Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 2 Agustus 2025
E-ISSN: 2827-9387, P- ISSN: 2827-9379, Hal 263-270
DOI: https://doi.org/10.55606/jutiti.v5i2.5518
Available Online at : https://journalshub.org/index.php/jutiti

Analisis Malware pada Perangkat Android Menggunakan *Tools Mobsf (Mobile Security Framework)*

Abdul Sakti[1*], Dafrid Cahyadi Arifin[2]
[1,2] Universitas Megarezky, Indonesia
abdulsakti@unimerz.ac.id[1] , mr.dafrid@gmail.com[2]

*Korespondensi penulis: abdulsakti@unimerz.ac.id**

Abstract: *The rapid development of mobile technology has significantly increased the global use of Android devices. However, the open-source nature of the Android operating system makes it vulnerable to malware attacks, especially from applications downloaded through unofficial sources. This study aims to analyze potential malware threats in Android applications using the Mobile Security Framework (MobSF) tool through static and dynamic analysis approaches. Five Android application samples (APK) were analyzed, consisting of apps obtained from both the Google Play Store and third-party websites. The results indicate that applications from unofficial sources carry higher security risks, as evidenced by excessive permissions, modified file structures, and communication with suspicious servers. In contrast, applications from official sources generally showed safer results, although minor vulnerabilities were still identified. MobSF proved to be effective in detecting suspicious behavior and provided security scores that can serve as references in application evaluations. This study emphasizes the importance of conducting security audits on mobile applications prior to widespread use and encourages the utilization of MobSF as a reliable tool for security analysis in Android application development and distribution.*

Keywords*: Android, Malware, MobSF, Static Analysis, Dynamic Analysis, Application Security*

Abstrak: Perkembangan teknologi mobile yang pesat telah meningkatkan penggunaan perangkat Android secara masif di seluruh dunia. Namun, keterbukaan sistem Android menjadikannya rentan terhadap serangan malware, terutama dari aplikasi yang diunduh melalui sumber tidak resmi. Penelitian ini bertujuan untuk menganalisis potensi ancaman malware pada aplikasi Android menggunakan tools MobSF (Mobile Security Framework) melalui pendekatan analisis statis dan dinamis. Lima sampel aplikasi Android (APK) dianalisis, terdiri dari aplikasi yang berasal dari Google Play Store dan situs pihak ketiga. Hasil penelitian menunjukkan bahwa aplikasi dari sumber tidak resmi memiliki tingkat risiko yang lebih tinggi, ditandai dengan izin akses berlebihan, struktur file yang dimodifikasi, dan komunikasi dengan server mencurigakan. Sementara itu, aplikasi dari sumber resmi umumnya menunjukkan hasil yang lebih aman, meskipun tetap ditemukan potensi kerentanan kecil. MobSF terbukti efektif dalam mendeteksi aktivitas mencurigakan dan memberikan skor keamanan yang dapat digunakan sebagai acuan dalam evaluasi aplikasi. Penelitian ini menegaskan pentingnya audit keamanan terhadap aplikasi mobile sebelum digunakan secara luas, serta mendorong pemanfaatan MobSF sebagai alat bantu analisis keamanan dalam pengembangan dan distribusi aplikasi Android.

Kata kunci: Android, Malware, MobSF, Analisis Statis, Analisis Dinamis, Keamanan Aplikasi

1. PENDAHULUAN

Perkembangan teknologi digital yang pesat telah memberikan dampak signifikan terhadap berbagai aspek kehidupan manusia, termasuk dalam hal komunikasi, transaksi keuangan, dan akses informasi. Salah satu wujud dari perkembangan tersebut adalah meningkatnya penggunaan perangkat mobile, terutama smartphone berbasis sistem operasi Android. Android menjadi sistem operasi paling populer di dunia karena bersifat open source, fleksibel, dan didukung oleh ekosistem pengembang yang luas. Namun, popularitas ini juga menjadikan Android sebagai sasaran utama serangan siber, khususnya dalam bentuk malware.

