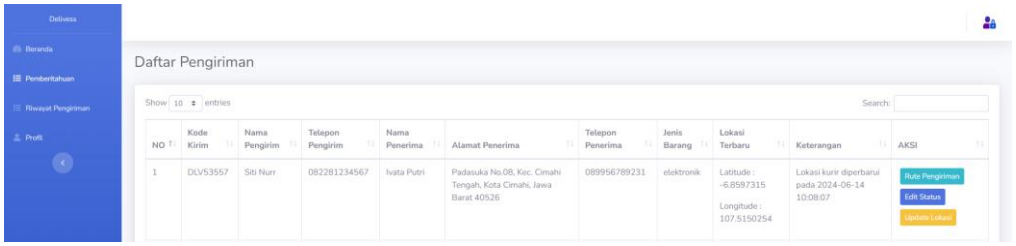
D. *Implementasi Algoritma AES (dekripsi)*

Setelah memastikan bahwa data lokasi pengirim dan penerima pada database tidak diubah, selanjutnya data tersebut akan di dekripsi yang kemudian pesanan tersebut akan masuk ke sistem admin, yang kemudian akan disetujui oleh admin dan diteruskan ke kurir. Ketika kurir akan mengirim paket, maka kurir terlebih dahulu melihat rute pengiriman, antar muka rute pengiriman kurir dapat dilihat pada Gambar 10 berikut ini.



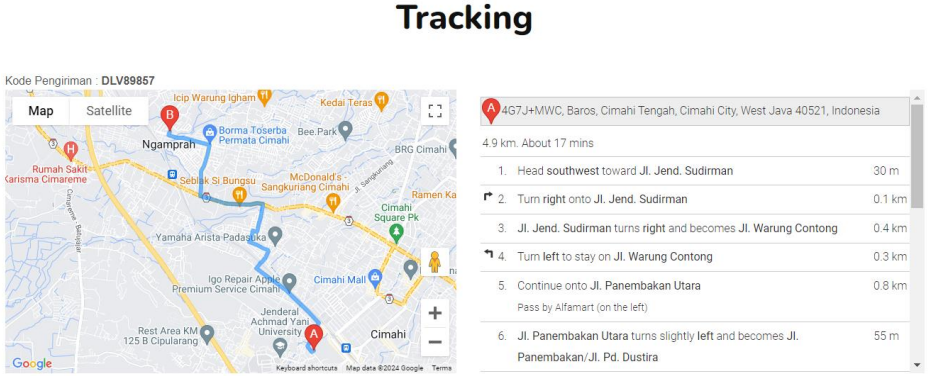
Gambar. 10. Rute Pengiriman (kurir)

Setelah kurir mengetahui lokasi pengiriman dan akan mengirim paket, maka dilakukan update lokasi kurir, dengan terlebih dahulu kurir memberi izin akses lokasi pada website agar dapat mengakses informasi lokasi dengan lebih akurat. Setelah disetujui akses lokasinya, pengambilan data lokasi dilakukan dengan melakukan update secara berkala oleh kurir di titik-titik check point yang telah ditentukan. Antar muka update lokasi kurir dapat dilihat pada Gambar 11 berikut ini.



Gambar. 11. Update lokasi (kurir)

Ketika berhasil mengambil lokasi kurir, maka langkah poin B dan C diulang sehingga lokasi kurir akan terenkripsi dan ter-*hashing* yang kemudian disimpan pada database, seperti terlihat pada Tabel II dan III. Kemudian, setelah memastikan bahwa data lokasi kurir pada database tidak diubah, selanjutnya data tersebut akan di dekripsi yang kemudian update lokasi kurir akan masuk ke sistem pelanggan, sehingga dapat melakukan lacak pengiriman paket setelah kurir melakukan update lokasi. Antar muka lacak pengiriman dapat dilihat pada Gambar 12 berikut ini.



Gambar. 12. Lacak Pengiriman (pelanggan)

E. *Pengujian t-test*

Pengujian ini dilakukan untuk membandingkan waktu tempuh aplikasi sebelum dan sesudah menggunakan Algoritma AES dan SHA-3. Pengujian dilakukan menggunakan tools BlazeMeter dan Apache JMeter. Kemudian hasilnya dibandingkan dan dianalisis menggunakan metode independent sample t-test untuk menentukan apakah terdapat perbedaan waktu respon yang signifikan pada website pengiriman antara sebelum dan sesudah penerapan Algoritma AES dan SHA-3.

