Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 8 Nomor 1 Maret 2025, Hal 1-11
ISSN 2723- 6129 (media online)
Link Jurnal: https://ejournal.sisfokomtek.org/index.php/jikom

Analisis Keamanan Data Pribadi Pada Aplikasi Satusehat Berbasis Mobile Android Dengan Metode Statis Dan Dinamis

Qoyum Milati Tri Rejeki
Informatika, Unversitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: qoyum1900018233@webmai.uad.ac.id
Email Penulis Korespondensi: qoyum1900018233@webmai.uad.ac.id

Abstrak−Pemerintah menggunakan aplikasi PeduliLindungi untuk mencegah penyebaran Covid-19, yang kini bertransformasi menjadi SatuSehat Mobile. Aplikasi SatuSehat Mobile memerlukan data pribadi pengguna dalam menjalankan aplikasi, namun meningkatnya penggunaan teknologi juga meningkatkan risiko *cybercrime*, sehingga pengguna meragukan keamanan aplikasi dan data pengguna pada aplikasi tersebut. Penelitian ini bertujuan untuk menganalisis celah keamanan pada aplikasi SatuSehat Mobile dan PeduliLindungi serta data pengguna melalui penerapan metode analisis statis dan analisis dinamis. Penelitian ini menggunakan analisis statis dan analisis dinamis dengan proses digital forensik *National Institute of Standards and Technology* yang terdiri dari *collection, examination, analysis* dan *reporting*. Alat forensik yang digunakan yaitu *Mobile Security Framework* (MobSF) dan *Intezer* dengan parameter penggunaan *dangerous permission, weak crypto, domain maleware check* dan *root detection*. *Collection* (pengumpulan) data digital dari *smartphone* android, *examination* (pemeriksaan) mencakup pemilihan data-data yang diperlukan dari file aplikasi, *analysis* dilakukan menggunakan *tools* MobSF dan *Intezer*, *reporting* (pelaporan) menuliskan penemuan dan laporan secara terstruktur. Hasil penelitian menunjukkan kedua aplikasi terdapat 4 *weak crypto*, yang terdiri dari 1 *high severity* dan 3 *warning severity*. Aplikasi SatuSehat Mobile memiliki 10 *dangerous permission* (*access_background_location, access_coarse_location, access_fine_location, camera, post_notifications, read_external_storage, read_media_audio, read_media_images, read_media_video, write_external_storage*), sedangkan aplikasi pedulilindungi memiliki 9 *dangerous permission (access_background_location, access_coarse_location, access_fine_location, bluetooth_advertise, bluetooth_connect, bluetooth_scan, camera, read_external_storage, write_external_storag)*. *Domain maleware check* dan *root detection* kedua aplikasi berstatus baik. *Maleware* berbahaya tidak terdeteksi dalam kedua aplikasi. Pengguna sebaiknya menonaktifkan izin yang tidak diperlukan oleh fungsionalitas aplikasi agar tidak tereksploitasi.

Kata Kunci: Keamanan aplikasi, SatuSehat Mobile, Forensik digital, *MobSF*, *NIST*.

Abstract−The government uses the PeduliLindungi application to prevent the spread of Covid-19, which has now transformed into SatuSehat Mobile. The SatuSehat Mobile application requires personal user data to run the application, but the increasing use of technology also increases the risk of cybercrime, so that users doubt the security of the application and user data on the application. This study aims to analyze security gaps in the SatuSehat Mobile and PeduliLindungi applications and user data through the application of static analysis and dynamic analysis methods. This study uses static analysis and dynamic analysis with the National Institute of Standards and Technology digital forensic process consisting of collection, examination, analysis and reporting. The forensic tools used are the Mobile Security Framework (MobSF) and Intezer with the parameters of using dangerous permission, weak crypto, domain malware check and root detection. Collection of digital data from Android smartphones, examination includes selecting the necessary data from application files, analysis is carried out using the MobSF and Intezer tools, reporting writes findings and reports in a structured manner. The results of the study showed that both applications contained 4 weak crypto, consisting of 1 high severity and 3 warning severity. SatuSehat Mobile application has 10 dangerous permissions (access_background_location, access_coarse_location, access_fine_location, camera, post_notifications, read_external_storage, read_media_audio, read_media_images, read_media_video, write_external_storage), while Pedulilindungi application has 9 dangerous permissions (access_background_location, access_coarse_location, access_fine_location, bluetooth_advertise, bluetooth_connect, bluetooth_scan, camera, read_external_storage, write_external_storage). Domain malware check and root detection of both applications have good status. Malicious malware was not detected in both applications. Users should disable permissions that are not required by the application's functionality to avoid exploitation.