Received: Juni 14, 2025; Revised: Juni 28, 2025; Accepted: Juli 10, 2025; Online Available: Juli 12, 2025

Malware atau *malicious software* adalah perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, atau mendapatkan akses tidak sah terhadap perangkat pengguna. Menurut Suhartono (2020), penyebaran malware pada perangkat Android meningkat seiring dengan rendahnya kesadaran pengguna terhadap keamanan siber dan tingginya penggunaan aplikasi dari sumber yang tidak terpercaya. Ancaman malware ini tidak hanya berpotensi mengganggu kinerja perangkat, tetapi juga dapat membahayakan data pribadi dan informasi sensitif pengguna.

Dalam beberapa tahun terakhir, berbagai jenis malware yang menyerang Android telah berkembang dengan teknik yang semakin canggih. Ramadhani dan Santoso (2021) mencatat bahwa malware tidak lagi hanya menyerang secara langsung, tetapi juga menyusup melalui aplikasi-aplikasi yang tampak sah. Hal ini menunjukkan pentingnya adanya langkah preventif dan deteksi dini untuk mengidentifikasi potensi ancaman sebelum aplikasi digunakan oleh publik.

Salah satu pendekatan yang kini banyak digunakan dalam menganalisis keamanan aplikasi mobile adalah dengan memanfaatkan tools analisis keamanan. Mobile Security Framework (MobSF) merupakan salah satu tools open-source yang efektif untuk menganalisis aplikasi Android secara statis maupun dinamis. Menurut Haryanto dan Nugraha (2023), MobSF mampu mengidentifikasi berbagai celah keamanan dalam aplikasi, termasuk izin yang mencurigakan, komunikasi jaringan tidak aman, hingga potensi keberadaan kode berbahaya dalam file APK.

MobSF memberikan kemudahan dalam melakukan proses reverse engineering terhadap file APK, serta menyajikan laporan keamanan yang terstruktur dan mudah dipahami. Tools ini tidak hanya relevan untuk pengembang aplikasi, tetapi juga penting digunakan dalam konteks penelitian keamanan siber dan forensik digital. Wahyuni (2021) menunjukkan bahwa MobSF berhasil mendeteksi aktivitas komunikasi tersembunyi pada aplikasi yang terinfeksi malware dengan tingkat akurasi tinggi.

Melihat urgensi dari peningkatan serangan malware di platform Android serta kebutuhan akan tools analisis yang handal, maka penting untuk melakukan penelitian yang mendalam terkait efektivitas MobSF dalam mengidentifikasi ancaman malware. Penelitian ini diharapkan dapat memberikan kontribusi dalam bidang keamanan mobile, khususnya dalam memberikan pemahaman tentang bagaimana analisis statis dan dinamis dapat digunakan untuk mendeteksi potensi serangan dari aplikasi Android.

Penelitian ini juga bertujuan untuk menguji dan mengevaluasi hasil analisis dari MobSF dalam konteks deteksi malware yang umum beredar di Indonesia. Dengan menganalisis

beberapa sampel aplikasi Android, baik yang resmi maupun tidak resmi, penelitian ini akan mengungkap pola umum serangan serta karakteristik aplikasi yang mengandung ancaman tersembunyi.

Selain itu, hasil dari penelitian ini diharapkan dapat menjadi referensi praktis bagi pengguna, pengembang aplikasi, maupun instansi yang bergerak di bidang keamanan informasi, untuk memahami pentingnya proses audit keamanan sebelum aplikasi digunakan secara luas. Ke depannya, dengan semakin berkembangnya ancaman digital, tools seperti MobSF perlu terus diperbarui dan diterapkan secara luas untuk meningkatkan ketahanan sistem dan perlindungan data pengguna Android.

Dengan latar belakang tersebut, penelitian ini mengangkat topik "Analisis Malware pada Perangkat Android Menggunakan Tools MobSF (Mobile Security Framework)" sebagai bentuk kontribusi terhadap pengembangan metode deteksi keamanan aplikasi mobile berbasis Android dalam upaya memperkuat keamanan siber nasional.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif yang bertujuan untuk menggambarkan dan menganalisis potensi ancaman malware pada aplikasi Android dengan bantuan tools MobSF (Mobile Security Framework). Pendekatan ini dipilih karena memungkinkan peneliti untuk mengkaji lebih dalam mengenai karakteristik aplikasi, pola perilaku mencurigakan, serta jenis kerentanan keamanan yang ditemukan melalui proses analisis statis dan dinamis. Data dikumpulkan melalui dokumentasi, observasi langsung, serta uji coba terhadap sampel aplikasi menggunakan MobSF.