TABEL V
HASIL PENGUJIAN PERFORMA SISTEM

Percobaan ke-	Banyak Data	Waktu tempuh tanpa algoritma AES dan SHA-3	Waktu tempuh dengan algoritma AES dan SHA-3	Peningkatan Waktu
1	10	4,277	5,649	1,372
2	20	4,474	5,952	1,478
3	30	4,660	6,021	1,361
4	40	4,852	6,040	1,188
5	50	5,092	6,489	1,397
6	60	5,274	6,598	1,324
7	70	5,320	6,967	1,647
8	80	5,509	6,968	1,459
9	90	6,175	7,614	1,439
10	100	6,484	8,061	1,577
Rata-rata		5,212	6,636	1,424

Terdapat ketentuan dalam pengambilan keputusan sebagai berikut:

H0: Tidak terdapat perbedaan yang signifikan pada waktu tempuh sebelum dan sesudah website pengiriman diimplementasikan Algoritma AES dan SHA-3.

H1: Terdapat perbedaan yang signifikan pada waktu tempuh sebelum dan sesudah website pengiriman diimplementasikan Algoritma AES dan SHA-3.

Kriteria untuk keputusan tersebut adalah sebagai berikut:

a. Probabilitas (sig.) > 0,05 maka H0 diterima;
b. Probabilitas (sig.) < 0.05 maka H0 ditolak.

Hasil pengukuran waktu tempuh website pengiriman menggunakan t-test menunjukkan bahwa nilai probabilitas (Sig.) masing-masing 0,00022 dan 0,00044. Karena nilai probabilitas (Sig.) berada di bawah 0.05, H0 ditolak dan H1 diterima, yang berarti ada perbedaan signifikan dalam waktu respon sebelum dan sesudah website delivery diterapkan Algoritma AES dan SHA-3. Perbedaan signifikan ini terjadi karena adanya dua kali pemrosesan algoritma pada data masukan. Pertama, data dimasukkan ke dalam Algoritma AES untuk menghasilkan output Cipher Text, yang kemudian digunakan sebagai masukan untuk Algoritma SHA-3 untuk menghasilkan Digest Text.

F. *Pengujian Avalanche Effect*

Pada pengujian *avalanche effect* ini dilakukan perubahan satu bit pada input teks atau pesan awal, dan akan dienkripsi menggunakan algoritma yang diuji, lalu hasilnya dibandingkan dengan output asli (sebelum bit diubah). Perbedaan antara kedua output diukur dengan menghitung jumlah bit yang berubah. Hasil pengujian akan menunjukkan apakah perubahan kecil pada input menghasilkan perubahan yang signifikan dan acak pada output, yang merupakan indikator kekuatan dan keamanan algoritma. Analisis ini dilakukan untuk memastikan bahwa algoritma memenuhi sifat *avalanche effect* yang diharapkan dalam kriptografi.

TABEL VI
HASIL PENGUJIAN AVALANCHE EFFECT

No	Input Awal	Ciphertext awal	Input yang diubah	Ciphertext yang diubah	Perbedaan Ciphertext (bit)	Persentase Perbedaan (%)
1	-6.909529	2jHSzC3kDlvU6WceNF/B/g==	-6.919529	Ia3R5U939BVks8qFoK1cTg==	77	40%
2	107.597495	2/RRjpNZJwgDqQqr0B/U+g==	107.597485	v2PCP6PQDK9Lw7ldFWAGzQ==	73	38%
3	-6.919529	Ia3R5U939BVks8qFoK1cTg==	-6.919549	w27DUDDUGQtt0juOdtbkqQ==	73	38%
4	107.597485	v2PCP6PQDK9Lw7ldFWAGzQ==	107.596485	wSaX1uazt/AaJSVhodznIw==	71	37%
5	-6.917549	YZwSRVqOoB3o+9jI3ETn	-6.617549	MhEDXe90NxY1UHQSvslw	77	40%
…	…	…	…	…	…	…
15	-6.914539	dmIdawYzAUUrUM2I9bpv	-6.714539	lflGQlfyVJk1qVYsAcBY	75	39%
Rata-rata					73.33	38.27%

Pada pengujian *avalanche effect* ini, target ideal adalah sekitar 50% perubahan bit pada output. Hal ini menunjukkan bahwa algoritma sangat sensitif terhadap perubahan kecil pada input, yang merupakan karakteristik keamanan yang diinginkan. Namun, rentang antara 45% hingga 60% masih dianggap sangat baik dan menunjukkan properti keamanan yang kuat [19].

Dalam pengujian yang telah dilakukan, didapat hasil rata-rata persentase perbedaan bit yakni sekitar 38.27%. Hasil ini menunjukkan bahwa algoritma AES untuk data lokasi tersebut memiliki properti *avalanche effect* yang dianggap kurang baik dan tidak memenuhi standar keamanan yang diharapkan karena tidak masuk dalam rentang nilai antara 45% hingga 60%.

