STORAGE – Jurnal Ilmiah Teknik dan Ilmu Komputer, Vol. 4 No. 1, Februari 2025, 22 - 28
e-ISSN: 2828-5344 | DOI: 10.55123

TINJAUAN LITERATUR: PERBANDINGAN SISTEM KEAMANAN PADA APLIKASI ANDROID DAN IOS

[1)]Fadhlurohman Fatikh Navintino, [2)]Muhammad Farhan Fahreza, [3)]Elkin Rilvani

[1,2,3)] Fakultas Teknik, Teknik Informatika, Universitas Pelita Bangsa
[1)] fadhlurohmanfn@gmail.com, [2)] farhanmhmmd064@gmail.com, [3)] elkin.rilvani@pelitabangsa.ac.id

INFO ARTIKEL

Riwayat Artikel :
Diterima : 14 Januari 2025
Disetujui : 25 Januari 2025

Kata Kunci :
Android, iOS, keamanan aplikasi, sistem operasi mobile, tinjauan literatur.

ABSTRAK

Keamanan aplikasi pada sistem operasi mobile adalah topik yang penting di era digital. Penelitian ini membandingkan sistem keamanan pada Android dan iOS melalui tinjauan literatur. Android, dengan sifat open-source, menawarkan fleksibilitas bagi pengembang, namun lebih rentan terhadap malware. Sebaliknya, iOS mengadopsi ekosistem tertutup yang memberikan kontrol lebih besar terhadap aplikasi, tetapi membatasi inovasi. Penelitian ini menemukan bahwa meskipun Android lebih populer karena fleksibilitasnya, iOS memiliki keamanan yang lebih tinggi karena kontrol ketatnya. Dengan memahami perbedaan ini, pengguna dan pengembang dapat membuat keputusan yang lebih bijak dalam memilih platform.

ARTICLE INFO

Article History :
Received : Jan 14, 2025
Accepted : Jan 25, 2025

Keywords*:*
Android, iOS, application security, mobile operating systems, literature review.

ABSTRACT

The security of mobile operating systems is a critical topic in the digital era. This study compares the security systems of Android and iOS through a literature review. Android, with its open-source nature, offers flexibility for developers but is more vulnerable to malware. Conversely, iOS adopts a closed ecosystem providing greater control over applications but limits innovation. This research finds that while Android is more popular due to its flexibility, iOS provides higher security due to its stringent control. Understanding these differences enables users and developers to make more informed platform choices.

1. PENDAHULUAN

Kemajuan teknologi dalam dua dekade terakhir telah membawa perubahan besar dalam cara manusia berinteraksi, bekerja, dan berkomunikasi. Perkembangan perangkat mobile, terutama smartphone, menjadi salah satu pendorong utama perubahan tersebut. Smartphone adalah ponsel yang dibuat berdasarkan sistem operasi dengan kemampuan komputasi dan konektivitas yang lebih maju daripada telepon (Arnomo and Hendra, 2019). Dalam perangkat bergerak sendiri terdapat sistem operasi khusus yang dinamakan sistem operasi perangkat bergerak (mobile operating system). Sistem operasi pada handphone sangat beragam dalam hal penyediasan fungsi dan fitur. Sistem operasi yang canggih bahkan memungkinkan handphone untuk memiliki dan menjalankan aplikasi cerdas (Hilman, 2018). Sistem operasi perangkat bergerak digunakan untuk menghubungkan antara aplikasi yang dipakai oleh pengguna dengan perangkat keras yang terdapat di perangkat bergerak tersebut untuk melakukan fungsi tertentu (Ridwan et al., n.d.). Sistem operasi smartphone telah meningkat ke posisi yang sangat penting. Sekarang, ada dua sistem operasi yang mendominasi pasar: iOS dan Android (Nurul Syaza Abdul Latif et al., 2023). Android, sebagai sistem operasi berbasis Linux yang dirancang untuk perangkat bergerak layar sentuh seperti telepon pintar dan komputer tablet, kini memiliki pengguna yang sangat banyak di seluruh dunia (Kartono et al., 2019). Berdasarkan data rentang waktu 2018–2020, tercatat sebanyak 74.95% pengguna perangkat mobile menggunakan Android sebagai sistem operasi utama mereka (Alviansyah and Ramadhani, 2021).