Keywords: Application security, SatuSehat Mobile, Digital forensics, MobSF, NIST

1. PENDAHULUAN

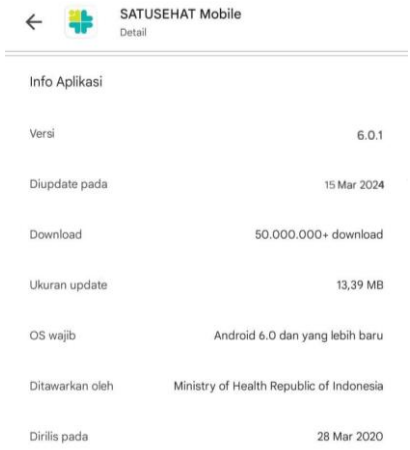
Munculnya penyakit Coronavirus Disease-2019 yang selanjutnya disebut COVID-19 disebabkan oleh Severe Acute Respiratory Syndrom Coronavirus-2 (SARS-COV-2) salah satu jenis Coronavirus, telah menjadikan Indonesia sebagai salah satu negara yang cukup terdampak akibat munculnya penyakit tersebut. Pemerintah telah mengambil berbagai cara untuk mencegah dan mengurangi penyebaran COVID-19, salah satunya melalui pemanfaatan teknologi. Pemerintah memanfaatkan aplikasi pengawasan bernama PeduliLindungi yang dikembangkan oleh Kementerian Badan Usaha Milik Negara bersama dengan Kementerian Komunikasi dan Informatika Republik Indonesia dan PT. Telkom

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 8 Nomor 1 Maret 2025, Hal 1-11
ISSN 2723- 6129 (media online)
Link Jurnal: https://ejournal.sisfokomtek.org/index.php/jikom

Indonesia. Aplikasi ini menggunakan data pribadi pengguna dan smartphone data untuk melacak lokasi pengguna dengan memanfaatkan jaringan Bluetooth[1].

Pada tanggal 01 Maret 2023 Kementrian Kesehatan Republik Indonesia resmi mentransformasikan PeduliLindungi menjadi aplikasi kesehatan masyarakat bernama SatuSehat Mobile[2]. SatuSehat Mobile dapat membantu pengguna melakukan pencegahan penyebaran COVID-19 melalui pemberitahuan status vaksin (Screening), Pelacakan (tracking) dan pemberitahun pringatan (warning and fencing), SatuSehat Mobile juga menjadi salah satu platform untuk berbagai informasi kesehatan dan program dari kementrian kesehatan. SatuSehat Mobile dilengkapi dengan fitur Resume Medis, Cari Obat, Cari Nakes, Pengingat Minum Obat, Vaksin dan Imunisasi, Diari Kesehatan, Hasil Tes COVID-19, Cari Rawat Inap dan Pelayanan Kesehatan. Aplikasi SatuSehat Mobile dalam penggunaannya memerlukan proses registrasi akun dengan menginputkan informasi terkait data pribadi pengguna seperti Kewarganegaraan, Nomor Handphone/Email, Nama Lengkap, Tanggal Lahir dan Nomor Induk Kependudukan.



Gambar 1. Detail Aplikasi SatuSehat Mobile pada *Android Play Store*

Pada Gambar 1 menunjukkan aplikasi SatuSehat Mobile telah di download 50.000.000 lebih pengguna dari Android Play Store sejak dirilis 28 Maret 2020. Meningkatnya penggunaan teknologi dan informasi dapat menyebabkan semakin tinggi peluang terjadinya cybercrime pada pengguna internet. Dilansir dari encyclopedia Britannica, cybercrime atau kejahatan komputer merupakan penggunaan komputer melakukan tindakan ilegal seperti melakukan penipuan, perdagangan konten pornografi anak, pencurian identitas dan pelanggaran privasi seseorang.

Gambar 1. Ulasan dan penilaian aplikasi SatuSehat Mobile pada *Android Play Store*

Rating ulasan dan penilaian pengguna aplikasi SatuSehat Mobile pada Android Play Store dapat dilihat pada Gambar 2 berdasarkan gambar tersebut tidak sedikit pengguna yang memberikan penilaian buruk pada aplikasi SatuSehat Mobile, pengguna mulai meragukan keamanan dan penggunaan data pribadi yang diberikan pengguna pada aplikasi SatuSehat Mobile tersebut. Mengingat telah banyak keamanan dan penggunaan data pribadi yang bocor pada situs resmi pemerintah khusunya identitas pribadi pengguna. Kasus pertama pada 04 September 2021 dengan bocornya Nomor Induk Kependudukan (NIK) Presiden Republik Indonesia, menimbulkan kepanikan pada masyarakat[3]. Hal tersebut menyebabkan tersebarnya sertifikat vaksin Presiden Republik Indonesia pada media sosial yang telah diakses

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

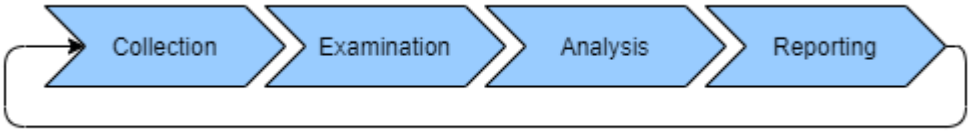
oleh pengguna lain dari aplikasi PeduliLindungi. Selain itu yang terbaru kasus pemalsuan sertifikat vaksin COVID-19 dampak dari belum meratanya vaksinasi COVID-19 di Indonesia[4].

