ANALISIS PENGGUNAAN *LOCATION-BASED SERVICE* DENGAN *K-ANONYMITY* UNTUK MENJAGA PRIVASI DAN KEAMANAN PENGGUNA SISTEM PEMANTAUAN DAN PERINGATAN DAERAH RAWAN KECELAKAAN

Doni Hadimas Aprilian, Asep Id Hadiana, Agus Komarudin
Teknik Informatika, Universitas Jenderal Achmad Yani
Jl. Terusan Jend. Sudirman, Cimahi, Jawa Barat, Indonesia
doni.hadimas@student.unjani.ac.id

ABSTRAK

Pemantauan dan peringatan memiliki proses penting dalam mengidentifikasi dan mengevaluasi perubahan serta kinerja sistem atau program. Dalam konteks keselamatan berkendara, pemantauan kondisi jalan dan peringatan terhadap situasi berbahaya sangat diperlukan untuk mengurangi risiko kecelakaan. Pengguna jalan memerlukan informasi terkait lokasi yang rentan kecelakaan agar dapat mengambil keputusan yang tepat. Location Based Services (LBS) menyediakan informasi geografis melalui telepon seluler, dengan dua metode implementasi yaitu pemrosesan data lokasi di server. Kompleksitas waktu algoritma geofencing, pemantauan, dan peringatan kecelakaan bersifat linier seiring dengan ukuran data. Implementasi K-Anonymity juga menunjukkan kompleksitas waktu linier. Hasil penelitian menunjukkan bahwa K-Anonymity, setelah diuji menggunakan entropi, mencapai nilai 3.2456767, yang mencerminkan keberhasilan dalam mengurangi ketidakpastian dalam distribusi probabilitas atribut lokasi pengguna. Selain itu, rasio K-Anonymity yang mencapai 0.21 mencerminkan keberhasilan dalam menjaga privasi pengguna dalam sistem peringatan kecelakaan, di mana setiap kelompok yang terbentuk rata-rata mencakup 21% dari total data yang ada.

Kata kunci : *Geofencing, K-Anonymity, Location Based Service*

1. PENDAHULUAN

Pemantauan merupakan sebuah proses pengumpulan, analisis dan interpretasi data yang dilakukan secara sistematis yang berfungsi untuk mengidentifikasi dan mengevaluasi perubahan ataupun kinerja dari suatu sistem atau program[1].

Sedangkan, peringatan merupakan suatu kegiatan atau tindakan memberikan notifikasi kepada seseorang ataupun kelompok mengenai situasi atau kondisi yang dapat membahayakan atau perlu melakukan sebuah tindakan terhadap suatu kondisi tersebut[2].

Seringkali pemantauan dan peringatan perlu atau penting dilakukan agar dapat mengambil keputusan secara cepat dan tepat, contohnya ketika berkendara, dalam kegiatan tersebut mungkin dapat terjadi kelalaian atau juga ketidaktahuan terhadap kondisi jalan di lokasi tersebut yang dapat membahayakan, sehingga diperlukan pemantauan dan juga pemberian peringatan ketika akan terjadi kelalaian pada saat berkendara pada saat berkendara atau ketika pengendara memasuki lokasi yang rentan kecelakaan, sehingga dengan melakukan pemantauan dan peringatan tersebut dapat meminimalisir terjadinya kecelakaan atau hal yang tidak diinginkan.

Pengendara atau pengguna jalan memerlukan informasi-informasi terkait kondisi jalan atau lokasi di sekitar pengguna jalan, khususnya informasi terkait lokasi yang rentan kecelakaan, dengan melakukan pemantauan dan juga peringatan terkait lokasi yang rentan kecelakaan sehingga dapat mengurangi faktor lingkungan yang menyebabkan kecelakaan serta membantu pengguna jalan dalam mengambil keputusan ketika memasuki area atau lokasi yang rentan kecelakaan[3].

Pemantauan dan peringatan yang melibatkan akses lokasi dari pengguna adalah salah satu hal yang perlu diperhatikan karena data tersebut termasuk ke dalam privasi pengguna sehingga penting untuk diamankan[4].

LBS atau *Location Based Service* adalah layanan yang dipergunakan untuk memberikan informasi terkait lokasi kepada pengguna berdasarkan informasi geografis yang didapatkan dari melalui telepon seluler pengguna[5].

Telepon seluler memiliki fitur untuk dapat mengakses berbagai layanan yang berbasis lokasi, dalam hal tersebut terdapat 2 metode untuk mengimplementasikan LBS yaitu, memproses data lokasi di *server* lalu dikirim dan di-*generate* respon ke *client*, Lokasi tersebut dapat direpresentasikan ke dalam ketentuan spasial, dimana lokasi spasial direpresentasikan dalam penggunakan sistem koordinat lintang bujur ketinggian[6].

Di penelitian sebelumnya yang berjudul "A Generalized Location Privacy Protection Scheme in Location Based Services" yang dilakukan oleh Jing-Jing Wang dkk, menyebutkan bahwa skema perlindungan privasi *generalized K-Anonymity* dapat menjamin pengguna mendapatkan lokasi yang akurat tanpa adanya kebocoran informasi dari geo-lokasi pengguna, serta hasil analisis dari penelitian tersebut menyatakan LPPS-GKA lebih aman untuk melindungi privasi yang termasuk didalamnya informasi dari region, dan juga lebih efisien daripada skema yang mirip dalam aspek komputasi dan komunikasi[4].

Penelitian lainnya yang dilakukan oleh Hasan Takabi dkk yang berjudul "A Collaborative K-Anonymity Approach for Location Privacy in Location-Based Services", menyatakan bahwa penelitian yang menggunakan pendekatan kooperatif terdistribusi untuk privasi LBS berdasarkan *K-Anonymity* tidak ada pihak yang dapat mempelajari atau mengetahui informasi tentang lokasi pengguna selain penyedia lokasi tersebut[7].

