**Indonesian Journal of Computer Science**
ISSN 2302-4364 (*print*) dan 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam, No. 1, Padang, Indonesia, Telp. (0751) 7056199, 7058325
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

# Desain Sistem Keamanan terhadap Spoofing GPS pada Aplikasi Android: Integrasi Program Perlindungan dalam Source Code

**Zaim Irfansyah Arbi[1], Banu Santoso[2]**
zaimirfansyah@students.amikom.ac.id, banu@amikom.ac.id
Universitas Amikom Yogyakarta

**Informasi Artikel**

Diterima : 27 Des 2023
Direview : 14 Jan 2024
Disetujui : 10 Feb 2024

**Kata Kunci**

Spoofing GPS, Keamanan Aplikasi Android, Integrasi Kode, Program Perlindungan.

**Abstrak**

Perkembangan aplikasi Android berbasis lokasi menghadapi ancaman serius dari serangan spoofing GPS yang semakin canggih. Penelitian ini mengusulkan sebuah sistem keamanan yang responsif dengan mengintegrasikan perlindungan langsung ke dalam source code aplikasi Android. Fokusnya adalah memblokir akses opsi pengembang, yang sering dimanfaatkan oleh aplikasi spoofing GPS di Play Store. Metode ini diharapkan dapat meningkatkan keamanan aplikasi Android berbasis lokasi. Tujuan utama adalah mencegah serangan spoofing dengan melindungi integritas data lokasi. Hasil penelitian menunjukkan efektivitas sistem dalam mengatasi celah keamanan yang spesifik ini, memberikan kontribusi penting dalam menjaga keamanan aplikasi Android di era serangan spoofing GPS yang semakin mengancam.

***Keywords***

*GPS Spoofing, Android Application Security, Code Integration, Protection Program.*

**Abstrak**

*The development of location-based Android applications faces serious threats from increasingly sophisticated GPS spoofing attacks. This research proposes a responsive security system by integrating protection directly into the Android application source code. The focus is on blocking access to developer options, which is often exploited by GPS spoofing apps in the Play Store. This method is expected to improve the security of location-based Android applications. The main goal is to prevent spoofing attacks by protecting the integrity of location data. The research results demonstrate the system's effectiveness in addressing this specific security gap, making an important contribution to maintaining the security of Android applications in an era of increasingly threatening GPS spoofing attacks.*

Attribution-ShareAlike 4.0 International License

## A. Pendahuluan

Perkembangan pesat aplikasi Android berbasis lokasi membawa tantangan signifikan dalam hal keamanan, khususnya terkait dengan ancaman spoofing GPS yang semakin canggih[1]. Spoofing GPS, yaitu manipulasi sinyal lokasi, dapat merugikan integritas aplikasi yang sangat bergantung pada data lokasi[2]. Fenomena ini semakin meningkat dan memerlukan solusi keamanan yang adaptif[3].

Latar belakang masalah ini berakar pada peningkatan serangan spoofing GPS yang dapat mengancam keberlangsungan operasional aplikasi Android. Kami sebagai peneliti melihat bahwa banyak aplikasi spoofing GPS yang tersedia di Play Store[4]. Aplikasi tersebut memerlukan akses opsi pengembang (developer options) pada perangkat Android[5]. Pemanfaatan metode ini oleh pelaku serangan membuat keamanan aplikasi Android semakin rentan[6].

Penelitian ini bertujuan untuk merancang sistem keamanan yang responsif terhadap spoofing GPS dengan mengintegrasikan program perlindungan langsung ke dalam source code aplikasi Android. Pilihan metode ini didasarkan pada kebutuhan untuk secara spesifik mengatasi celah keamanan yang terkait dengan aplikasi spoofing GPS yang menggunakan opsi pengembang[7]. Dengan memblokir akses opsi pengembang, diharapkan dapat mencegah aplikasi spoofing untuk melakukan tindakan spoofing dengan lebih efektif.