Berdasarkan permasalahan diatas maka perlu dilakukan sebuah penelitian dengan judul "Analisis Keamanan Data Pribadi Pada Aplikasi SatuSehat Berbasis Mobile Android dengan Metode Analisis Statis dan Dinamis". Penelitian ini mencoba menganalisis keamanan data pribadi pengguna aplikasi SatuSehat Mobile serta bagaimana pengolahan data pribadi pada aplikasi SatuSehat Mobile, yang dimana nantinya tidak terlepas dari proses digital forensik. Digital forensik sebagai alat untuk mengumpulkan bukti dalam kasus pembunuhan prospektif yang dapat dituntut secara hukum, forensik digital menggunakan teknik analitis dan investigasi untuk mencari, mengumpulkan, memeriksa, dan menyajikan informasi yang direkam secara magnetis dikomputer atau media digital lainnya[5]. Melakukan digital forensik dibutuhkan alur kerja atau metode untuk mempermudah dalam pelaksanaannya. Metode dalam penelitian ini adalah Analisis Statis dan analisis Dinamis dengan proses digital forensik National Institute of Standards and Technology (NIST) yang terdiri dari collection, examination, analysis dan reporting yang akan dilakukan dengan tools Mobile Security Fremwork (MobSF) dan Intezer. Keamanan data pribadi pada aplikasi SatuSehat Mobile akan dilihat dengan menganalisis Weak Crypto, Dangerous Permission, Domain Maleware Check, Root detection, Data dan Database. Penggunaan algoritma kriptografi lemah dapat menjadi celah rentannya data pengguna terhadap pencurian atau manipulasi, sehingga pentingnya menggunakan algoritma yang memadai untuk melindungi data. Dangerous Permission pada aplikasi harus dianalisis untuk mencegah penyalahgunaan data dalam memberikan perizinan akses. Domain Malware Check diperlukan untuk memberikan perlindungan dari ancaman luar seperti malware atau phishing. Root detection pada perangkat membantu mengurangi risiko keamanan. Data dan Database merupakan pusat penyimpanan informasi dalam aplikasi. Keamanan dalam penyimpanan data sangat penting untuk mencegah kebocoran data, pencurian informasi, atau manipulasi data yang dapat merugikan pengguna. Setelah itu akan diperolah hasil seperti apa keamanan data pribadi pada aplikasi SatuSehat Mobile serta ada atau tidaknya potensi kebocoran data pada aplikasi tersebut yang dapat membahayakan pengguna aplikasi.

Penelitian ini dilakukan dengan harapan dapat mengetahui keamana data pribadi pada aplikasi SatuSehat Mobile, sehingga pengguna aplikasi SatuSehat Mobile tidak perlu merasa khawatir terkait keamanan data pribadi yang telah diberikan saat menggunakan aplikasi SatuSehat Mobile.

2. METODOLOGI PENELITIAN

Metode yang digunakan dalam analisis aplikasi SatuSehat Mobile adalah menggunakan metode analisis statis dan analisis dinamis. Dimana metode analisis ini tidak terlepas dari digital forensik dalam melakukan analisis. Pada dasarnya analisis statis dan analisis dinamis pada aplikasi mobile android dapat dilakukan secara bersamaan atau tidak mengikat terkait urutan prosesnya[6]. Tahapan penelitian ini menggunakan langkah digital forensik untuk menganalisis keamanan data pada aplikasi SatuSehat Mobile dan Aplikasi PeduliLindungi yang dapat dilihat pada Gambar 3.1 berikut.



Gambar 3. Tahapan Digital Forensik [7]

Gambar 3 merupakan 4 tahapan digital forensik unutk melakukan analisis keamanan aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi, yaitu sebagai berikut:

Collection, merupakan pengumpulan pada proses investigasi forensik digital melibatkan kegiatan mengambil, menyalin, dan memperoleh bukti digital atau data yang dapat digunakan untuk penelitian[8]. Pada tahapan ini mengambil aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi yang dirilis oleh Kementrian Kesehatan republik Indonesia pada smartphone android di google play store yang kemudian akan digunakan untuk analisis lebih lanjut.

Examination. Examination merupakan tahapan forensik dengan melakukan backup data atau pencadangan data serta mengidentifikasi data mana saja yang dapat digunakan sebagai barang bukti untuk dilakukan pengujian menggunakan tools forensik[8]. Pada tahapan ini file apk SatuSehat Mobile dan PeduliLindungi akan dilihat Source code yang terdapat dalam aplikasi tersebut menggunakan tools jdax untuk kemudian dilakukan analisis.

Analysis, merupakan tahapan yang dilakukan dengan menganalisis data-data untuk menemukan dan menghasilkan sebuah fakta dalam penyelidikan[8]. Pada tahapan ini aplikasi satusehat mobile dan aplikasi PeduliLindungi akan di analisis dengan parameter Dangerous Permission, Weak Crypto, Root detection dan Domain Maleware Check, Data dan Database

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 8 Nomor 1 Maret 2025, Hal 1-11
ISSN 2723- 6129 (media online)
Link Jurnal: https://ejournal.sisfokomtek.org/index.php/jikom

Reporting, merupakan tahap terakhir dalam proses investigasi forensik digital. Reporting dilakukan dengan menuliskan hasil yang telah diperoleh dari analisis aplikasi SatuSehat mobile dan aplikasi PeduliLindungi dalam bentuk laporan uraian dari analisis dan penyelidikan yang telah dilakukan[8]. Pada tahapan ini akan diperoleh celah keamanan pada aplikasi SatuSehat Mobile untuk mengetahui keamana data aplikasi tersebut.