Di sisi lain, iOS adalah sistem operasi seluler yang kuat, dikembangkan oleh Apple Inc. dan pertama kali diluncurkan pada tahun 2007. Hingga saat ini, iOS tetap menjadi sistem operasi terpopuler kedua di dunia (Sikder et al., 2020). Dengan pendekatan ekosistem yang lebih tertutup, iOS menawarkan tingkat kontrol yang lebih tinggi terhadap aplikasi yang diizinkan masuk ke App Store.

Kenyamanan pengguna adalah aspek kunci dalam meningkatkan adopsi dan kepuasan sistem operasi seluler, termasuk iOS dan Android (Pandusaputri et al., 2024). Keamanan aplikasi mobile tidak hanya penting bagi pengembang, tetapi juga bagi pengguna akhir yang mempercayakan data pribadi mereka kepada aplikasi-aplikasi tersebut. Android, sebagai platform yang lebih terbuka dan fleksibel, sering dianggap lebih rentan terhadap serangan. Sebaliknya, iOS, dengan pendekatan ekosistem yang lebih tertutup, menawarkan tingkat kontrol yang lebih tinggi terhadap aplikasi yang diizinkan masuk ke App Store. Namun, kedua platform ini tidak sepenuhnya bebas dari kerentanan keamanan. Aplikasi Android terus berkembang dari waktu ke waktu. Penambahan fitur pada suatu aplikasi sejalan dengan temuan kelemahan baru pada aplikasi tersebut (Yasa and Nugraha, 2024).

Penelitian ini bertujuan untuk membandingkan sistem keamanan pada aplikasi Android dan iOS melalui tinjauan literatur. Dengan memahami perbedaan mendasar dalam pendekatan keamanan kedua platform, diharapkan dapat memberikan wawasan bagi pengembang aplikasi dan pengguna untuk membuat keputusan yang lebih baik terkait keamanan data.

Ruang lingkup penelitian ini terbatas pada tinjauan literatur yang relevan dengan sistem keamanan aplikasi Android dan iOS. Penelitian ini tidak mencakup analisis teknis mendalam, melainkan fokus pada identifikasi keunggulan, kelemahan, serta kerentanan yang telah didokumentasikan dalam studi-studi sebelumnya.

Dengan demikian, penelitian ini diharapkan dapat menjadi referensi yang bermanfaat bagi para peneliti, pengembang, dan pengguna dalam memahami dan meningkatkan aspek keamanan aplikasi pada kedua platform mobile yang dominan ini.

2. METODE

Penelitian ini menggunakan pendekatan studi literatur untuk mengkaji dan membandingkan sistem keamanan pada aplikasi Android dan iOS. Pendekatan ini dipilih karena memungkinkan peneliti untuk mengakses dan menganalisis berbagai sumber informasi yang relevan secara efisien.

2.1. Pengumpulan Data

Data yang digunakan dalam penelitian ini diperoleh dari berbagai sumber yang relevan,

antara lain: (1) Artikel jurnal ilmiah yang membahas topik terkait sistem keamanan. (2) Publikasi yang diterbitkan dalam konferensi akademik yang fokus pada topik keamanan aplikasi. (3) Dokumentasi resmi dari Google dan Apple yang menyajikan informasi terkait fitur keamanan pada platform Android dan iOS.

2.2. Analisis Data

Data yang terkumpul dianalisis menggunakan pendekatan deskriptif dan komparatif. Pendekatan deskriptif digunakan untuk memaparkan fitur keamanan yang ada pada masing-masing platform, sementara pendekatan komparatif digunakan untuk mengidentifikasi perbedaan, keunggulan, dan kelemahan dalam sistem keamanan antara Android dan iOS.

2.3. Validitas dan Reliabilitas

Untuk memastikan validitas dan reliabilitas hasil penelitian, sumber literatur yang digunakan dievaluasi berdasarkan kredibilitas penerbit dan relevansinya dengan topik yang dikaji. Selain itu, analisis dilakukan secara sistematis untuk menghindari adanya bias dalam interpretasi data yang dapat mempengaruhi kesimpulan penelitian.