Prosedur penelitian dilakukan dalam beberapa tahapan utama, yaitu: (1) pengumpulan sampel aplikasi Android berupa file APK dari berbagai sumber, baik dari Google Play Store maupun situs pihak ketiga; (2) analisis statis menggunakan MobSF untuk mengevaluasi struktur file, izin akses, dan kode sumber aplikasi; dan (3) analisis dinamis yang dilakukan dalam sandbox MobSF untuk mengamati perilaku runtime aplikasi seperti aktivitas jaringan, komunikasi dengan server eksternal, dan penggunaan API mencurigakan. Setiap hasil dianalisis secara sistematis dan dibandingkan untuk mengidentifikasi indikasi malware atau aktivitas mencurigakan lainnya.

Validitas data diperkuat dengan melakukan triangulasi teknik, yaitu membandingkan hasil analisis MobSF dengan referensi data dari platform keamanan lain seperti VirusTotal atau laporan komunitas keamanan siber. Analisis data dilakukan secara kualitatif dengan menginterpretasikan hasil scan dan log aktivitas yang dihasilkan MobSF, kemudian

dikategorikan sesuai dengan jenis ancaman dan dampak potensialnya. Hasil akhir dari penelitian ini diharapkan memberikan gambaran yang jelas mengenai efektivitas MobSF dalam mendeteksi malware serta menjadi rujukan bagi pengguna dan pengembang aplikasi dalam mengamankan ekosistem Android.

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan dengan menganalisis lima sampel aplikasi Android (file APK) yang diunduh dari dua sumber berbeda, yaitu Google Play Store dan situs pihak ketiga yang tidak resmi. Penggunaan dua sumber ini bertujuan untuk membandingkan tingkat keamanan antara aplikasi resmi dan aplikasi dari sumber tidak terpercaya. Setiap sampel dianalisis menggunakan MobSF melalui dua pendekatan utama, yakni analisis statis dan analisis dinamis.

Pada tahap analisis statis, ditemukan bahwa tiga dari lima aplikasi memiliki *permission* yang berlebihan atau tidak sesuai dengan fungsi utamanya. Misalnya, satu aplikasi kalkulator dari situs tidak resmi meminta akses ke kontak, lokasi, serta kamera. Menurut laporan MobSF, hal ini mengindikasikan adanya potensi penyalahgunaan data pengguna. Selain itu, ditemukan pula adanya *hardcoded API key* dan informasi kredensial dalam file AndroidManifest.xml dan res/values/strings.xml, yang seharusnya tidak ditanamkan langsung dalam kode aplikasi.

Dari sisi struktur file dan kode sumber, dua aplikasi dari sumber tidak resmi menunjukkan adanya file dex tambahan yang telah dipaket ulang, serta obfuscation tingkat tinggi pada kelas Java-nya. MobSF menandai keberadaan kelas dengan nama acak dan fungsi-fungsi yang tidak terdokumentasi sebagai indikator potensi aktivitas tersembunyi, seperti pengumpulan data secara diam-diam atau komunikasi ke server tertentu.

Pada analisis dinamis, yang dilakukan di lingkungan sandbox milik MobSF, ditemukan bahwa dua aplikasi yang teridentifikasi mencurigakan mencoba melakukan komunikasi dengan server eksternal yang berasal dari luar negeri, menggunakan protokol HTTP yang tidak dienkripsi. Salah satu aplikasi bahkan secara aktif mengirim data lokasi GPS dan status perangkat tanpa izin eksplisit dari pengguna. Log aktivitas jaringan dari MobSF menunjukkan pola pengiriman data secara periodik setelah aplikasi dijalankan.

Aplikasi dari Play Store umumnya menunjukkan hasil yang lebih aman, dengan izin akses yang relevan dengan fungsi aplikasi, serta tidak ditemukan aktivitas mencurigakan selama sesi runtime. Meskipun begitu, satu aplikasi tetap menunjukkan adanya potensi kerentanan berupa pemanggilan fungsi *WebView* tanpa validasi input, yang dapat dimanfaatkan untuk serangan injeksi jika tidak diperbaiki. Temuan ini menegaskan bahwa bahkan aplikasi dari sumber resmi tetap perlu diaudit secara berkala.