Oleh karena itu penelitian ini akan memfokuskan untuk menganalisa penerapan *K-Anonymity* untuk pemantauan dan peringatan kecelakaan bagi pengguna jalan menggunakan *Location Based Service* dapat menjaga informasi terkait data data sensitif pengguna ketika dilakukan pemantauan dan peringatan kepada pengguna.

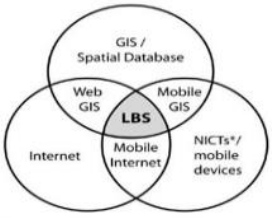
2. TINJAUAN PUSTAKA

2.1. Location Based Service

Location Based Service (LBS) adalah layanan yang berbasis pada posisi geografis pengguna. Teknologi ini sering digunakan untuk mencari tempat yang akan dituju, mirip dengan pencarian menggunakan peta biasa, namun LBS juga menyediakan informasi tambahan tentang posisi objek yang bergerak [8].

Location Based Services menggunakan nilai longitude dan latitude untuk menentukan lokasi yang diinput. Longitude dan latitude adalah sistem koordinat geografis yang digunakan untuk menentukan lokasi di permukaan bumi. Latitude menunjukkan posisi utara atau selatan ekuator, sedangkan longitude menunjukkan posisi di wilayah barat atau timur [9].

Location Based Service direpresentasikan sebagai sebuah layanan yang berada pada pertemuan tiga teknologi yaitu: *Geographic Information System, Internet Service,* dan *Mobile Devices*, yang dapat dilihat pada Gambar 1 berikut ini:



Gambar 1. Location Based Service Sebagai Persimpangan Tiga Teknologi

2.2. Geofencing

Geofencing adalah sebuah teknologi yang dapat mengetahui lokasi pengguna ketika pengguna memasuki atau melewati area *geofence*[12].

Geofencing terdiri dari batas virtual yang dibuat di sekitar zona geografis atau lokasi tertentu, yang dapat disebut dengan *geofence*[13].

Geofence dapat digambarkan dengan area geografik, dimana area geografik tersebut ada beberapa tipe[14], yaitu :

Table 1. Tipe Area Geofence

Category	Schema Addressing	Instances	Example
Spatial Geofence	Geometris	Bulat, Poligon, Polylines	"Wilayah Bandung"
Hierarchy based Geofences	Simbolis	Country, City, Street,...	Indonesia, Bandung, Banjaran
Network Based Geofences	Simbolis	Cell-Id, WLAN-B, SSID	"BSSID WLAN di KFC"
Semantic Geofences	Geometris dan Simbolis	Kombinasi Dari 3 kategori di atas	"Dekat dengan Restoran KFC"

Geofencing mempertimbangkan geo-konteks, yang berkaitan dengan area tertentu. Ketika pengguna memasuki area dengan nilai konteks yang sesuai, perangkat dapat mengirimkan notifikasi dan informasi tentang area tersebut [15].

Fungsi utama geofencing adalah memonitor smartphone melalui peta virtual saat perangkat keluar atau memasuki area yang dibatasi oleh pagar virtual. Beberapa teknik utama geofencing meliputi *Geofenced Area, Proximity with a Point of Interest, Route Adherence*, dan *Route and Schedule Adherence*. Dalam penelitian ini, teknik yang digunakan adalah Geofenced Area.

2.3. Haversine Formula

Algoritma yang digunakan untuk menghitung suatu jarak dengan mengambil kedua titik permukaan bumi yang digunakan dalam suatu rute dan memberikan suatu jarak lingkaran besar dengan mengambil *longitude* dan *latitude* sebagai inputannya, sehingga *latitude* dan *longitude* dapat memberikan informasi jarak dari kedua titik tersebut[16]. Berikut ini rumus Formula *Haversine*.

$$\Delta lat = \frac{\pi}{180} * (lat_1 - lat_2) \quad (1)$$

$$\Delta long = \frac{\pi}{180} * (long_1 - long_{2)} \quad (2)$$

$$\alpha = sin^2\left(\frac{\Delta lat}{2}\right) + \cos(lat_1) . \cos(lat_2) . sin^2\left(\frac{\Delta long}{2}\right) \quad (3)$$

$$c = 2 . atan^2(\sqrt{1-a}, \sqrt{a}) \quad (4)$$

$$d = R . c \quad (5)$$

Dimana:
Δlat : *Latitude*
$\Delta long$: *Longitude*
R : Jari-Jari bumi sebesar 6371 (km)
c : Titik potong sumbu atau jarak angular (radian)
d : Jarak (km)

Perhitungan Algoritma *Haversine* dilakukan dengan menggunakan jarak lingkaran antara garis lintang dan garis bujur, yang mana jari-jari diasumsikan 6.371 km, dan 2 titik pada koordinat lintang dan bujur[17].

Nilai Koordinat didapatkan dari hasil perhitungan dari *latitude* dan *longitude*, *latitude* direpresentasikan dengan simbol *Phi*, sedangkan *longitude* disimbolkan dengan *Lambda*[18].

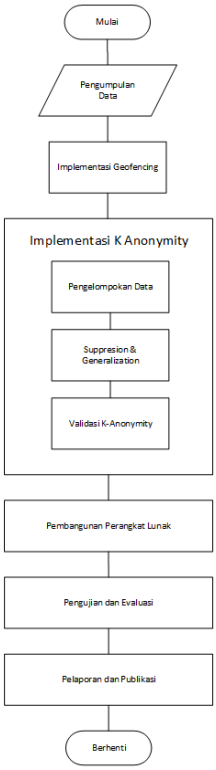
2.4. Global Positioning System (GPS)

Sistem navigasi satelit yang berfungsi untuk menentukan lokasi, kecepatan, dan arah, melalui *signal* yang diterima lebih dari 24-32 satelit yang berorbit 20.000 km (11.000 mil laut) di atas bumi disebut dengan *Global Positioning System* (GPS). GPS *receiver* memerlukan empat atau lebih satelit untuk menghasilkan jarak mereka, dan menggunakan informasi ini untuk menyimpulkan lokasi mereka. Sehingga operasi ini disebut dengan *triangulation*[10].