3. KAJIAN PUSTAKA

Model keamanan iOS lebih ketat dibandingkan dengan Android. iOS adalah sistem tertutup, di mana pengembang dapat mengembangkan aplikasi mereka sendiri tetapi kode sumbernya tidak dirilis, seperti halnya Android (Garg and Baliyan, 2021). Sifat sumber tertutup dari sistem operasi iOS, termasuk penggunaan bahasa pemrograman dan kompiler khusus Apple, membuat upaya analisis menjadi lebih kompleks (Kollnig et al., 2022). Dengan pendekatan ini, Apple dapat memastikan tingkat kontrol yang tinggi terhadap aplikasi yang diizinkan masuk ke ekosistemnya, sehingga mengurangi risiko malware dan aplikasi berbahaya.

Ketika seseorang membobol sistem seluler, orang tersebut mengambil keuntungan dari berbagai faktor seperti teknologi, penyimpangan dalam prosedur atau manajemen (atau kombinasi dari semuanya), memungkinkan akses atau tindakan yang tidak sah. Kegagalan spesifik dari kontrol ini disebut kerentanan atau cacat keamanan (Adascalitei, 2019).

Pada dasarnya, sistem operasi seluler (OS) dapat menjadi rentan dan mengalami serangan berbahaya karena menjalankan banyak aplikasi (aplikasi) selama menjelajahi web atau mengunduh aplikasi dari Internet (Taleby et al., 2017).

Android adalah sistem operasi yang berfokus pada pengguna akhir. Meskipun Android mengupayakan fleksibilitas, fokus utamanya adalah pada pengguna pada umumnya. Implikasi yang jelas adalah bahwa, sebagai OS konsumen, OS ini harus berguna bagi pengguna dan menarik bagi pengembang (Mayrhofer et al., 2021).

Beberapa penelitian sebelumnya telah mengidentifikasi bahwa fleksibilitas Android, meskipun memberikan banyak keuntungan bagi pengembang, juga membuka peluang lebih besar bagi malware untuk menyusup. Di sisi lain, kontrol ketat Apple terhadap aplikasi di ekosistem iOS memberikan keamanan yang lebih tinggi, meskipun membatasi kebebasan pengembang.

Literatur terkait menunjukkan bahwa kerentanan utama pada sistem operasi mobile disebabkan oleh kombinasi faktor teknis dan prosedural. Oleh karena itu, pendekatan keamanan yang holistik diperlukan untuk mengurangi risiko serangan yang merugikan pengguna dan pengembang.

4. HASIL DAN PEMBAHASAN

4.1. Hasil

Berdasarkan tinjauan literatur yang telah dilakukan, diperoleh beberapa temuan utama terkait sistem keamanan pada aplikasi Android dan iOS.

Pendekatan Keamanan Android: (1) Android mengadopsi model keamanan berbasis "open-source," yang memungkinkan pengembang untuk memodifikasi sistem operasi. (2) Pengguna Android memiliki wewenang untuk menerima atau menolak izin aplikasi yang diinstal (Sarkar et al., 2019), namun seringkali pengguna kurang memahami risiko yang terkait. (3) Google Play Protect telah diimplementasikan untuk memindai aplikasi dari ancaman malware, meskipun tidak sepenuhnya mencegah serangan berbahaya.

Pendekatan Keamanan iOS: (1) Apple tidak memperbolehkan distribusi aplikasi iOS di luar

App Store (Alamsyah et al., 2024). (2) iOS menerapkan fitur sandboxing yang membatasi akses aplikasi ke data pengguna dan sistem lainnya. (3) Sistem otentikasi dua faktor (2FA) untuk akun Apple ID menambah lapisan keamanan bagi pengguna.

Kerentanan yang Terdokumentasi: (1) Android lebih sering menjadi target serangan malware karena pangsa pasarnya yang lebih besar dan ekosistemnya yang lebih terbuka. (2) Meskipun iOS memiliki kontrol yang lebih ketat, serangan terhadap iOS sering kali lebih terfokus pada eksploitasi zero-day yang kompleks.