MobSF juga menghasilkan skor keamanan (security score) untuk setiap aplikasi, dengan rentang nilai 0–100. Dua aplikasi dari sumber tidak resmi mendapatkan skor di bawah 50, menandakan tingkat risiko tinggi, sementara aplikasi dari Play Store rata-rata mendapatkan skor di atas 75. Ini menunjukkan bahwa penggunaan MobSF mampu memberikan gambaran kuantitatif terkait seberapa besar potensi risiko yang dimiliki sebuah aplikasi.

Dalam aspek komunikasi jaringan, fitur *network monitoring* pada MobSF berhasil mencatat semua permintaan keluar yang dilakukan oleh aplikasi. Aktivitas ini penting untuk mendeteksi apakah aplikasi mencoba mengakses domain yang terasosiasi dengan malware atau server anonim. Dua aplikasi diketahui mengakses domain yang telah masuk dalam daftar hitam berdasarkan database VirusTotal, memperkuat indikasi bahwa aplikasi tersebut bersifat berbahaya.

Secara keseluruhan, penggunaan MobSF terbukti efektif dalam mengidentifikasi pola-pola yang mengarah pada keberadaan malware dalam aplikasi Android. Baik dari segi struktur kode, izin akses, aktivitas runtime, hingga komunikasi jaringan, semua komponen penting dalam penilaian keamanan aplikasi dapat terdeteksi secara sistematis. Temuan ini menunjukkan bahwa MobSF dapat dijadikan alat bantu utama dalam proses audit keamanan aplikasi mobile.

Berdasarkan hasil tersebut, penelitian ini menyimpulkan bahwa aplikasi Android dari sumber tidak resmi memiliki potensi risiko keamanan yang jauh lebih tinggi dibandingkan aplikasi dari sumber resmi. Oleh karena itu, pengguna disarankan untuk hanya mengunduh aplikasi dari toko aplikasi yang terpercaya, serta pengembang perlu secara rutin melakukan uji keamanan menggunakan tools seperti MobSF guna memastikan aplikasi bebas dari elemen berbahaya yang dapat merugikan pengguna.

Pembahasan

Hasil penelitian menunjukkan bahwa aplikasi Android yang berasal dari sumber tidak resmi memiliki risiko keamanan yang jauh lebih tinggi dibandingkan dengan aplikasi dari toko resmi seperti Google Play Store. Temuan ini sejalan dengan pernyataan Ramadhani dan Santoso (2021) yang menyatakan bahwa toko aplikasi pihak ketiga sering kali tidak memiliki sistem validasi keamanan yang ketat, sehingga memungkinkan malware menyusup dalam bentuk aplikasi palsu. Dalam penelitian ini, dua dari lima aplikasi mengandung kode obfuscated dan izin yang tidak relevan, yang menunjukkan adanya potensi penyalahgunaan data pengguna.

Analisis statis menggunakan MobSF berhasil mengungkap keberadaan *hardcoded credentials* dan struktur file APK yang telah dimodifikasi. Temuan ini memperkuat pendapat

Suhartono (2020) bahwa metode analisis statis sangat penting dalam mengidentifikasi potensi serangan melalui rekayasa balik (reverse engineering). Dengan melihat struktur kode dan metadata aplikasi, peneliti dapat mendeteksi indikasi awal dari ancaman siber, bahkan sebelum aplikasi dijalankan.

Pada sisi analisis dinamis, penggunaan sandbox MobSF mampu mengungkap aktivitas mencurigakan seperti komunikasi ke server asing, pengiriman data lokasi, dan penggunaan API tanpa enkripsi. Aktivitas seperti ini sesuai dengan karakteristik spyware dan trojan, sebagaimana dijelaskan oleh Wahyuni (2021) yang menyebutkan bahwa malware canggih saat ini sering menyamar sebagai aplikasi biasa tetapi diam-diam mengakses data pengguna dan mengirimkannya ke pihak ketiga. Hasil dari log aktivitas dan pemantauan jaringan MobSF memperkuat kesimpulan tersebut.