Sistem ini menggunakan lebih dari 4 satellit untuk dapat mengirimkan gelombang mikro ke bumi, dan kemudian sinyal akan diterima di permukaan oleh *receiver* yang dapat digunakan untuk menentukan posisi, kecepatan, arah, dan waktu[19].

Cara kerja GPS dimulai dengan perhitungan triangulasi dari tiga satelit terdekat untuk menentukan posisi receiver. Jarak antara titik persilangan ketiga satelit akan diidentifikasi sebagai lokasi receiver. Posisi ini kemudian dikirim ke satelit melalui controller di bumi. Untuk menghitung jarak yang akurat, posisi dan ketinggian orbit satelit perlu diketahui. Setelah itu, controller mengoreksi delay sinyal yang terjadi selama perjalanan di atmosfer hingga diterima kembali oleh receiver.

3. METODE PENELITIAN



Gambar 2. Metodologi Penelitian

Penelitian ini menggunakan beberapa tahapan yang dilakukan, pertama yaitu pengumpulan data untuk menentukan data-data yang akan digunakan, kedua implementasi geofencing, tahap ketiga implementasi K-Anonymity dimana meliputi pengelompokan data, suppresion, generization, serta validasi K-anonymity. Tahap keempat pembangunan perangkat lunak, tahap kelima pengujian dan evaluasi, tahap terakhir yaitu pelaporan dan publikasi imliah.

3.1. Analisis Implementasi Geofencing

Dataset titik titik rawan kecelakaan di Kota Bandung dan Kabupaten Bandung di saring atau dilakukan filter data dengan menggunakan haversine formula dengan radius 200 meter dari lokasi terkini pengguna, berikut simulasi perhitungan untuk menentukan titik titik yang ditampilkan dengan haversine formula.

Misalkan:
$Titik\ A : (-6.9175, 107.6189)$
$Titik\ A : (-6.9173, 107.6190)$
Konversi Koordinat lokasi Kedalam Radian :

$$lat1 = -6.9175 \times \left(\frac{3.14}{180}\right) = -0{,}1205\ rad \quad (1)$$

$$lat2 = -6.9173 \times \left(\frac{3.14}{180}\right) = -0.1204\ rad \quad (2)$$

$$lon1 = 107.6189 \times \left(\frac{3.14}{180}\right) = 1.8789\ rad \quad (3)$$

$$lon2 = 107.6190 \times \left(\frac{3.14}{180}\right) = 1.8789\ rad \quad (4)$$

Perhitungan Selisih Koordinat Titik A dan B

$$\Delta lat = lat2 - lat1 = -0.0001\ rad \quad (5)$$

$$\Delta lon = lon2 - lon1 = -0.0000\ rad \quad (6)$$

Perhitungan dengan menggunakan Haversine Formula:

$$a = sin^2\left(\frac{\Delta lat}{2}\right) + \cos(lat1) \cdot \cos(lat2) \cdot sin^2\left(\frac{\Delta lon}{2}\right) = 0.000001 \quad (7)$$

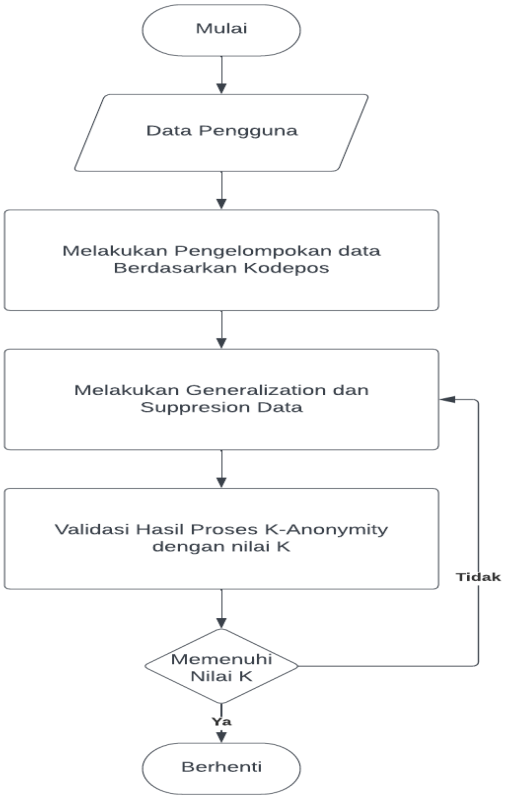
$$c = 2 \cdot atan^2\left(\sqrt{0.000001}, \sqrt{1 - 0.000001}\right) = 0.0025 \quad (8)$$

$$distance = 6371000 \cdot 0.0025 = 15.9\ meter \quad (9)$$

Setelah mengidentifikasi titik yang berjarak kurang dari 200 meter dari lokasi pengguna, data tersebut diproses untuk membuat circular geofence dengan radius 116.5 meter (0.0015 derajat) dan melibatkan 20 titik di sekitarnya. Menggunakan Haversine formula, sistem memberikan peringatan kepada pengguna hanya jika mereka berada dalam jarak 200 meter dari titik rawan kecelakaan, memastikan peringatan yang relevan dan memungkinkan tindakan pencegahan yang lebih efektif.

3.2. Analisis Implementasi K-Anonymity

Dalam implementasi K-Anonymity pada dataset pengguna, langkah awal dilakukan dengan menciptakan dummy data tambahan (500-1000 entitas) untuk menghasilkan dataset yang cukup besar. Dataset ini mencakup atribut penting seperti nama, alamat, nomor handphone, email, tanggal lahir, dan lokasi terkini pengguna. Tahapan implementasi K-Anonymity dapat dilihat pada gambar berikut.