G. *Pengujian Integritas*

Pengujian ini bertujuan untuk memastikan validitas *hashing* data. Algoritma SHA-3 tidak memungkinkan digest text yang dihasilkan untuk diubah kembali ke plain text. Untuk memastikan keakuratannya, dilakukan pengujian integritas dengan mencocokkan hasil digest text dari dua inputan yang sama. Jika hasil dari kedua pengujian tersebut identik, maka Algoritma SHA-3 yang digunakan dapat dianggap valid. Hasil pengujian ini adalah sebagai berikut.

TABEL VII
HASIL PENGUJIAN INTEGRITAS

No	Ciphertext AES	Digest text SHA-3	Digest text SHA-3 (database)	Integritas Terjamin
1	I4cHvAJnljgmOslIqqx7nA==	3937a47279bf2a182c5ea5ffd124cb9de38ffdcfd6ccb9c0192b1f71970f171f	3937a47279bf2a182c5ea5ffd124cb9de38ffdcfd6ccb9c0192b1f71970f171f	Ya
2	BK1o2/W3+f/MSbkHadHV1A==	217a2a35f7fd09e832ecc674b0a1ad5b740223662f1dd2fc275848860db79554	217a2a35f7fd09e832ecc674b0a1ad5b740223662f1dd2fc275848860db79554	Ya
3	c5e2Q64oaDeJZld8yBumLw==	54882d18f3288e710c47753a43bcf2dabfc7acbf1eff7f0a2569d5a7f6341d28	54882d18f3288e710c47753a43bcf2dabfc7acbf1eff7f0a2569d5a7f6341d28	Ya
4	wBV53YZJXkzl+NQ4963Mtw==	7aae8d57ee83284e15ee6e3cbf7d09d15e195c7923fc32e17f4ddb59eed9a878	7aae8d57ee83284e15ee6e3cbf7d09d15e195c7923fc32e17f4ddb59eed9a878	Ya
5	+4fdgJdHHihsSRWqBahOtg==	dd5f55e4f2756a8bcb0033de11d92464488f7d82069f4b3b55c17052be7c0351	dd5f55e4f2756a8bcb0033de11d92464488f7d82069f4b3b55c17052be7c0351	Ya
…	…	…	…	…

30	oXXbVmdLXxB98K4II7ko3A==	b9d73015564080df9ba8409c3ed9a7fd9b0659943f7b22b23ff18c3be4b2a651	b9d73015564080df9ba8409c3ed9a7fd9b0659943f7b22b23ff18c3be4b2a651	Ya

Dari Tabel VII tersebut, dapat disimpulkan bahwa digest text yang dihasilkan sesuai dengan hasil dari percobaan digest pertama. Dengan demikian, aspek integritas terpenuhi, dan Algoritma SHA-3 yang digunakan terbukti valid.

V. KESIMPULAN

Penelitian ini menunjukkan bahwa penggunaan algoritma AES dan SHA-3 untuk pengamanan data lokasi pada layanan berbasis lokasi (LBS) berupa website pengiriman, memberikan perlindungan privasi yang efektif dengan performa sistem yang memadai. Waktu enkripsi dan dekripsi serta *hashing* berada dalam batas yang dapat diterima, dengan integritas data terjaga selama transmisi dan penyimpanan, meskipun algoritma AES untuk data lokasi ini menunjukkan *avalanche effect* yang kurang baik. Hasil pengujian menunjukkan bahwa kombinasi AES untuk enkripsi dan SHA-3 untuk *hashing* memberikan performa sistem yang memadai, dengan waktu rata-rata yang diperlukan untuk melakukan pemrosesan data dari saat pengguna melakukan pemesanan hingga data masuk dan diterima oleh kurir dan admin dengan menggunakan Algoritma AES dan SHA-3 adalah 6,636 detik, dimana terdapat peningkatan waktu proses sebesar 1,424 detik setelah implementasi Algoritma AES dan SHA-3. Di samping itu, algoritma AES untuk data lokasi ini tidak memenuhi kriteria *avalanche effect*, dimana perubahan kecil pada input menghasilkan perubahan signifikan pada output, yang penting untuk keamanan kriptografi. Namun, aspek integritas dapat dipenuhi dari penerapan SHA-3 yang dibuktikan dengan adanya pengujian integritas. Digest text yang dihasilkan pada beberapa percobaan dengan inputan sama terbukti menghasilkan digest text yang sama, menunjukkan bahwa tidak ada perubahan atau manipulasi selama transmisi atau penyimpanan. Hasil penelitian ini sejalan dengan teori-teori kriptografi sebelumnya yang mengemukakan bahwa AES dan SHA-3 adalah algoritma yang aman dan efisien. Dengan menyediakan bukti empiris bahwa kombinasi kedua algoritma ini efektif dalam melindungi data lokasi dalam konteks LBS, penelitian ini membuka peluang untuk penerapan yang lebih luas dalam aplikasi serupa.