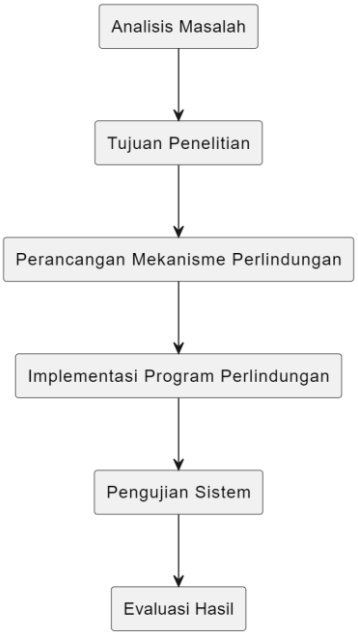
Landasan teori penelitian ini melibatkan tinjauan literatur mengenai teknologi lokasi Android, serangan spoofing GPS, dan penggunaan opsi pengembang dalam konteks keamanan aplikasi. Penelitian sebelumnya memberikan pemahaman yang kuat tentang metode perlindungan yang dapat diimplementasikan dalam source code aplikasi Android, khususnya terkait dengan opsi pengembang.

Dengan menggabungkan latar belakang masalah, landasan teori, dan pilihan metode perlindungan, penelitian ini bertujuan untuk memberikan solusi keamanan yang dapat menanggulangi celah keamanan yang spesifik[8]. Tujuan utama adalah mengembangkan sistem keamanan yang tidak hanya dapat mencegah akses opsi pengembang yang dimanfaatkan oleh aplikasi spoofing GPS, tetapi juga melindungi integritas data lokasi dalam konteks aplikasi Android berbasis lokasi.

Hasil penelitian ini diharapkan dapat memberikan kontribusi konseptual dan praktis dalam meningkatkan keamanan aplikasi Android berbasis lokasi[9]. Selain itu, penelitian ini diharapkan dapat memberikan wawasan lebih mendalam tentang metode perlindungan yang efektif dalam melawan serangan spoofing GPS yang memanfaatkan opsi pengembang. Dengan demikian, penelitian ini tidak hanya mengidentifikasi masalah keamanan, tetapi juga menawarkan solusi proaktif untuk melindungi integritas data lokasi dalam konteks aplikasi Android.

## B. Metode Penelitian

Peneliti akan membahas langkah-langkah yang diambil menggunakan suatu kerangka kerja terstruktur. Kerangka kerja ini diciptakan untuk membimbing dalam menyelesaikan masalah penelitian. Berbagai tahapan dari merumuskan masalah hingga menganalisis hasil. Setiap langkah penelitian dapat diuraikan sebagai berikut:




**Gambar 1**.Kerangka Kerja

Dengan merujuk pada struktur kerangka kerja yang tergambar di atas, setiap langkahnya dapat dijelaskan sebagai berikut:

1. Analisis Masalah, proses analisis dimulai dengan mengidentifikasi dan merinci masalah keamanan terkait serangan spoofing GPS pada aplikasi Android berbasis lokasi. Fokus utama analisis adalah pada kerentanan aplikasi yang mungkin dimanfaatkan oleh serangan dan implikasinya terhadap integritas data lokasi.
2. Tujuan penelitian, merancang dan mengimplementasikan sistem keamanan terhadap serangan spoofing GPS. Dalam konteks mitigasi spoofing, penelitian ini berfokus pada upaya penanggulangan terhadap serangan spoofing[10]. Strategi perlindungan terhadap akses opsi pengembang menjadi pendekatan pada penelitian ini.
3. Perancangan Mekanisme Perlindungan, melibatkan perancangan alur kerja program dan spesifikasi teknis terinci untuk integrasi program perlindungan ke dalam source code aplikasi Android. Proses ini menitikberatkan pada mekanisme pemblokiran akses opsi pengembang
4. Implementasi Program Perlindungan, mencakup penyisipan dan pengkodean program perlindungan ke dalam source code aplikasi Android sesuai dengan perancangan yang telah dibuat. Langkah ini memastikan efektivitas dan keterpaduan program perlindungan dalam konteks aplikasi yang bersangkutan.
5. Pengujian Sistem, mencakup uji fungsional dari sistem perlindungan dengan tujuan untuk memvalidasi sejauh mana efektivitas sistem perlindungan terhadap serangan spoofing GPS. Proses ini dirancang dengan tujuan memastikan bahwa sistem perlindungan beroperasi sesuai dengan harapan yang telah ditetapkan.