Gambar 3. Flow Implementasi K-Anonymity

4. HASIL DAN PEMBAHASAN

4.1. Pengumpulan Atribut Data Pengguna

Pengumpulan atribut data pengguna ini digunakan tujuh buah atribut diantaranya yaitu id, nama, alamat, nomor telepon, email, tanggal lahir, dan lokasi yang dimana dapat dilihat pada Tabel 2 dibawah ini.

Table 2. Atribut Data Pengguna

No	Atribut Data	Deskripsi
1	id	Id unik yang digunakan untuk mengidentifikasi data
2	nama	Nama dari pengguna aplikasi
3	alamat	Berisikan detail Alamat pengguna meliputi kampung, desa, kode pos, kota, provinsi, dan negara
4	nomor_ handphone	Nomor Handphone yang didaftarkan pada aplikasi
5	email	Email yang didaftarkan pada aplikasi
6	tanggal_ lahir	Tanggal lahir pengguna
7	lokasi	Lokasi berisikan latitude dan longitude pengguna secara realtime

4.2. Dataset Pengguna

Dataset berikut adalah beberapa contoh data dummy pengguna yang di generate manual dengan format JSON, karena keterbatasan device untuk melakukan implementasi algoritma K-Anonymity sehingga mengharuskan untuk melakukan generate data dummy pengguna yang di perlukan. Pada penggunaan dataset ini terdiri dari id, nama, alamat secara detail, nomor telepon, email, tanggal lahir, dan lokasi dalam bentuk latitude serta longitude untuk digunakan dalam penelitian ini.

4.3. Atribut Data Titik Lokasi Rawan Kecelakaan

Pada Tabel 3 dibawah ini menjelaskan mengenai informasi data yang akan digunakan untuk menunjang penelitian ini yaitu sebagai berikut.

Table 3. Atribut Titik Lokasi Rawan Kecelakaan

No	Atribut Data	Deskripsi
1	type	Type data dari mapbox
2	geometry	Geometry berisikan type dan coordinates dari data meliputi type feature, longitude dan latitude
3	properties	Berisikan data data tambahan terkait dari data lokasi tersebut yang meliputi frequency_accident dan accident_cause

4.4. Dataset Titik Kecelakaan

Berikut adalah contoh data titik rawan kecelakaan yang didapatkan dari API Mapbox yang digunakan untuk menampilkan geofence dari titik titik rawan kecelakaan tersebut. Data set titik kecelakaan menggunakan beberapa atribut diantaranya yaitu type dan geometry.

4.5. Implementasi Geofencing

Gambar 4. Implementasi Geofencing

Proses implementasi geofencing pada aplikasi ditampilkan di menu home, yang menunjukkan peta lokasi pengguna dan geofence dari titik-titik rawan kecelakaan. Hanya titik-titik rawan yang berada dalam radius 200 meter dari pengguna yang ditampilkan, memastikan pengguna menerima peringatan yang relevan dan dapat mengambil tindakan pencegahan secara efektif, sebagaimana terlihat pada Gambar 4.

Setiap Titik rawan kecelakaan berisi informasi terkait titik rawan kecelakaan tersebut, seperti penyebab kecelakaan dan juga frekuensi kecelakaan pada titik tersebut, yang dapat dilihat pada Gambar 5.

Gambar 5. Informasi Terkait Titik Kecelakaan

Ketika Pengguna memasuki area geofencing titik rawan kecelakaan, pengguna akan mendapatkan notifikasi pada handphone pengguna yang berisi informasi penyebab kecelakaan, serta terdapat notifikasi suara sehingga pengguna tidak perlu melihat handphone ketika memasuki area rawan kecelakaan.

Gambar 6. Notifikasi Ketika Pengguna Memasuki Area geofencing

Gambar 7. Response time Pembuatan Geofencing

Pada aplikasi disediakan Analisis data performa aplikasi ketika pembuatan geofencing dalam bentuk chart sehingga mudah dipahami, yang dapat dilihat pada Gambar 7.

Terdapat juga chart analisis data response time mengirimkan pemberitahuan atau notifikasi ke pengguna ketika memasuki area rawan kecelakaan yang dapat dilihat pada Gambar 8.

Gambar 8. Response Time Mengirimkan Notifikasi

4.6. Implementasi K-Anonymity

Implementasi K-Anonymity pada halaman home menampilkan lokasi pengguna dan marker pengguna lain di sekitarnya. Data pengguna dikelompokkan berdasarkan kode pos, kemudian dilakukan generalisasi dan penyensoran. Selanjutnya, data divalidasi untuk memastikan memenuhi nilai K yang disimpan dalam pengaturan.

Gambar 9. Implementasi Marker Pengguna Lain

Gambar 10. Detail Pengguna Lain setelah diimplementasi K-Anonymity

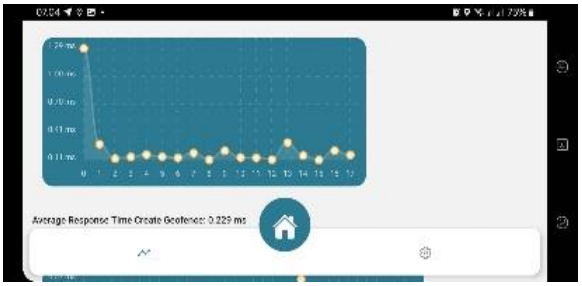
4.7. Pengujian

Proses ini melibatkan serangkaian langkah untuk memastikan perangkat lunak bebas dari kesalahan, dengan tujuan utama menemukan dan memperbaiki masalah. Dalam penelitian ini, fokus pengujian adalah mengukur efisiensi implementasi Geofencing dan K-Anonymity. Beberapa skenario rute ditetapkan untuk mengukur respons dan notifikasi saat pengguna memasuki area geofencing serta waktu respons dari implementasi K-Anonymity pada data pengguna. Beberapa contoh skenario rute melibatkan perjalanan dari:

1. Jl. Palalangon No.12 (-7.10401, 107.59641) ke Tugu Perintis (-7.08546, 107.56174)
2. Jl. Lengkong Bojongsoang (-6.97268, 107.63616) ke Miko Mall (-6.96013, 107.59075)

Pengujian pertama mengenai pengkuran waktu respons geofencing dan pengiriman notifikasi yang dimana ketahanan sistem bertujuan mengukur efisiensi notifikasi saat pengguna memasuki area geofencing titik rawan kecelakaan, dengan fokus pada waktu respons optimal. Tujuannya adalah memastikan notifikasi diterima cepat untuk mendukung respons dan kesadaran situasional, sehingga meningkatkan efektivitas tindakan pencegahan oleh pengguna. Pengujian dilakukan dengan dua rute berbeda untuk mendapatkan hasil yang diharapkan.

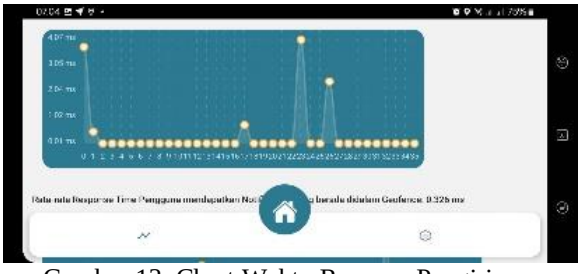
a. Rute Pertama



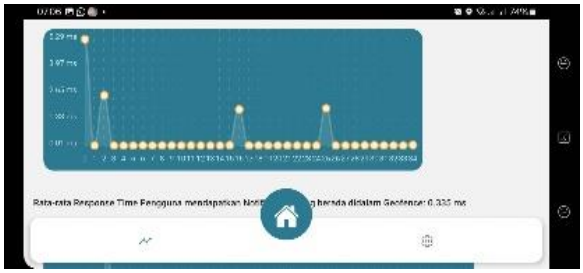
Gambar 11. Chart Waktu Respons Pembuatan Geofence Dengan K-Anonymity

Gambar 12. Chart Waktu Respons Pembuatan Geofence tanpa K-Anonymity

Rata-rata waktu respons untuk pembuatan geofence dengan penerapan K-Anonymity adalah sekitar 0.253 ms, sebagaimana terlihat pada Gambar 11. Sementara itu, pada implementasi tanpa K-Anonymity, mencapai rata-rata waktu respons sebesar 0.361 ms, sebagaimana ditunjukkan pada Gambar 12.



Gambar 13. Chart Waktu Respons Pengiriman Notifikasi dengan K-Anonymity

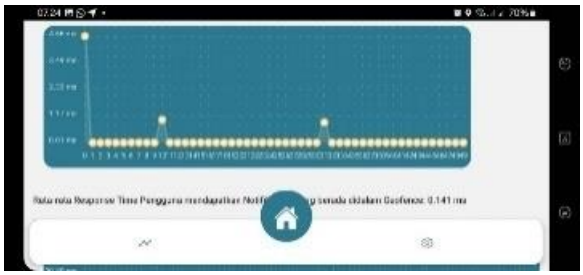


Gambar 14. Chart Waktu Respons Pengiriman Notifikasi tanpa K-Anonymity

Untuk rata-rata pengiriman notifikasi kepada pengguna, implementasi K-Anonymity memberikan hasil sekitar 0.326 ms, seperti yang terlihat pada Gambar 13. Sementara itu, pada implementasi tanpa K-Anonymity, rata-rata waktu pengiriman notifikasi adalah 0.335 ms, sebagaimana ditunjukkan pada Gambar 14.

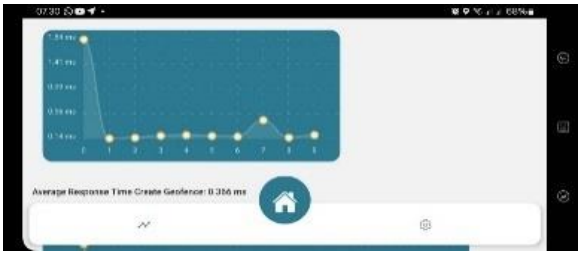
b. Rute Kedua

Gambar 15. Chart Waktu Respons Pembuatan Geofence dengan K-Anonymity



Gambar 16. Chart Waktu Respons Pembuatan Geofence tanpa K-Anonymity

Pada pengujian rute kedua, rata-rata waktu respons pembuatan geofence dengan implementasi K-Anonymity mencapai sekitar 0.263 ms, seperti yang terlihat pada Gambar 15. Sementara itu, pada implementasi tanpa K-Anonymity, waktu respons rata-rata adalah sekitar 0.141 ms, sebagaimana tergambar pada Gambar 16.



Gambar 17. Chart Waktu Respons Pengiriman Notifikasi dengan K-Anonymity

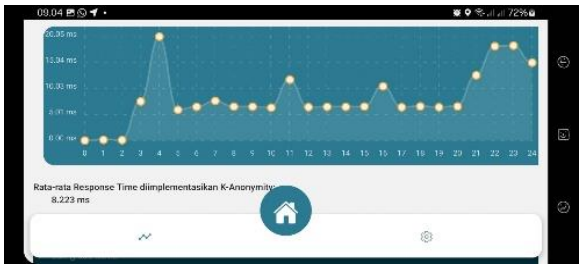
Gambar 18. Chart Waktu Respons Pengiriman Notifikasi tanpa K-Anonymity

Pada pengujian rute kedua, waktu respons rata-rata pengiriman notifikasi kepada pengguna dengan implementasi K-Anonymity mencapai sekitar 0.366 ms, sebagaimana terlihat pada Gambar 17. Sementara itu, untuk implementasi tanpa K-Anonymity, waktu respons rata-rata adalah sekitar 0.206 ms, seperti yang ditunjukkan pada Gambar 18.