Pentingnya pengawasan pada komunikasi aplikasi melalui protokol jaringan juga didukung oleh penelitian Lestari dkk. (2022), yang menemukan bahwa sebagian besar malware Android modern memanfaatkan protokol HTTP tanpa enkripsi untuk mengirim data karena lebih sulit dideteksi oleh antivirus konvensional. Dalam penelitian ini, dua aplikasi dari sumber tidak resmi menunjukkan aktivitas komunikasi dengan domain berisiko, yang telah tercatat dalam database hitam seperti VirusTotal.

MobSF juga memberikan skor keamanan berdasarkan hasil analisis terhadap izin akses, kerentanan, dan aktivitas runtime. Skor ini memberikan gambaran awal bagi pengguna atau auditor keamanan untuk mengukur seberapa berisiko suatu aplikasi. Yulianto dan Prasetyo (2024) menyatakan bahwa skor keamanan dari MobSF dapat digunakan sebagai parameter awal dalam proses audit keamanan aplikasi, terutama dalam proses *penetration testing* atau *security assessment* terhadap produk digital yang akan dipublikasikan.

Temuan bahwa beberapa aplikasi dari Play Store juga memiliki potensi kerentanan meskipun lebih kecil mengindikasikan bahwa tidak ada aplikasi yang benar-benar aman tanpa pengujian tambahan. Hal ini sejalan dengan pendapat Firmansyah (2023) yang menyebutkan bahwa meskipun platform resmi seperti Google Play memiliki sistem keamanan yang lebih baik, tetap diperlukan *manual auditing* atau *external scanning* untuk menjamin keamanan aplikasi secara menyeluruh, terutama jika aplikasi digunakan dalam skala besar seperti di sektor keuangan atau pemerintahan.

Penggunaan MobSF terbukti menjadi langkah yang efektif dan efisien dalam menganalisis keamanan aplikasi Android. Tools ini tidak hanya mendeteksi kerentanan teknis, tetapi juga mengidentifikasi pola perilaku mencurigakan yang mengarah pada aktivitas malware. Hal ini didukung oleh Haryanto dan Nugraha (2023) yang menyatakan bahwa MobSF

adalah salah satu tools open-source paling komprehensif dalam konteks analisis keamanan mobile karena kemampuannya untuk melakukan analisis statis, dinamis, dan analisis kode sumber sekaligus.

Dengan mempertimbangkan hasil dan pendapat para ahli, maka dapat disimpulkan bahwa MobSF memiliki keandalan tinggi sebagai alat bantu utama dalam audit keamanan aplikasi Android. Di tengah meningkatnya ancaman digital yang terus berevolusi, pendekatan preventif seperti ini menjadi semakin penting. Penelitian ini juga memperlihatkan bahwa edukasi kepada pengguna untuk lebih waspada terhadap sumber aplikasi sangat krusial dalam memutus rantai penyebaran malware.

Secara keseluruhan, pembahasan ini menegaskan bahwa penggunaan tools seperti MobSF dapat menjadi bagian penting dari strategi keamanan aplikasi mobile. Selain bermanfaat untuk pengembang dan peneliti, penerapan MobSF juga relevan bagi institusi pemerintah atau swasta yang ingin menjaga keamanan informasi internal mereka dari potensi ancaman yang berasal dari perangkat mobile, sejalan dengan kebutuhan keamanan digital nasional yang semakin meningkat di era transformasi digital saat ini.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa MobSF (Mobile Security Framework) merupakan tools yang efektif dan komprehensif dalam menganalisis potensi ancaman malware pada aplikasi Android. Melalui pendekatan analisis statis dan dinamis, MobSF mampu mengidentifikasi berbagai indikator berbahaya, seperti izin akses yang mencurigakan, struktur kode yang dimodifikasi, komunikasi jaringan tidak terenkripsi, dan keberadaan file yang menunjukkan tanda-tanda rekayasa.