4.2. Pembahasan

Hasil penelitian menunjukkan bahwa kedua platform memiliki pendekatan keamanan yang berbeda, dengan kelebihan dan kekurangan masing-masing:

Aspek	Kelebihan Android	Kelemahan Android
Sistem Operasi	Sistem open-source memberikan fleksibilitas tinggi bagi pengembang dan produsen perangkat.	Sistem terbuka meningkatkan risiko malware karena aplikasi dapat diunduh dari sumber tidak resmi.
Verifikasi Aplikasi	Dukungan komunitas open-source membantu mendeteksi dan memperbaiki bug dengan cepat.	Proses verifikasi aplikasi di Google Play Store kurang ketat dibandingkan iOS.
Fitur Keamanan Bawaan	Menyediakan berbagai fitur keamanan, seperti Google Play Protect dan enkripsi perangkat.	Tidak semua perangkat Android mendukung fitur keamanan terbaru karena fragmentasi.
Pembaruan Keamanan	Produsen dapat menyediakan pembaruan khusus untuk perangkat mereka.	Pembaruan keamanan sering kali tertunda atau tidak tersedia untuk semua perangkat.
Proteksi Data Pengguna	Mendukung autentikasi biometrik (fingerprint, face unlock) dan enkripsi data.	Proteksi data kurang konsisten karena tergantung pada implementasi produsen.
Risiko Malware	Beragam aplikasi keamanan pihak ketiga tersedia untuk melindungi perangkat.	Pengguna cenderung mengabaikan risiko keamanan, seperti mengaktifkan pemasangan dari sumber tidak dikenal.

Gambar 1. Kelebihan dan Kelemahan Sistem Keamanan Android.

Android memiliki beberapa kelebihan dalam hal sistem keamanan. Sebagai sistem operasi open-source, Android memberikan fleksibilitas tinggi bagi pengembang dan produsen perangkat untuk memodifikasi sistem operasi sesuai kebutuhan. Selain itu, dukungan dari komunitas open-source global memungkinkan deteksi dan perbaikan bug secara cepat melalui kolaborasi pengembang.
Android juga dilengkapi dengan fitur keamanan bawaan seperti Google Play Protect, enkripsi perangkat, dan autentikasi biometrik, yang dirancang untuk melindungi perangkat dari ancaman. Produsen perangkat Android juga memiliki kemampuan untuk menawarkan pembaruan keamanan khusus, yang dapat meningkatkan perlindungan perangkat. Keunggulan lain dari ekosistem Android adalah beragamnya pilihan aplikasi dan perangkat yang memungkinkan pengguna untuk menyesuaikan kebutuhan mereka dengan fleksibilitas harga.

Namun, Alasan eskalasi besar-besaran dalam malware Android adalah karena Android adalah sistem operasi sumber terbuka (Shrivastava and Kumar, 2019). Proses verifikasi aplikasi di Google Play Store dianggap kurang ketat dibandingkan dengan App Store, sehingga lebih banyak aplikasi berbahaya yang dapat lolos. Selain itu, fragmentasi sistem operasi Android menyebabkan pembaruan keamanan tidak tersedia untuk semua perangkat secara konsisten. Kesadaran pengguna terhadap keamanan juga menjadi tantangan, karena banyak yang mengabaikan risiko dengan mengaktifkan pengaturan "Unknown Sources" tanpa memahami konsekuensinya. Terakhir, implementasi fitur keamanan pada perangkat Android bervariasi di antara produsen, sehingga proteksi data pengguna tidak seragam di seluruh perangkat Android.