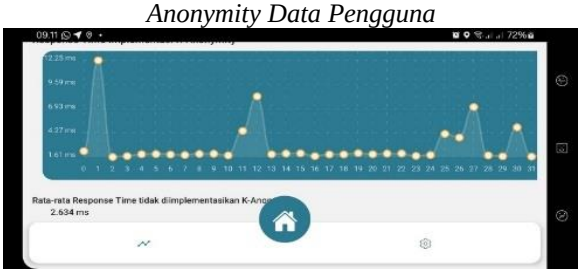
4.8. Pengujian Ukuran Waktu Respons K-Anonymity

Pengujian ketahanan sistem bertujuan untuk mengukur efisiensi implementasi K-Anonymity saat pengguna bergerak, dengan fokus pada waktu respons optimal setelah deteksi. Tujuannya adalah menjaga privasi data pengguna dan meningkatkan efektivitas tindakan pencegahan terhadap potensi kejahatan atau penyalahgunaan data pribadi di lingkungan tersebut.

a. Rute Pertama



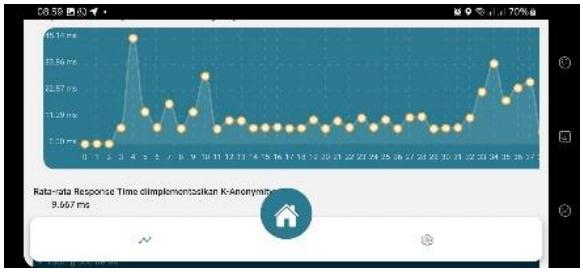
Gambar 19. Waktu respons Implementasi K-Anonymity Data Pengguna



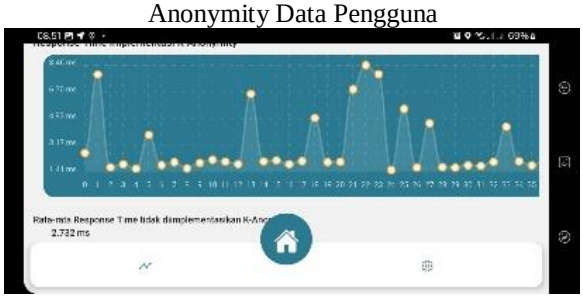
Gambar 20. Waktu respons tanpa Implementasi K-Anonymity Data Pengguna

Rata-rata waktu respons untuk Implementasi K-Anonymity pada data pengguna sistem adalah sekitar 8.223 ms, sebagaimana terlihat pada Gambar 19. Sementara itu, pada implementasi tanpa K-Anonymity, mencapai rata-rata waktu respons sebesar 2.634 ms, sebagaimana ditunjukkan pada Gambar 20.

b. Rute Kedua



Gambar 21. Waktu respons Implementasi K-Anonymity Data Pengguna



Gambar 22. Waktu respons tanpa Implementasi K-Anonymity Data Pengguna

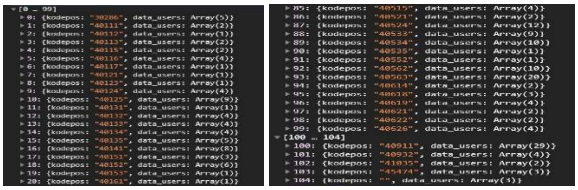
Pada Rute Kedua Rata-rata waktu respons untuk Implementasi K-Anonymity pada data pengguna sistem adalah sekitar 9.667 ms, sebagaimana terlihat pada Gambar 21. Sementara itu, pada implementasi tanpa K-Anonymity, mencapai rata-rata waktu respons sebesar 2.732 ms, sebagaimana ditunjukkan pada Gambar 22.

Meskipun terdapat perbedaan signifikan dalam waktu respons antara implementasi K-Anonymity dan tanpa K-Anonymity, perbedaan ini perlu dilihat dari segi keuntungan perlindungan privasi yang ditawarkan K-Anonymity. Rata-rata waktu respons untuk K-Anonymity adalah sekitar 8.223 ms, sedangkan tanpa K-Anonymity mencapai 2.634 ms. Pada rute kedua, perbedaan semakin jelas, dengan K-Anonymity mencatat rata-rata waktu respons sekitar 9.667 ms, sementara tanpa K-Anonymity sekitar 2.732 ms.

4.9. Perhitungan Entropy Data Hasil Implementasi

Perhitungan entropi dalam konteks K-Anonymity dilakukan untuk mengukur tingkat kepastian atau keacakan data setelah transformasi. Hasil implementasi K-Anonymity pada 500 data pengguna menunjukkan sekitar 105 kelompok dengan

kode pos berbeda, di mana setiap kelompok memiliki jumlah data antara 1 hingga 30.



Gambar 23. Data Hasil Implementasi K-Anonymity mulai 0-99

Untuk melakukan perhitungan Entropy digunakan formula sebagai berikut:

$$H(X) = -\sum_{i=1}^{n} P(xi) \cdot \log 2\,(P(xi))$$

Sehingga untuk menghitung entropy dari data hasil implementasi K-Anonymity langkah awal adalah Menghitung Probabilitas munculnya data pada setiap kodepos dari hasil implementasi K-Anonymity seperti berikut:

$$P(1) = \frac{20}{105} \qquad P(9) = \frac{2}{105}$$
$$P(2) = \frac{15}{105} \qquad P(10) = \frac{2}{105}$$
$$P(3) = \frac{17}{105} \qquad P(11) = \frac{1}{105}$$
$$P(4) = \frac{18}{105} \qquad P(12) = \frac{4}{105}$$
$$P(5) = \frac{8}{105} \qquad P(15) = \frac{1}{105}$$
$$P(6) = \frac{6}{105} \qquad P(20) = \frac{1}{105}$$
$$P(7) = \frac{4}{105} \qquad P(29) = \frac{1}{105}$$
$$P(8) = \frac{4}{105} \qquad P(30) = \frac{1}{105}$$