3. HASIL DAN PEMBAHASAN

Mobile Security Framework (MobSF) merupakan framework open-source yang digunakan untuk melakukan analisis keamanan statis dan dinamis secara otomatis [9]. MobSF menghasilkan laporan analisis berupa penilaian kerentanan yang mengidentifikasi celah-celah keamanan pada plikasi mobile yang ditemukan melalui serangkaian pengujian keamanan yang dijalankan oleh MobSF pada saat proses analisis. Laporan analisis ini Memberikan informasi detail tentang berbagai kelemahan dan potensi celah keamanan pada aplikasi yang dianalisis oleh MobSF[9].

MobSF dalam melakukan analisis pengujian aplikasi memiliki keunggulan yaitu, pengujian pada MobSF tidak dilakukan di cloud hosting pihak ketiga. Maksud dari cloud hosting pihak ketiga adalah layanan hosting yang disediakan oleh perusahaan eksternal yang menawarkan infrastruktur dan platform untuk menyimpan, mengelola, dan mengakses data serta aplikasi melalui internet, Penyedia layanan cloud hosting pihak ketiga biasanya memiliki dan mengelola pusat data (data center) serta infrastruktur komputasi yang memungkinkan pengguna untuk menyewa sumber daya sesuai kebutuhan tanpa harus berinvestasi dalam perangkat keras fisik. Hal tersebut Memberikan tingkat keamanan dan privasi yang lebih baik karena data dan aplikasi yang dilakukan pengujian tidak pernah terekspos atau diunggah ke pihak eksternal, semuanya akan dilakukan secara locak di lingkungan dan dibawah kendali pengguna MobSF[9].

Dengan demikian, MobSF Memberikan solusi komperhensif untuk asesmen keamanan aplikasi mobile dimana pengguna mendapatkan laporan kerentanan aplikasi yang dianalisis serta dapat mempertahankan keamanan san privasi data aplikasinya sendiri selama pengujian dengan MobSF berlangsung.

MobSF melakukan analisis menggunakan metode analisis diantaranya adalah Static Application Security Testing (SAST) dan Dynamic Application Security Testing (DAST). MobSF dalam melakukan analisis memiliki alur kerja dari input sampai dengan output. Alur kerja MobSF dalam melakukan analisis statis seperti pada Gambar 2.3.

Gambar 4 Alur kerja Analisi MobSF [9]

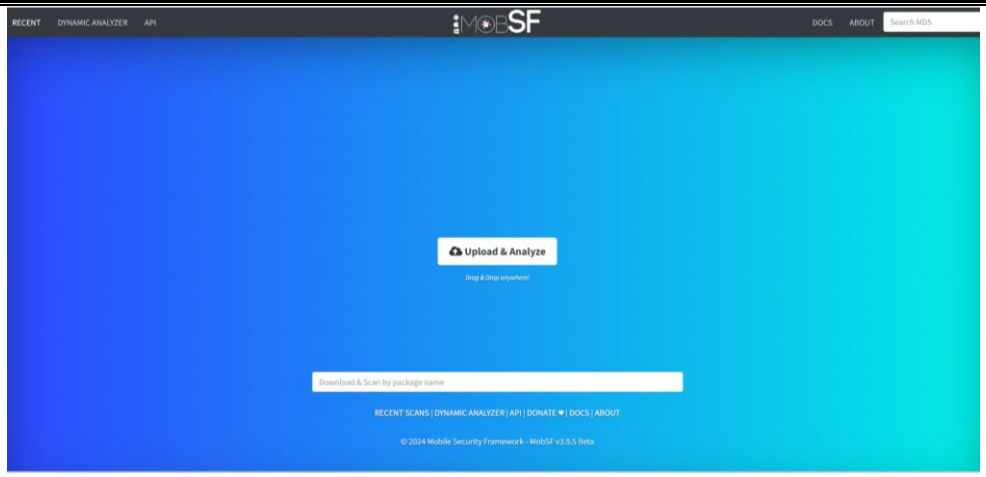
Gambar 4 merupakan alur kerja tools Mobile Security Framework, adapun penjelasan setiap tahapan kerja yang harus dilalui dalam proses tersebut adalah sebagai berikut:

1) Input, pada tahapan ini MobSF akan dijalankan dijaringan lokal pengguna. Kemudian, upload file aplikasi android yang akan dianalisis pada MobSF.
2) Anlysis, tahapan ini MobSF akan menjalankan proses analisis pada aplikasi android.
3) Output, tahapan ini akan menghasilkan laporan penilaian kerentana atau vulnerability assessment report yang berdasarkan hasil pengujian keamanan aplikasi pada MobSF yang telah dilakukan.

Proses analisis file aplikasi SatuSehat Mobile dan aplikasi Pedulilindungi menggunakan MobSF dimulai dengan menginstal serta mengkonfigurasi MobSF dalam windows. MobSF diambil dari github https://github.com/MobSF/Mobile-Security-Framework-MobSF. Setelah konfigurasi dan proses instalasi MobSF pada windows selesai maka MobSF dapat digunakan untuk melakukan analisis aplikasi Mobile.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)
Volume 8 Nomor 1 Maret 2025, Hal 1-11
ISSN 2723- 6129 (media online)
Link Jurnal: https://ejournal.sisfokomtek.org/index.php/jikom



Gambar 5. Halaman Utama *Mobile security framework*[31]