6. Evaluasi Hasil, mencakup analisis data dari pengujian sistem untuk menilai sejauh mana tujuan penelitian tercapai. Kesimpulan dari hasil evaluasi memberikan wawasan mengenai efektivitas sistem keamanan dan potensi pengembangan lanjutan.

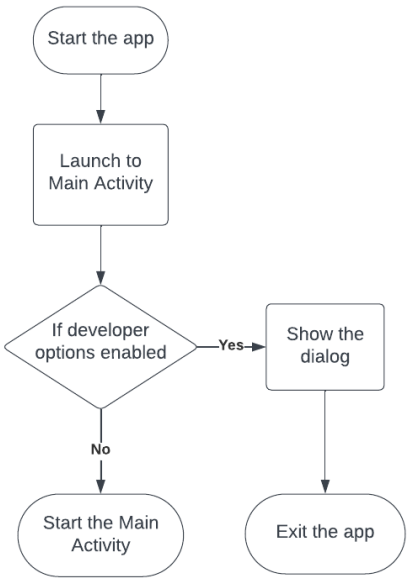
## C. Hasil dan Pembahasan

Dalam menghadapi ancaman serius dari serangan spoofing GPS terhadap perkembangan aplikasi Android berbasis lokasi, penelitian ini mengusulkan sebuah sistem keamanan responsif dengan mengintegrasikan perlindungan langsung ke dalam source code aplikasi Android. Fokus utama penelitian adalah memblokir akses opsi pengembang yang kerap dimanfaatkan oleh aplikasi spoofing GPS di Play Store. Metode ini dirancang untuk meningkatkan keamanan aplikasi Android berbasis lokasi, dengan tujuan utama mencegah serangan spoofing dan melindungi integritas data lokasi.

### 1. Perancangan

Dalam perancangan ini, peneliti memaparkan langkah-langkah yang diambil untuk menciptakan sistem keamanan. Perancangan program ini mencakup dua aspek, yakni flowchart dari program dan user interface diagram. Flowchart digunakan untuk menyajikan visualisasi struktur logika program, sementara user interface diagram memberikan gambaran interaksi dan aktivitas pengguna.