Setelah dilakukan perhitungan Probabilitas Munculnya data pada setiap kelompok, selanjutnya dilakukan perhitungan logaritma basis 2 pada setiap probabilitas

$$P(1) = \log 2\left(\frac{20}{105}\right) \qquad P(9) = \log 2\left(\frac{2}{105}\right)$$
$$P(2) = \log 2\left(\frac{15}{105}\right) \qquad P(10) = \log 2\left(\frac{2}{105}\right)$$
$$P(3) = \log 2\left(\frac{17}{105}\right) \qquad P(11) = \log 2\left(\frac{1}{105}\right)$$
$$P(4) = \log 2\left(\frac{18}{105}\right) \qquad P(12) = \log 2\left(\frac{4}{105}\right)$$
$$P(5) = \log 2\left(\frac{8}{105}\right) \qquad P(15) = \log 2\left(\frac{1}{105}\right)$$
$$P(6) = \log 2\left(\frac{6}{105}\right) \qquad P(20) = \log 2\left(\frac{1}{105}\right)$$
$$P(7) = \log 2\left(\frac{4}{105}\right) \qquad P(29) = \log 2\left(\frac{1}{105}\right)$$
$$P(8) = \log 2\left(\frac{4}{105}\right) \qquad P(30) = \log 2\left(\frac{1}{105}\right)$$

Sehingga untuk menghitung nilai entropy dengan memasukan hasil dari probabilitas munculnya data dengan hasil perhitungan logaritma dari hasil probabilitas data yang muncul sehingga didapatkah hasil seperti berikut:

i	P(i)	Log2(P(i))	P(i). Log2(P(i))
1	$\frac{20}{105}$	-2.3923174227787602	-0.38487
2	$\frac{15}{105}$	-2.807354922057604	-0.40105
3	$\frac{17}{105}$	-2.6267826764157833	-0.42630
4	$\frac{18}{105}$	-2.5443205162238103	-0.44090
5	$\frac{8}{105}$	-3.7142455176661224	-0.24373
6	$\frac{6}{105}$	-4.129283016944966	-0.34968
7	$\frac{4}{105}$	-4.714245517666122	-0.15349
8	$\frac{4}{105}$	-4.714245517666122	-0.15349
9	$\frac{2}{105}$	-5.714245517666122	-0.10926
10	$\frac{2}{105}$	-5.714245517666122	-0.10926
11	$\frac{1}{105}$	-6.714245517666122	-0.06403
12	$\frac{4}{105}$	-4.714245517666122	-0.15349
15	$\frac{1}{105}$	-6.714245517666122	-0.06403
20	$\frac{1}{105}$	-6.714245517666122	-0.06403
29	$\frac{1}{105}$	-6.714245517666122	-0.06403
30	$\frac{1}{105}$	-6.714245517666122	-0.06403
Total			-3,24567

H(X) = -(-3,24567)
H(X) = 3,2456767

Hasil pengujian implementasi K-Anonymity menunjukkan nilai entropi sebesar 3.2456767, yang mengindikasikan keberhasilan metode ini dalam mengurangi ketidakpastian distribusi probabilitas atribut lokasi pengguna. Nilai entropi yang positif menunjukkan bahwa K-Anonymity efektif dalam melindungi privasi dengan mengagregasi data lokasi dan meminimalkan potensi kebocoran identitas. Selain itu, nilai entropi yang tinggi menunjukkan adanya variasi dalam data lokasi, menekankan perlunya keseimbangan antara privasi dan fungsionalitas sistem.

4.10. Perhitungan K-Anonymity Ratio

Rasio ini memberikan gambaran tentang seberapa baik privasi data dapat dijaga dengan cara memastikan bahwa setiap individu dalam kelompok memiliki setidaknya K-1 individu lain yang memiliki nilai atribut serupa. Berikut adalah formula K-Anonymity Ratio:

$$KAnonymity\ Ratio = \frac{Jumlah\ Kelompok\ KAnonim}{Total\ Data}$$

Pada Data yang diimplementasikan K-Anonymity pada penelitian berjumlah sekitar 500 Data, dan setelah dilakukan implementasi jumlah hasil pengelompokannya adalah 105 kelompok sehingga dapat dihitung K-Anonymity Rationya seperti berikut:

$$KAnonymity\ Ratio = \frac{105}{500}$$
$$KAnonymity\ Ratio = 0{,}21$$

Hasil perhitungan K-Anonymity Ratio sebesar 0.21 menunjukkan keberhasilan implementasi K-Anonymity dalam menjaga privasi pengguna dalam sistem pemantauan dan peringatan daerah rawan kecelakaan. Setiap kelompok pengelompokan rata-rata mengandung 21% dari total data sebelumnya, menjadikan identitas individu lebih sulit diidentifikasi. K-Anonymity Ratio ini mencerminkan upaya mencapai keseimbangan antara privasi dan kegunaan data. Meskipun hasil ini positif, evaluasi lanjutan diperlukan untuk memahami dampak keseluruhan implementasi K-Anonymity, termasuk analisis kelompok data, uji coba skenario serangan, dan pertimbangan keamanan tambahan.

5. KESIMPULAN DAN SARAN

Penelitian ini menggunakan sistem Location-Based Services (LBS) untuk memantau lokasi pengguna secara real-time dan memberikan peringatan saat memasuki area rawan kecelakaan. Sistem ini memanfaatkan Geofencing dan Haversine Formula. Namun, sistem ini juga menimbulkan kekhawatiran privasi data pengguna. Oleh karena itu, penelitian ini menerapkan konsep k-anonymity untuk menjaga privasi pengguna. Pengujian menunjukkan bahwa penerapan k-anonymity hanya sedikit meningkatkan waktu respons, tetapi memberikan tingkat privasi yang lebih tinggi. Kompleksitas waktu algoritma geofencing dan k-anonymity sebanding dengan ukuran data. Pengujian juga menunjukkan bahwa k-anonymity berhasil mengurangi variasi data dan menjaga privasi pengguna. Meskipun terdapat peningkatan waktu respons, penerapan k-anonymity tetap dianjurkan karena manfaat perlindungan privasi yang signifikan.