Aspek	Kelebihan iOS	Kelemahan iOS
Sistem Operasi	Sistem tertutup (closed system) memberikan kontrol penuh terhadap keamanan.	Sistem tertutup membatasi fleksibilitas pengguna untuk menyesuaikan pengaturan keamanan.
Verifikasi Aplikasi	Proses verifikasi aplikasi yang ketat menurunkan risiko malware dan aplikasi berbahaya.	Proses ketat dapat memperlambat atau menolak inovasi aplikasi tertentu.
Fitur Keamanan Bawaan	Sandboxing mencegah aplikasi saling memengaruhi, melindungi data pengguna.	Keterbatasan dalam penyesuaian fitur keamanan oleh pengguna.
Pembaruan Keamanan	Pembaruan keamanan rutin langsung dari Apple memastikan perangkat tetap aman.	Pengguna sepenuhnya bergantung pada Apple untuk pembaruan keamanan.
Proteksi Data Pengguna	Fitur seperti Face ID, Touch ID, dan enkripsi end-to-end melindungi privasi data.	Ketergantungan pada perangkat keras tertentu untuk fitur keamanan (misalnya, Face ID).
Risiko Malware	Risiko malware sangat rendah karena aplikasi hanya dapat diunduh melalui App Store resmi.	Tidak mendukung pemasangan aplikasi dari luar App Store, yang mungkin membatasi opsi pengguna.

Gambar 2. Kelebihan dan Kelebihan Sistem Keamanan iOS.

iOS dianggap sebagai salah satu OS yang paling aman untuk smartphone. Sistem operasi ini memiliki kontrol yang ketat terhadap berbagai komponennya: perangkat keras, OS, dan aplikasi (Wukkadada et al., 2015). Salah satu keunggulan utama iOS adalah penerapan sistem operasi tertutup (closed system). Dengan sistem ini, Apple memiliki kendali penuh atas perangkat keras, perangkat lunak, dan distribusi aplikasi. Pendekatan ini secara signifikan meningkatkan keamanan dengan membatasi celah yang dapat dimanfaatkan oleh serangan

eksternal. Selain itu, Apple menerapkan proses verifikasi aplikasi yang ketat untuk setiap aplikasi yang ingin masuk ke App Store. Proses ini memastikan risiko aplikasi berbahaya, seperti malware, tetap sangat rendah.

iOS juga dilengkapi dengan berbagai fitur keamanan bawaan seperti sandboxing, Face ID, dan Touch ID yang dirancang untuk melindungi data pengguna dari ancaman eksternal. Pembaruan keamanan rutin yang dirilis oleh Apple menjadi salah satu langkah strategis untuk menjaga keamanan perangkat dari ancaman terbaru. Selain itu, penggunaan teknologi seperti enkripsi end-to-end dan autentikasi biometrik semakin memperkuat proteksi terhadap privasi data pengguna.

Namun, meskipun memiliki keunggulan dalam aspek keamanan, iOS juga memiliki beberapa kelemahan. Salah satunya adalah keterbatasan fleksibilitas yang disebabkan oleh sistem tertutup. Aplikasi iOS hanya dapat diunduh dari iOS App Store. Tidak dimungkinkan untuk mengunduh dan menginstal aplikasi iOS selain dari App Store (Joshi and Sharma, 2019). Selain itu, sistem ini menciptakan ketergantungan penuh pada Apple untuk pembaruan keamanan, tanpa alternatif dari pihak ketiga.

Kebijakan verifikasi aplikasi yang ketat juga dapat menjadi penghambat inovasi, karena beberapa aplikasi mungkin ditolak jika tidak sesuai dengan kebijakan Apple. Proteksi hanya untuk perangkat baru juga menjadi kelemahan lain, di mana fitur keamanan tertentu seperti Face ID hanya tersedia pada perangkat keras terbaru, sehingga pengguna perangkat lama tidak dapat menikmati fitur tersebut. Terakhir, kurangnya dukungan untuk aplikasi khusus di luar ekosistem App Store dapat menjadi tantangan bagi pengguna yang membutuhkan aplikasi tertentu yang tidak tersedia di platform resmi.

Dengan pendekatan yang berfokus pada keamanan tinggi, iOS berhasil menciptakan ekosistem yang relatif aman. Namun, beberapa batasan yang melekat pada sistem ini menjadi pertimbangan penting bagi pengguna, terutama dalam hal fleksibilitas dan aksesibilitas.