Gambar 5 merupakan halaman utama dari MobSF yang diakses dengan browser pada halaman http://localhost:8000/. Unggah file Apk yang akan dianalisis pada MobSF, tunggu hingga proses analisis selesai. Pada analisis menggunakan MobSF ini aplikasi satuSehat Mobile dan aplikasi PeduliLindungi akan dianalisis dengan parameter dangerous permission, weak crypto, root detection dan maleware check

Setelah melakukan analisis pada aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi menggunakan MobSF, maka diperoleh hadil yang dapat dilihat pada Tabel 1 berikut:

Tabel 1. Hasil Analisis Aplikasi SatuSehat Mobile dan Aplikasi PeduliLindungi

Apk	*Dangerous Permission*	*Weak Crypto*	*Root detection*	*Domain Maleware Check*	*Security Score*
SatuSehat	*Yes*	*Yes*	*Yes*	*Good*	45
PeduliLindungi	*Yes*	*Yes*	*Yes*	*Good*	61

Berdasarkan Tabel 1 diatas dapat dituliskan hasil analisisi aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi sebagai berikut:

3.1 Aplikasi SatuSehat Mobile

a. Dangerous Permission
Terdeteksi 10 dangerous permission Aplikasi SatuSehat Mobile yaitu:
1) android.permission.ACCESS_BACKGROUND_LOCATION,
2) android.permission.ACCESS_COARSE_LOCATION,
3) android.permission.ACCESS_FINE_LOCATION,
4) android.permission.CAMERA,
5) android.permission.POST_NOTIFICATIONS,
6) android.permission.READ_EXTERNAL_STORAGE,
7) android.permission.READ_MEDIA_AUDIO,
8) android.permission.READ_MEDIA_IMAGES,
9) android.permission.READ_MEDIA_VIDEO,
10) android.permission.WRITE_EXTERNAL_STORAGE.

b. Weak Crypto
Aplikasi SatuSehat Mobile terdeteksi memiliki 4 Weak Crypto yang terdiri dari 1 high severity dan 3 warning severity, yaitu:
1) Aplikasi SatuSehat Mobile menggunakan mode enkripsi CBC dengan padding PCKS5/PCKS7, konfigurasi ini rentan terhadap serangan oracle padding yang termasuk High severity.
2) SHA-1 adalah hash lemah yang diketahui memiliki tabrakan hash yang termasuk warning severity.
3) MD5 adalah hash lemah yang diketahui memiliki tabrakan hash warning severity.
4) Aplikasi ini menggunakan generator Angka Acak yang tidak aman warning severity.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

c. Root Detectionn
Aplikasi SatuSehat Mobile memiliki kemampuan root detection yang terdapat dalam Source code file com/telkom/tracencare/MainActivity.java.

d. Domain Maleware Check
Domain maleware check Aplikasi SatuSehat Mobile tidak menunjukkan terdeteksinya domain-domain maleware yang berbahaya, domain-domain aplikasi SatuSehat Mobile berstatus “ok” yang berarti domain aplikasi tersebut tidak terindikasi maleware berrbahaya.

e. Security secore
Security secore aplikasi SatuSehat Mobile menggunakan Mobile Security Framework (MobSF) sebesar 45 (medium risk) yang artinya terdapat beberapa kerentanan atau potensi masalah keamanan namun tidak dalam tingkatan yang sangat kritis.

3.2 Aplikasi PeduliLindungi

a. Dangerous Permission
Terdeteksi 10 dangerous permission Aplikasi PeduliLindungi yaitu:
1) android.permission.ACCESS_BACKGROUND_LOCATION,
2) android.permission.ACCESS_COARSE_LOCATION,
3) android.permission.ACCESS_FINE_LOCATION,
4) android.permission.BLUETOOTH_ADVERTISE,
5) android.permission.BLUETOOTH_CONNECT,
6) android.permission.BLUETOOTH_SCAN,
7) android.permission.CAMERA,
8) android.permission.READ_EXTERNAL_STORAGE,
9) android.permission.WRITE_EXTERNAL_STORAGE.

b. Weak Crypto
Aplikasi PeduliLindungi terdeteksi memiliki 4 Weak Crypto yang terdiri dari 1 high severity dan 3 warning severity, yaitu:
1) Aplikasi SatuSehat Mobile menggunakan mode enkripsi CBC dengan padding PCKS5/PCKS7, konfigurasi ini rentan terhadap serangan oracle padding yang termasuk High severity.
2) SHA-1 adalah hash lemah yang diketahui memiliki tabrakan hash yang termasuk (warning severity).
3) MD5 adalah hash lemah yang diketahui memiliki tabrakan hash (warning severity).
4) Aplikasi ini menggunakan generator angka acak yang tidak aman (warning severity).

c. Root detection
Aplikasi PeduliLindungi Aplikasi SatuSehat Mobile memiliki kemampuan root detection yang terdapat dalam Source code file defpackage/oo0.java.

d. Domain Maleware Check
Domain maleware check Aplikasi PeduliLindungi tidak menunjukkan terdeteksinya domain-domain maleware yang berbahaya, domain-domain aplikasi PeduliLindungi berstatus “ok” yang berarti domain aplikasi tersebut tidak terindikasi maleware berrbahaya.

e. Security Secore
Security secore aplikasi SatuSehat Mobile menggunakan Mobile Security Framework (MobSF) sebesar 61 (low risk) yang berarti bahwa aplikasi PeduliLindungi tidak menunjukkan tanda-tanda masalah keamanan atau privasi yang signifikan atau relatif aman.

Aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi merupakan aplikasi front end yang terhubung dengan server melalui web service, sehingga aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi tidak memerlukan database lokal di perangkat smartphone pengguna, data yang diperlukan oleh aplikasi akan diambil langsung dari server melalui koneksi internet saat pengguna menjalankan aplikasi.

Alamat URL host yang ditampilkan oleh aplikasi SatuSehat Mobile pada file AndroidManifest.xml adalah “com.telkom.tracencare”, sedangkan URL host yang ditampilkan oleh aplikasi PeduliLindungi pada file

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

AndroidManifest.xml adalah pdl.id, dev.pdl.id dan stage.pd.id, jika diakses halaman-halaman dari kedua aplikasi tersebut menyediakan layanan API yang hanya merespons terhadap perintah yang dikirim kepadanya.

Aplikasi Pedulilindungi dan aplikasi SatuSehat mobile ketika dijalankan secara langsung dapat dilihat bahwa aplikasi PeduliLindungi tidak otomatis logout saat pengguna menutup layar aplikasi, pengguna harus melalukan logout secara mandiri atau manual agar ketika aplikasi pedulilindungi dibuka tidak langsung masuk pada tampilan beranda. Sedangkan pada aplikasi SatuSehat Mobile akan terkunci kembali secara otomatis setelah 15 detik pengguna tidak aktif yang berarti berarti jika pengguna tidak melakukan aktivitas apa pun pada aplikasi selama 15 detik aplikasi akan secara otomatis mengunci untuk menjaga keamanan data pengguna, pengguna harus memasukkan PIN atau sandi jika ingin mengakses kembali pada aplikasi SatuSehat Mobile. Hal tersebut dapat mengantisipasi keamana data pengguna yang hanya dapat diakses oleh pengguna yang memiliki kewenangan.

3.3 Rekomendasi

a. Dangerous Permission

Aplikasi SatuSehat Mobile terdapat 10 dangerous permission, berikut rekomendasi untuk dangerous permission pada aplikasi SatuSehat Mobile yang dapat dilihat pada Tabel 2.

Tabel 2. Rekomendasi Untuk dangerous permission

NO	*DANGEROUS PERMISSION*	KETERANGAN	REKOMENDASI
1	*android.permission.ACCESS_BACKGROUND_LOCATION*	*Dangerous*	Mengizinkan akses lokasi dilatar belakang dapat memungkinkan pelacakan yang tidak diinginkan, sehingga pengguna dapat dipantau tanpa sepengetahuannya, hal tersebut juga meningkatkan risiko pelanggaran privasi jika data lokasi jatuh ke pihat yang tidak bertanggungjawab. Peneliti menyarankan untuk membatasi penggunaan izin ini hanya jika sangat diperlukan, memastikan aplikasi memberikan notifikasi yang jelas ketika lokasi diakses dilatar belakang sehingga pengguna dapat memutuskan apakah menginginkan izin ini tetap aktif.
2	*android.permission.ACCESS_COARSE_LOCATION*	*Dangerous*	Perizinan ini memberikan akses ke perkiraan lokasi pengguna yang dapat digunakan untuk melacak pergerakan pengguna. Jika disalah gunakan perizinan tersebut dapat mengarah pada pelanggaran privasi. Peneliti menyarakan menggunaan izin ini hanya untuk fitur yang memerlukan perkiraan lokasi, seperti pencarian lokasi terdekat. Informasikan pengguna tentang penggunaan data lokasi dan memberikan opsi untuk menonaktifkan fitur ini jika tidak diperlukan.
3	*android.permission.ACCESS_FINE_LOCATION*	*Dangerous*	Perizinan ini Memberikan akses ke lokasi yang lebih presisi yang dapat digunakan untuk melacak pergerakan pengguna secara detail. Potensi pelanggaran privasi lebih besar dibandingkan dengan *ACCESS_COARSE_LOCATION* jika disalahgunakan. Peneliti menyarankan untuk memastikan izin ini hanya digunakan untuk fitur yang benar-benar membutuhkannya. Pengguna harus mengetahui dengan jelas terkait bagaimana data lokasi pengguna akan digunakan dan disimpan.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