Adapun saran untuk penelitian selanjutnya yaitu Gunakan algoritma yang lebih baik untuk mengirimkan notifikasi hanya pada rute yang dilalui pengguna, ukur tingkat akurasi dan keamanan data yang mengimplementasikan geofencing dan k-anonymity, dan pertimbangkan untuk menggunakan konsep privasi lain seperti Tokenization atau Differential Privasi, dengan tetap mempertimbangkan performa aplikasi.

DAFTAR PUSTAKA

[1] B. Dahal, U Uprety, 2015, "Monitoring & Evaluation System: Measuring Development Results-Based".

[2] Domingo, Sonny N and M. Arvie Joy A, 2018, "*Disaster Preparedness and Local Governace in The Philippines*".

[3] I. Samsudin, "ANALISA FAKTOR PENYEBAB KECELAKAAN PADA RUAS JALAN Ir. H. ALALA KOTA KENDARI DITINJAU DARI PRASARANA DAN GEOMETRIK JALAN," *Jurnal Penelitian Transportasi Darat*, vol. 21, no. 1, pp. 59–66, Feb. 2020.

[4] J. J. Wang, Y. L. Han, and J. Y. Chen, "A generalized location privacy protection scheme in location based services," in *Communications in Computer and Information Science*, Springer Verlag, 2016.

[5] S. Steiniger, M. Neun, A. Edwardes, and B. Lenz, "Foundations of LBS Responsible persons." [Online]. Available: http://www.e-cartouche.ch

[6] "Providing emergency services using location based tracking on mobile devices 1Ankita Deshpande 2.DevashishLokhande 3Shrutika Vithalkar," 2014.

[7] S Zhang, X Li, Z Tan, T Peng, and G Wang, "*A chacing and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services*", 2019.

[8] "RANCANG BANGUN PANIC BUTTON SYSTEM TERINTEGRASI MENGGUNAKAN LBS PADA KEPOLISIAN RESOR KOTA PEKANBARU", 2020.

[9] N. Alvira Julita and M. Hasnawi, "Buletin Sistem Informasi dan Teknologi Islam Rancang Bangun Sistem Pelaporan Kriminal Menggunakan Metode Location Based Services (LBS) INFORMASI ARTIKEL ABSTRAK," vol. 1, no. 3, pp. 182–186, 2020.

[10] B. Yulianto, "Teknologi Location Based Service (Global Positioning System) Pada Perangkat Mobile," *ComTech: Computer, Mathematics and Engineering Applications*, vol. 1, no. 1, p. 61, Jun. 2010.

[11] Institute of Electrical and Electronics Engineers, *2013 IEEE Wireless Communications and Networking Conference (WCNC) : ... took place April 7-10, 2013 in Shanghai, P.R. China.*

[12] "A Comparative Study on privacy preserving techniqwues for kb", 2018.

[13] R. Mallik, A. P. Hazarika, S. Ghosh Dastidar, D. Sing, and R. Bandyopadhyay, "Development of An Android Application for Viewing Covid-19 Containment Zones and Monitoring Violators Who are Trespassing into It Using Firebase and Geofencing," *Transactions of the Indian National Academy of Engineering*, vol. 5, no. 2, pp. 163–179, Jun. 2020.

[14] International Conference on Electrical Engineering and Computer Science 2017 Palembang, Institute of Electrical and Electronics Engineers Indonesia Section, International Conference on Electrical Engineering and Computer Science 2017.08.22-23 Palembang, ICECOS Conference 2017.08.22-23 Palembang, and ICECOS 2017.08.22-23 Palembang, *Sustaining the cultural heritage toward the smart environment for better future ICECOS 2017 Conference : proceedings : August 22-23, 2017, Horison Ultima Hotel, Palembang*.

[15] S. R. Garzon and B. Deva, "Geofencing 2.0: Taking location-based notifications to the next level," in *UbiComp 2014 - Proceedings of the*

2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Association for Computing Machinery, Inc, 2014, pp. 921–932. doi: 10.1145/2632048.2636093.

[16] D. D. Prihantoro and M. I. Wahyuddin, "Implementasi Algoritma Haversine Formula dan Location Based Service Pada Aplikasi Pencarian Lokasi Bird Contest Berbasis Android," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 1, p. 663, Jan. 2022, doi: 10.30865/mib.v6i1.3546.

[17] G. H. Prakarsha, H. D. K. Lumbantobing, R. R. M, and I. Prihandi, "Haversine Algorithm Design using the Google Maps API Method for Android-based Public Security Applications," *International Journal of Computer Trends and Technology*, vol. 69, no. 2, pp. 53–60, Feb. 2021, doi: 10.14445/22312803/ijctt-v69i2p108.

[18] N. Krishnan, M. Karthikeyan, Institute of Electrical and Electronics Engineers. Madras Section. Podhigai Subsection, Institute of Electrical and Electronics Engineers. Madras Section. Signal Processing/Computational Intelligence/Computer Joint Societies Chapter, and Institute of Electrical and Electronics Engineers, *2016 IEEE International Conference on Computational Intelligence and Computing Research : 2016 December 15-17*.

[19] M. Telekomunikasi and D. Informasi, "AUDIT TEKNOLOGI INFORMASI PADA PT XYZ MENGGUNAKAN FRAMEWORK COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)," *Jurnal Sistem Informasi dan Telematika*, vol. 10, no. 1, 2019.