5. PENUTUP

5.1. Kesimpulan

Penelitian ini telah mengkaji perbandingan sistem keamanan pada aplikasi Android dan iOS berdasarkan tinjauan literatur. Android, sebagai sistem operasi open-source, menawarkan fleksibilitas yang tinggi bagi pengembang, tetapi juga membuka lebih banyak peluang bagi kerentanan dan serangan keamanan. Sebaliknya, iOS dengan ekosistem tertutupnya memberikan kontrol yang lebih ketat terhadap aplikasi, sehingga menawarkan tingkat keamanan yang lebih tinggi. Pangsa pasar Android akan terus berkembang dan terbukti bahwa tidak akan ada persilangan antara Android dan iOS dalam waktu dekat. Peningkatan pangsa pasar dan sifat open-source Android disebabkan oleh meningkatnya kerentanan dibandingkan dengan sifat tertutup iOS (Garg and Baliyan, 2021).

Selain itu, Android dikenal karena keterjangkauannya dan fitur-fitur yang menarik, sehingga direkomendasikan oleh kalangan kelas menengah. Di sisi lain, iOS, dengan respons yang baik dan fitur yang mudah digunakan, lebih disukai oleh kalangan atas (Qiya et al., 2020). Dengan memahami kelebihan dan kekurangan masing-masing sistem operasi, pengguna dapat memilih platform yang sesuai dengan kebutuhan mereka.

5.2. Saran

Seiring dengan berkembangnya teknologi mobile, keamanan aplikasi menjadi salah satu prioritas utama yang harus diperhatikan oleh pengembang dan pengguna. Pengembang Android perlu meningkatkan langkah-langkah keamanan untuk mengurangi risiko yang timbul akibat sifat open-source platform ini. Sebagai platform yang lebih terbuka, Android memiliki potensi untuk dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Oleh karena itu, pengembang perlu memperkuat proses verifikasi aplikasi dan memastikan pembaruan keamanan yang lebih cepat serta konsisten.

Bagi pengguna Android, disarankan untuk lebih berhati-hati dalam mengunduh aplikasi, terutama dari sumber yang tidak terpercaya. Mengunduh aplikasi hanya dari Google Play Store atau sumber yang terverifikasi akan membantu mengurangi kemungkinan terkena malware atau aplikasi berbahaya yang dapat membahayakan perangkat dan data pribadi.

Sementara itu, meskipun pengembang iOS telah menerapkan kontrol ketat terhadap aplikasi

yang masuk ke platform mereka, mereka dapat mempertimbangkan untuk memberikan lebih banyak fleksibilitas tanpa mengorbankan kontrol terhadap keamanan. Fleksibilitas ini penting untuk mendukung inovasi dan memberikan lebih banyak pilihan bagi pengguna, tanpa mengurangi standar keamanan yang tinggi yang sudah diterapkan oleh Apple.

Dari sisi pengguna, disarankan untuk memilih sistem operasi yang sesuai dengan prioritas mereka, baik dari segi keamanan, harga, maupun fitur yang dibutuhkan. Keputusan ini harus didasarkan pada pemahaman yang mendalam tentang kelebihan dan kekurangan masing-masing sistem operasi.

Dengan upaya bersama antara pengembang dan pengguna, diharapkan keamanan aplikasi mobile dapat terus ditingkatkan. Pendekatan kolaboratif ini akan menciptakan pengalaman yang lebih aman dan nyaman bagi semua pihak yang terlibat, baik pengembang, pengguna, maupun penyedia layanan aplikasi mobile. Keamanan yang lebih baik akan memperkuat kepercayaan pengguna terhadap platform mobile dan memungkinkan ekosistem aplikasi berkembang dengan lebih positif.

6. DAFTAR PUSTAKA

Adascalitei, I., 2019. Smartphones and IoT Security. IE 23, 63–75. https://doi.org/10.12948/issn14531305/23.2.2019.06

Alamsyah, J., Artamevia, K., Siraj, M., 2024. Perbandingan Keunggulan dan Kelemahan Android dan iOS: Fitur, UI, Keamanan. Universitas Islam Indonesia.

Alviansyah, A., Ramadhani, E., 2021. Implementasi Dynamic Application Security Testing pada Aplikasi Berbasis Android.