NO	*DANGEROUS PERMISSION*	KETERANGAN	REKOMENDASI
4	*android.permission.CAMERA*	*Dangerous*	Mengizinkan akses kamera dapat disalahgunakan untuk mengambil gambar atau merekam video tanpa sepengetahuan pengguna yang dapat menjadi pelanggaran serius terhadap privasi. Peneliti menyarankan hanya minta izin atau mengizinkan akses kamera saat diperlukan untuk fitur spesifik, seperti mengambil foto atau video. memastikan pengguna mengetahui kapan kamera diaktifkan, seperti dengan menampilkan pratinjau bahwa kamera sedang digunakan oleh aplikasi.
5	*android.permission.POST_NOTIFICATIONS*	*Dangerous*	Izin ini memungkinkan aplikasi untuk menampilkan notifikasi kepada pengguna aplikasi. Jika disalahgunakan aplikasi dapat mengirim notifikasi yang berlebihan atau tidak diinginkan kepada pengguna. Peneliti menyarankan membatasi notifikasi hanya untuk informasi yang penting dan relevan, memberikan pengguna kontrol atas jenis notifikasi yang ingin diterima serta memastikan tidak mengirim spam atau informasi yang tidak relevan.
6	*android.permission.READ_EXTERNAL_STORAGE*	*Dangerous*	Akses ke penyimpanan eksternal dapat memungkinkan pihak yang tidak bertanggungjawab mengakses data pribadi yang disimpan pengguna pada perangkat android, yang dapat berujung pada kebocoran data dan informasi. Peneliti menyarankan membatasi akses hanya pada file atau direktori yang diperlukan untuk menjalankan aplikasi.
7	*android.permission.READ_MEDIA_AUDIO*	*Dangerous*	Memberikan perizinan ini berarti aplikasi dapat membaca file audio diperangkat pengguna. Jika digunakan oleh pihak yang tidak bertanggungjawab aplikasi dapat mengakses atau membagikan file audio pribadi tanpa sepengetahuan pengguna. Peneliti menyarankan untuk membatasi akses hanya file audio yang benar-benar diperlukan oleh fungsi aplikasi. menginformasikan kepada pengguna tentang file yang diakses serta memberikan kontrol kepada pengguna untuk membatasi akses aplikasi.
8	*android.permission.READ_MEDIA_IMAGES*	*Dangerous*	Aplikasi dapat membaca gambar yang tersimpan diperangkat pengguna sehingga berisiko mengekspos foto pribadi atau sensitif yang bisa disalahgunakan jika data pengguna tersebut diakses atau dibagikan tanpa izin. Peneliti menyarankan menggunakan izin ini hanya jika diperlukan untuk fitur spesifik seperti galeri foto. Sama seperti dengan *READ_MEDIA_AUDIO* peneliti menyarankan untuk membatasi akses hanya file audio yang benar-benar diperlukan oleh fungsi aplikasi.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

NO	*DANGEROUS PERMISSION*	KETERANGAN	REKOMENDASI
			menginformasikan kepada pengguna tentang file yang diakses serta memberikan kontrol kepada pengguna untuk membatasi akses aplikasi
9	*android.permission.READ_MEDIA_VIDEO*	*Dangerous*	Perizinan ini memungkinkan aplikasi membaca file video di perangkat pengguna. Jika disalahgunakan dapat menyebabkan kebocoran atau penyalahgunaan konten video pribadi pengguna. Peneliti menyarankan hanya menggunakan izin ini untuk fitur yang membutuhkan akses ke video, seperti pemutaran video dari penyimpanan local, memastikanpengguna memiliki kontrol untuk membatasi akses jika diperlukan.
10	*android.permission.WRITE_EXTERNAL_STORAGE*	*Dangerous*	Perizinan ini memberikan aplikasi kemampuan untuk menulis ke penyimpanan eksternal pengguna, hal tersebut dapat berisiko jika aplikasi menulis atau menghapus data penting tanpa persetujuan pengguna. Peneliti menyarankan menggunakan izin ini dengan sangat hati-hati hanya untuk menyimpan data yang diperlukan oleh aplikasi. Menanyakan persetujuan pengguna sebelum menulis atau menghapus file, dan memberikan opsi untuk menyimpan data ke penyimpanan lokasi yang aman dan terpisah.

Memberikan izin akses yang tidak perlu yang diminta oleh aplikasi dapat secara signifikan meningkatkan risiko serangan malware, karena berpotensi untuk aplikasi jahat mengeksploitasi izin tersebut untuk melakukan tindakan yang tidak sah[10]. Jika pengguna merasa bahwa izin tersebut tidak diperlukan untuk fungsionalitas aplikasi, disarankan untuk menonaktifkannya. Hal tersebut bertujuan untuk Menjaga keamanan serta mengurangi risiko penyalahgunaan data pada penyimpanan dan data pribadi pengguna.

b. Weak Crypto

Aplikasi SatuSehat Mobile terdapat 4 weak crypto yang terdiri dari 1 high severity dan 3 warning security, berikut ini rekomendasi bagian weak crypto pada aplikasi Satu Sehat Mobile yang dapat dilihat pada Tabel 3.

Tabel 3. Rekomendasi Bagian Weak Crypto Pada Aplikasi Satu Sehat Mobile

NO	*WEAK CRYPTO*	KETERANGAN	REKOMENDASI
1	Aplikasi ini menggunakan mode enkripsi *CBC dengan padding PKCS5/PKCS7*. Konfigurasi ini rentan terhadap serangan *padding oracle.*	*High Severity* *OWASP Top 10: M5: Insufficient Cryptography*	Mode enkripsi *AES* dengan *CBC* dan *padding PKCS5/PKCS7* rentan terhadap serangan *oracle padding*, pengembang sebaiknya mempertimbangkan untuk menggunakan mode enkripsi yang lebih aman seperti *AES-GCM (Galois/Counter Mode)* atau *AES-CCM (Counter with CBC-MAC)* yang menyediakan enkripsi dan integritas data.
2	Aplikasi ini menggunakan *Random Number Generator*.	*Warning Security*	Penggunaan generator angka acak yang tidak aman dapat menyebabkan kelemahan dalam proses pembangkitan kunci enkripsi dan token otentikasi, baiknya pengembang menggunakan