Aplikasi yang diperoleh dari sumber tidak resmi terbukti memiliki tingkat risiko keamanan yang jauh lebih tinggi dibandingkan aplikasi dari Google Play Store. Temuan ini menguatkan pentingnya memilih sumber aplikasi yang terpercaya dan menunjukkan perlunya pengujian keamanan sebelum aplikasi digunakan secara luas. Hasil skor keamanan dan log aktivitas runtime dari MobSF memberikan bukti kuat bahwa banyak aplikasi berpotensi melakukan pelanggaran privasi pengguna.

Dengan demikian, penggunaan MobSF tidak hanya penting bagi pengembang aplikasi dalam mengamankan produknya sebelum dirilis, tetapi juga sangat relevan digunakan oleh peneliti keamanan, instansi pemerintah, dan pengguna umum yang peduli terhadap perlindungan data pribadi. Penelitian ini menegaskan bahwa pendekatan preventif melalui

audit aplikasi menggunakan tools seperti MobSF harus menjadi bagian integral dari strategi keamanan digital di era transformasi teknologi yang terus berkembang.

DAFTAR PUSTAKA

Azizah, S., & Kurniawan, B. (2022). Evaluasi Keamanan Mobile Application Menggunakan Static Code Analysis. Jurnal Rekayasa Perangkat Lunak, 5(2), 119–130.

Fadli, M., & Hartono, R. (2021). Tinjauan Terhadap Teknik Obfuscation dalam Penyembunyian Malware Android. Jurnal Keamanan Sistem Informasi, 2(1), 33–45.

Firmansyah, I. (2023). Urgensi Keamanan Aplikasi Android di Era Digital: Studi Audit Keamanan Berbasis MobSF. Jurnal Teknologi dan Informasi Terkini, 5(1), 66–74.

Haryanto, R., & Nugraha, T. (2023). Penerapan Mobile Security Framework dalam Audit Keamanan Aplikasi Android. Jurnal Keamanan Siber Indonesia, 5(2), 112–125.

Lestari, D., Firmansyah, A., & Widodo, B. (2022). Analisis Keamanan Aplikasi Android dari Sumber Tidak Resmi Menggunakan Sandbox Analysis. Jurnal Teknologi Informasi dan Keamanan, 6(1), 45–59.

Maulana, I. (2020). Ancaman Keamanan Mobile: Tren dan Mitigasi di Indonesia. Jurnal Teknologi dan Keamanan Siber Nasional, 1(1), 1–10.

Nugroho, D., & Alfian, R. (2020). Implementasi Analisis APK Menggunakan MobSF dalam Mendeteksi Potensi Malware. Jurnal Keamanan Teknologi Informasi, 2(2), 51–60.

Nurhaliza, R. (2022). Penerapan Reverse Engineering dalam Deteksi Malware Aplikasi Mobile. Prosiding Seminar Nasional Teknologi Informasi, 4(1), 101–110.

Oktaviani, M. (2023). Keamanan Data Pribadi dalam Aplikasi Android: Studi Literatur pada Tools Analisis Mobile. Jurnal Penelitian Teknologi dan Privasi, 6(3), 78–85.

Ramadhani, M., & Santoso, E. (2021). Ancaman Malware pada Perangkat Android: Studi Kasus Aplikasi Pihak Ketiga. Jurnal Ilmiah Teknologi dan Keamanan Informasi, 3(2), 76–88.

Saputra, D. A., & Hidayat, R. (2021). Perbandingan Efektivitas Analisis MobSF dengan Tools Lain dalam Deteksi Ancaman Mobile. Jurnal Rekayasa Keamanan Siber, 3(2), 92–104.

Suhartono, A. (2020). Keamanan Sistem Operasi Android terhadap Ancaman Malware. Jurnal Sistem dan Informatika, 8(1), 33–40.

Wahyuni, S. (2021). Analisis Statis dan Dinamis Aplikasi Android Menggunakan MobSF untuk Deteksi Malware. Jurnal Informatika dan Komputer, 4(3), 90–100.

Widiyanto, P. (2024). Analisis Forensik Digital Terhadap Aplikasi Android Berbahaya. Jurnal Digital Forensik Indonesia, 4(1), 18–28.

Yulianto, D., & Prasetyo, F. (2024). Pengukuran Risiko Keamanan Aplikasi Mobile Menggunakan Metode Penilaian MobSF. Jurnal Riset Keamanan Digital, 7(1), 12–22.