Arnomo, S., Hendra, H., 2019. Perbandingan Fitur Smartphone, Pemanfaatan Dan Tingkat Usability Pada Android Dan iOS Platforms. InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan) 3, 184–192. https://doi.org/10.30743/infotekjar.v3i2.1002

Garg, S., Baliyan, N., 2021. Comparative analysis of Android and iOS from security viewpoint. Computer Science Review 40, 100372. https://doi.org/10.1016/j.cosrev.2021.100372

Hilman, A., 2018. Studi Perbandingan Sistem Operasi Android Os 2.2 Dengan Ios Os 4 Dari Segi Arsitektur, Fitur Dan Keamanan. Universitas Esa Unggul.

Joshi, S., Sharma, R., 2019. A Review of Android Security System. International Journal of Scientific Research & Engineering Trends 5.

Kartono, A., Sularsa, A., Ismail, S.J.I., 2019. MEMBANGUN SISTEM PENGUJIAN KEAMANAN APLIKASI ANDROID MENGGUNAKAN MOBSF 5, 146.

Kollnig, K., Shuba, A., Binns, R., Kleek, M.V., Shadbolt, N., 2022. Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. Proceedings on Privacy Enhancing Technologies 2022, 6–24. https://doi.org/10.2478/popets-2022-0033

Mayrhofer, R., Stoep, J.V., Brubaker, C., Hackborn, D., Bonné, B., Tuncay, G.S., Jover, R.P., Specter, M.A., 2021. The Android Platform Security Model (2023). ACM Trans. Priv. Secur. 24, 1–35. https://doi.org/10.1145/3448609

Nurul Syaza Abdul Latif, Mohamed Hafizi Mohamed Nawi, Nurin Nazifa Md Nasir, Ratna Herdiana, 2023. Stability Analysis of Competition Model of iOS and Android. ARASET 30, 372–382. https://doi.org/10.37934/araset.30.3.372382

Pandusaputri, A., Mokodompit, R., Simangunsong, P., Irwansyah, I., 2024. Kenyamanan Pengguna IOS dan Android di Kalangan Generasi Z. SLJIL 9, 3357–3373. https://doi.org/10.36418/syntax-literate.v9i5.16042

Qiya, R., Islam, N., Rai, A., Khan, N., 2020. Usability Analysis of Android and iOS Operating Systems. IJETT 68, 105–111. https://doi.org/10.14445/22315381/IJETT-V68I10P218

Ridwan, K., Hidayanto, B.C., Si, S., Kom, M., n.d. SECURITY COMPARATIVE

ANALYSIS OF INSTANT MESSENGER LINE, WHATSAPP AND TELEGRAM IN.

Sarkar, A., Goyal, A., Hicks, D., Sarkar, D., Hazra, S., 2019. Android Application Development: A Brief Overview of Android Platforms and Evolution of Security Systems, in: 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Presented at the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), IEEE, Palladam, India, pp. 73–79. https://doi.org/10.1109/I-SMAC47947.2019.9032440

Shrivastava, G., Kumar, P., 2019. SensDroid: Analysis for Malicious Activity Risk of Android Application. Multimed Tools Appl 78, 35713–35731. https://doi.org/10.1007/s11042-019-07899-1

Sikder, R., Khan, M.S., Hossain, M.S., Khan, W.Z., 2020. A survey on android security: development and deployment hindrance and best practices. TELKOMNIKA 18, 485. https://doi.org/10.12928/telkomnika.v18i1.13288

Taleby, M., Li, Q., Rabbani, M., Raza, A., 2017. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. ijacsa 8. https://doi.org/10.14569/IJACSA.2017.081005

Wukkadada, B., Nambiar, R., Nair, A., 2015. Mobile Operating System: Analysis and Comparison of Android and iOS 2.

Yasa, R., Nugraha, A., 2024. Perbandingan Keamanan Aplikasi Pesan Instan Android Menggunakan MobSF (Mobile Security Framework) Berdasarkan Beberapa Standar 18, 9–14. https://doi.org/10.56706/ik.v18i1.88