a. Flowchart Program

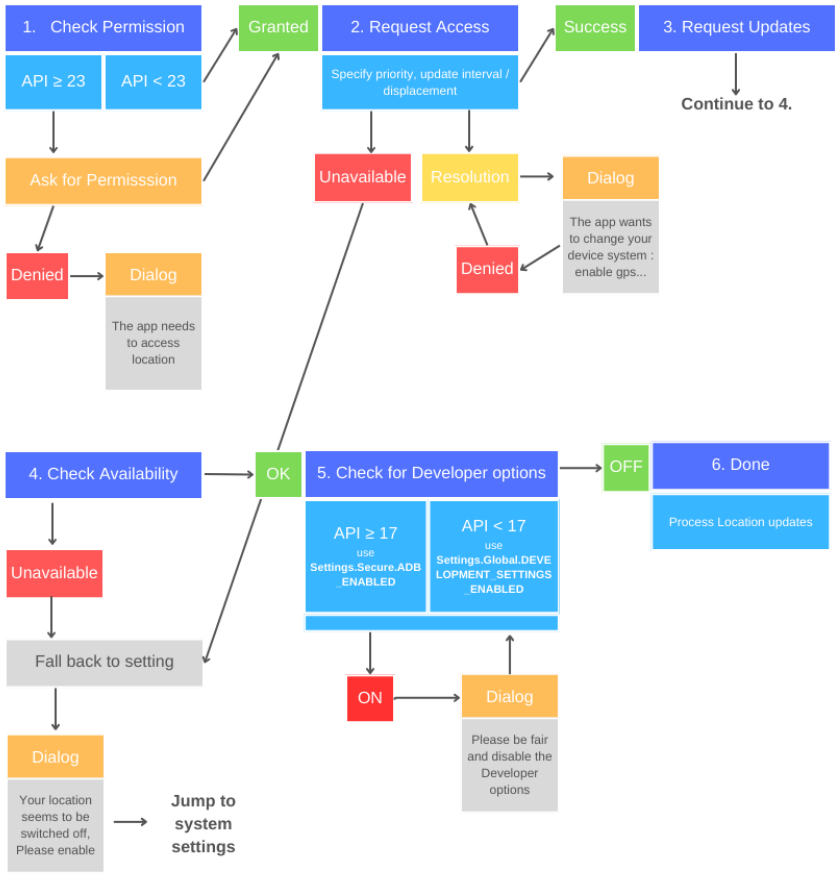



**Gambar 2**. Flowchart Program

Aplikasi ini dimulai ketika pengguna membukanya kemudian membawa mereka ke main activity yang merupakan layar utama atau antarmuka pengguna. Namun, sebelum melanjutkan, aplikasi melakukan

pemeriksaan penting untuk mengetahui apakah opsi pengembang diaktifkan pada perangkat pengguna. Jika ternyata opsi pengembang telah diaktifkan, aplikasi merespons dengan segera dengan menampilkan dialog alert atau pemberitahuan kepada pengguna. Dialog ini dirancang khusus untuk memberikan peringatan kepada pengguna, memberitahu pengguna bahwa aplikasi memerlukan opsi pengembang dinonaktifkan, jika tidak maka aplikasi tidak dapat dijalankan.

b. User Interface Diagram