DAFTAR PUSTAKA

[1] N. Imansyah and S. H. Widiastuti, "Layanan Berbasis Lokasi Hotel Menggunakan Realitas Tertambah," *Jurnal Sistem Informasi Bisnis*, vol. 7, no. 2, p. 120, Nov. 2017, doi: 10.21456/vol7iss2pp120-130.

[2] M. Ali Mukhti and Malabay, "Rancang Bangun Sistem Informasi Sembako Online Berbasis Web dengan Layanan Berbasis Lokasi Studi Kasus : Agen Sembako H. Nasril," 2022. [Online]. Available: http://jurnal.umj.ac.id/index.php/semnaslit

[3] B. Raka Sakti, W. Witanti, and A. I. Hadiana, "Sistem Informasi Bank Darah dengan Location Based Service untuk Meningkatkan Efisiensi Pencarian Golongan Darah (Studi Kasus: UTD PMI Cimahi)," *IJIRSE: Indonesian Journal of Informatic Research and Software Engineering*, vol. 1, pp. 105–111, Sep. 2021, Accessed: Nov. 18, 2023. [Online]. Available: https://journal.irpi.or.id/index.php/ijirse

[4] A. Nur and A. Ansar, "Pengaruh Aplikasi Pelacak Lokasi Terhadap Keamanan Privasi Pengguna Media Sosial," *Jurnal Penelitian Ilmu Hukum*, vol. 2, no. 3, pp. 112–120, 2022, doi: 10.56393/nomos.v1i5.599.

[5] Y. He and J. Chen, "User location privacy protection mechanism for location-based services," *Digital Communications and Networks*, vol. 7, no. 2, pp. 264–276, May 2021, doi: 10.1016/j.dcan.2020.07.012.

[6] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location Privacy-preserving Mechanisms in Location-based Services," *ACM Computing Surveys*, vol. 54, no. 1. Association for Computing Machinery, Apr. 01, 2021. doi: 10.1145/3423165.

[7] I. Liliasari, R. Yusvi, A. Kusyanti, and D. P. Kartikasari, "Implementasi Algoritme Grain dan SHA-3 untuk Data Lokasi," 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[8] R. Wijaya, K. Farandi, and S. Miharja, "Implementasi Algoritma AES-128 Dan SHA-256 dalam Perancangan Aplikasi Pengamanan File Dokumen," 2021.

[9] S. Praptodiyono, M. A. Sidiq, and F. Muhammad, "Implementasi Algoritma SHA-3 Dan AES Sebagai Sistem Keamanan Pada Proses Pensinyalan Mobile IPv6," *Setrum : Sistem Kendali-Tenaga-elektronika-telekomunikasi-komputer*, vol. 10, no. 2, Nov. 2021, doi: 10.36055/setrum.v10i2.13075.

[10] V. M. Ferreira and F. Ramos, "Promoting Face-to-Face Communication through the Use of a New Micro-broadcasting Location Based-service," *Procedia Technology*, vol. 16, pp. 150–162, 2014, doi: 10.1016/j.protcy.2014.10.078.

[11] A. Soraja, "Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Prespektif HAM," Dec. 2021.

[12] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," vol. 4, no. 2, p. 75, 2021.

[13] J. A. Buchmann, "AES," 2004, pp. 139–149. doi: 10.1007/978-1-4419-9003-7_6.

[14] I. Lewenusa and P. Karo Karo, "Kriptografi Algoritma Advanced Encryption Standard Dan Pengecekan Error Detection Cyclic Redundancy Check." [Online]. Available: http://fti.tarumanagara.ac.id/jurnal/index.php/jki

[15] D. S. Maylawati, W. Darmalaksana, and M. A. Ramdhani, "Systematic Design of Expert System Using Unified Modelling Language," *IOP Conf Ser Mater Sci Eng*, vol. 288, p. 012047, Jan. 2018, doi: 10.1088/1757-899X/288/1/012047.

[16] F. Kurniawan, A. Kusyanti, and H. Nurwarsito, "Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost," 2017. [Online]. Available: http://j-ptiik.ub.ac.id

[17] R. Kurniawan Endrayanto, A. Muttaqin, and R. A. Setyawan, "Advanced Encryption Standard (AES) pada Modul Internet of Things (IoT)," *TELKA*, vol. 5, no. 2, pp. 103–113, 2019.

[18] D. Calista, A. Farissi, and M. Diana Marieska, "Sistem Pengamanan Data Menggunakan Kriptografi AES dan Blockchain Berbasis Android," Bulan Oktober, 2021.

[19] I. Fitriani and A. Baskoro Utomo, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa," 2020.