**Gambar 3**. User Interface Diagram

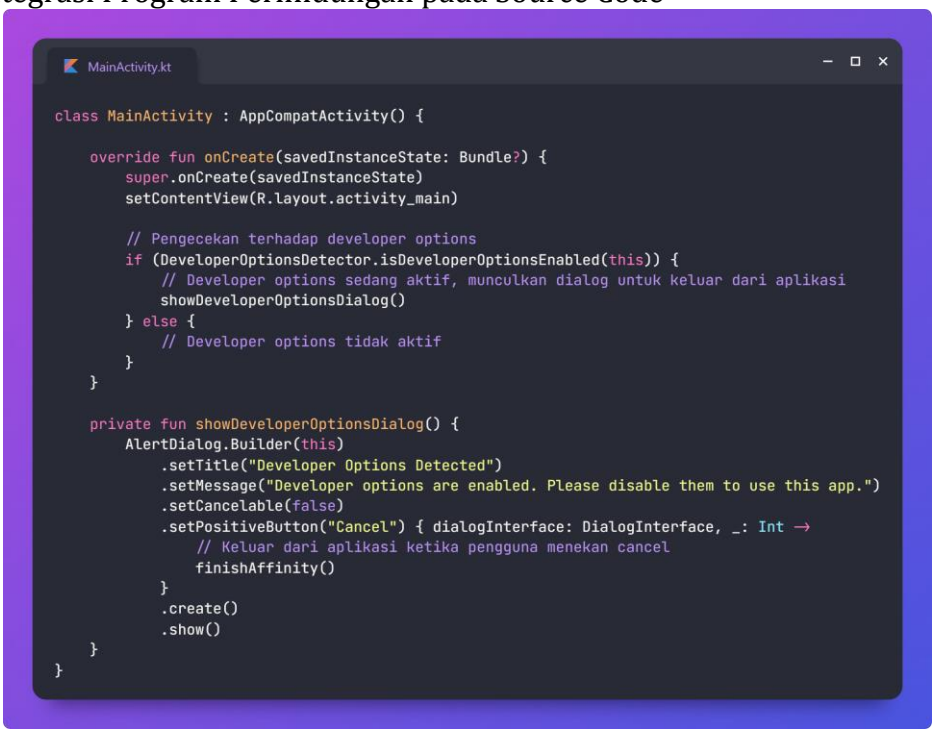
Dalam User Interface Diagram (UID) ini, dapat terlihat secara detail bagaimana interaksi antara pengguna dan aplikasi terjadi. Saat pengguna membuka aplikasi, mereka akan diminta untuk memberikan izin guna mengaktifkan lokasi pada perangkat mereka. Setelah izin diberikan, langkah selanjutnya adalah aplikasi melakukan pengecekan untuk memastikan apakah pengguna sudah memberikan izin akses data lokasi. Apabila izin sudah diotorisasi, aplikasi kemudian memulai program perlindungan yang melibatkan pengecekan terhadap status opsi pengembang. Jika opsi pengembang terdeteksi aktif, aplikasi akan memberikan output melalui sebuah dialog alert kepada pengguna.

Melalui UID ini, pemahaman terhadap setiap langkah dalam interaksi antara pengguna dan aplikasi menjadi lebih mudah.

## 2. Implementasi

Penelitian melangkah ke tahap pengaplikasian konsep keamanan yang akan dirancang ke dalam source code aplikasi. Langkah-langkah praktis dilakukan untuk mengintegrasikan program perlindungan ke dalam source code berdasarkan perancangan sistem atau alur kerja program yang telah disusun sebelumnya.

a. Integrasi Program Perlindungan pada Source Code



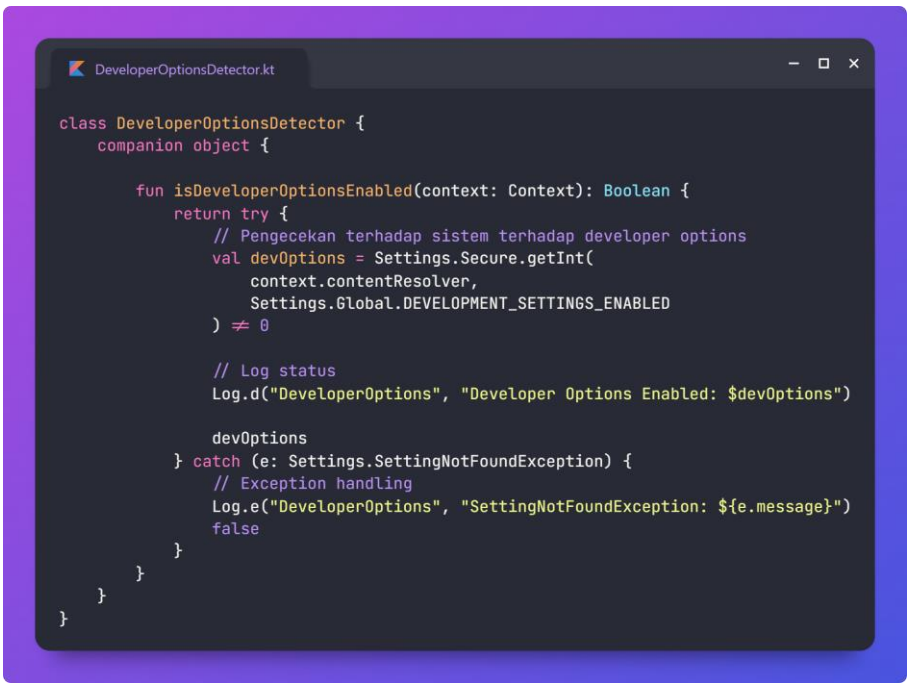

**Gambar 4**. Source Code di dalam Main Activity

Dalam gambar 4, terlihat source code pada main activity yang telah diintegrasikan dengan program perlindungan untuk mendeteksi status opsi pengembang. Source code ini merupakan inti dari implementasi keamanan yang telah dirancang sebelumnya. Gambar tersebut memberikan pandangan langsung tentang bagaimana program perlindungan diaplikasikan ke dalam source code aplikasi. Pada tahap ini, dapat ditemukan sejumlah perubahan atau tambahan pada struktur kode guna mendukung deteksi dan respons terhadap status opsi pengembang.

b. Implementasi Logic Programming

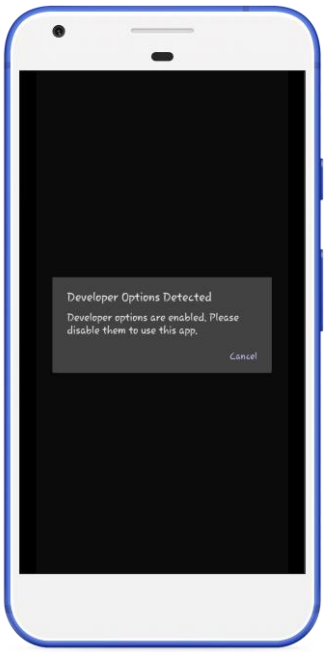
Pada Gambar 5, peneliti melakukan pengaplikasian logika pemrograman yang telah disusun berdasarkan flowchart atau alur kerja program guna mencapai tujuan penelitian. Logika ini disusun dan dituliskan dalam file class terpisah yang nantinya akan dipanggil oleh

main activity saat pengguna membuka atau menjalankan aplikasi. Dengan cara ini, terdapat pemisahan antara logika program yang telah dirancang dengan tugas utama main activity, memungkinkan untuk pengelolaan dan pemeliharaan kode yang lebih efisien dan membantu menciptakan struktur program yang terorganisir dan mudah dipahami.




**Gambar 5.** Logic Programming

### 3. Pengujian




**Gambar 6.** Hasil Pengujian

Hasil pengujian menunjukkan bahwa sistem perlindungan berhasil mendeteksi opsi pengembang, membantu mengurangi risiko serangan spoofing GPS. Sistem ini berhasil mengidentifikasi opsi pengembang yang aktif. Dengan deteksi ini, risiko spoofing GPS dapat dicegah serta meningkatkan keamanan aplikasi Android berbasis lokasi.

**Tabel 1.** Hasil Pengujian pada perangkat Android

| No | Versi Android | *API Level* | *Hasil* |
|---|---|---|---|
| 1 | Android 13 | 33 | Berhasil |
| 2 | Android 12 | 32, 31 | Berhasil |
| 3 | Android 11 | 30 | Berhasil |
| 5 | Android 10 | 29 | Berhasil |
| 6 | Android 9 | 28 | Berhasil |

Dengan merujuk pada tabel di atas, hasil pengujian menunjukkan kinerja yang memuaskan dari sistem perlindungan pada berbagai versi Android. Sistem ini berhasil beroperasi dengan baik dan konsisten pada variasi versi Android yang berbeda. Penelitian ini menunjukkan bahwa sistem perlindungan mampu efektif menjaga keamanan aplikasi di berbagai jenis perangkat Android.

## D. Simpulan

Penelitian ini berhasil mengembangkan sistem keamanan untuk melawan serangan spoofing GPS pada aplikasi Android berbasis lokasi. Dengan mengintegrasikan perlindungan langsung ke dalam source code, khususnya dengan memblokir akses opsi pengembang, aplikasi dapat lebih efektif menghadapi ancaman serangan. Eksperimen menunjukkan keberhasilan sistem dalam mencegah serangan dan menjaga integritas data lokasi. Penerapan metode perlindungan ini memberikan solusi proaktif, memperkuat keamanan aplikasi, dan memberikan kontribusi signifikan dalam melindungi integritas data lokasi pada platform Android. Kesimpulan ini diharapkan dapat menjadi landasan untuk pengembangan sistem keamanan lebih lanjut dan memberikan panduan praktis bagi pengembang aplikasi Android.

## E. Ucapan Terima Kasih

Peneliti ingin menyampaikan rasa terima kasih kepada Universitas Amikom Yogyakarta atas dukungan yang luar biasa selama pelaksanaan penelitian ini. Keterlibatan universitas dalam memberikan izin dan saran selama proses penelitian sangatlah berharga.

## F. Referensi

[1] D. Spoljar, K. Lenac, D. Zigman, and M. Marovic, "A Mobile Network-Based GNSS Anti-Spoofing," in *2018 26th Telecommunications Forum (TELFOR)*, IEEE, Nov. 2018, pp. 1–3. doi: 10.1109/TELFOR.2018.8612130.

[2] R. Hartono, "PENINGKATAN PERFORMA PENDETEKSIAN GPS FAKE DRIVER GO-JEK MENGGUNAKAN METODE ENSEMBLE LEARNING," *J. Ilmu Komput.*, vol. 6, Jan. 2023, Accessed: Dec. 20, 2023. [Online]. Available: https://jurnal.pranataindonesia.ac.id/index.php/jik/article/view/152

[3] Nelson Michael and Paolina Centonze, "GPS Spoofing for Android and iOS Mobile Systems," *ICIMP 2019 Fourteenth Int. Conf. Internet Monit. Prot.*, 2019.

[4] A. Arshad, H. Abbas, W. Bin Shahid, and A. Azhar, "Deceiving Eavesdroppers by Real Time Persistent Spoofing of Android Users' Location Coordinates for Privacy Enhancement," in *2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, IEEE, Sep. 2020, pp. 107–112. doi: 10.1109/WETICE49692.2020.00029.

[5] N. Spens, D.-K. Lee, , Filip Nedelkov, and D. Akos, "Detecting GNSS Jamming and Spoofing on Android Devices," *Navig. J. Inst. Navig.*, vol. 69, no. 3, p. navi.537, Sep. 2022, doi: 10.33012/navi.537.

[6] S. Azam, R. Singh Sumra, B. Shanmugam, K. Cher Yeo, M. Jonokman, and G. Narayana Samy, "Security Source Code Analysis of Applications in Android OS," *Int. J. Eng. Technol.*, vol. 7, no. 4.15, p. 30, Oct. 2018, doi: 10.14419/ijet.v7i4.15.21366.

[7] Y. Chang, C.-L. Hu, and Y. L. Hwang, "Fake GPS Defender: A Server-side Solution to Detect Fake GPS," in *ACCSE 2018 : The Third International Conference on Advances in Computation, Communications and Services*, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:251767867

[8] P. Bethi, S. Pathipati, and A. P, "Stealthy GPS Spoofing: Spoofer Systems, Spoofing Techniques and Strategies," in *2020 IEEE 17th India Council International Conference (INDICON)*, IEEE, Dec. 2020, pp. 1–7. doi: 10.1109/INDICON49873.2020.9342317.

[9] A. Rustamov, N. Gogoi, A. Minetto, and F. Dovis, "Assessment of the Vulnerability to Spoofing Attacks of GNSS Receivers Integrated in Consumer Devices," in *2020 International Conference on Localization and GNSS (ICL-GNSS)*, IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ICL-GNSS49876.2020.9115489.

[10] M. Ahmad and M. Akhtar, "Impact and Detection of GPS Spoofing and Countermeasures against Spoofing," in *2019 International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019* , Dec. 2019.