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

NO	*WEAK CRYPTO*	KETERANGAN	REKOMENDASI
		WASP Top 10: M5: Insufficient Cryptography.	generator angka acak yang aman (SecureRandom) berfungsi untuk menginisialisasi kunci kriptografis yang diciptakan oleh *KeyGenerator*.
	SHA-1 dan MD5 adalah *hash* lemah yang diketahui memiliki tabrakan *hash.*	*Warning Security* *WASP Top 10: M5: Insufficient Cryptography.*	SHA-1 dan MD5 diketahui memiliki kelemahan yang memungkinkan terjadinya tabrakan *hash* dan rentan terhadap serangan *brute-force*, baiknya menggunakan algoritma *hash* yang lebih kuat seperti SHA-3. Hasil penelitian menunjukkan bahwa penggunaan SHA-1 untuk sertifikat atau otentikasi dalam *handshake* TLS, SSH, atau IKE berisiko, karena telah terbukti rentan terhadap serangan *collision* dan dapat disalahgunakan oleh penyerang[11]. SHA-1 dapat digantikan dengan SHA-3 yang memiliki ketahanan lebih baik terhadap serangan *brute-force* karena waktu yang diperlukan untuk memperoleh *plaintext* dengan panjang 8, 9, dan 10 karakter dari *hash* SHA-3 lebih lama[12]. MD5 dapat dikombinasikan dengan algoritma kriptografi lainnya, seperti *vigenere cipher*. Kombinasi algoritma MD5 dan *vigenere cipher* dapat memberikan keamanan yang lebih baik dibandingkan hanya menggunakan MD5, karena proses enkripsi dilakukan dua kali[13]. *Vigenere cipher* adalah metode enkripsi yang menggunakan beberapa pergeseran yang diwakili oleh satu kata kunci.

4. KESIMPULAN

Analisis keamanan pada aplikasi SatuSehat Mobile dan aplikasi PeduliLindungi dapat dilakukan dengan pendekatan analisis statis dan analisis dinamis menggunakan tools MobSF dan Intezer dengan parameter dangerous permission, weak crypto, root detection, domain maleware check. Aplikasi SatuSehat Mobile dan PeduliLindungi menunjukkan adanya 4 weak crypto, yang terdiri dari 1 high severity dan 3 warning severity. Aplikasi SatuSehat Mobile memiliki 10 dangerous permission, sedangkan aplikasi PeduliLindungi memiliki 9 dangerous permission. Domain maleware check dan root detection dari kedua aplikasi tersebut berstatus good. Aplikasi SatuSehat Mobile dan PeduliLindungi merupakan aplikasi front end yang berkomunikasi dengan server melalui web service, kedua aplikasi tersebut tidak memerlukan database lokal di perangkat smartphone pengguna. Data yang diperlukan oleh aplikasi diambil langsung dari server melalui koneksi internet saat aplikasi dijalankan. URL host yang digunakan oleh aplikasi SatuSehat Mobile dalam file AndroidManifest.xml adalah com.telkom. tracencare, sedangkan aplikasi Peduli Lindungi menggunakan URL host pdl.id, dev.pdl.id, dan stage.pdl.id. Jika halaman-halaman dari kedua aplikasi tersebut diakses menyediakan layanan API yang hanya merespons perintah yang dikirim kepada aplikasi. Aplikasi SatuSehat Mobile yang terinstal didalam android/data/com.telkom.tracencare pada smartphone menujukkan tidak terdapat ataupun tersimpan file database dari aplikasi SatuSehat Mobile, kecuali ketika pengguna mendownload file sertifikat COVID-19 maka akan tersimpan pada smartphone dalam bentuk pdf pada folder download. Aplikasi SatuSehat Mobile telah menerapkan penggunaan PIN untuk meningkatkan keamanan dan privasi data pengguna yang hanya dapat diakses oleh penguna yang berwenang, mengurangi resiko akses tidak sak teruama jika perangkat pengguna hilang atau dicuri.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] S. R. Andani, "Analysis of Information Security in Data Leaks in The PeduliLindungi Application," *Int. J. Informatics Comput. Sci.*, vol. 5, no. 3, pp. 246–249, 2021, doi: 10.30865/ijics.v5i3.3406.

[2] "PeduliLindungi Resmi Berubah Menjadi SATUSEHAT," *https://promkes.kemkes.go.id/*, 2023. https://promkes.kemkes.go.id/pedulilindungi-resmi-berubah-menjadi-satusehat#:~:text=Tepat pada tanggal 1 Maret,aplikasi kesehatan masyarakat SATUSEHAT Mobile. (accessed Mar. 05, 2023).

[3] A. N. Dzulfaroh, "Saat Nomor KTP (NIK) Jokiwi Bocor," 2021. https://www.kompas.com/tren/read/2021/09/04/170500165/saat-nomor-ktp-nik-jokowi-bocor-?page=all (accessed Jan. 15, 2023).

[4] J. Nadhifah, "UPT Perpustakaan Perpustakaan Universitas Universitas Jember Jember," *Asuhan Keperawatan Pada AN.J Dan AN.Z Bronkopneumonia Dengan Masal. Keperawatan Ketidakefektifan Bersihan Jalan Nafas Di Ruang Bougenv. RSUD dr Haryoto LumajangTahun 2018*, pp. 1–71, 2018.

[5] V. Sargaiyan, M. Sapat, R. S. Yadav, S. Bhatele, S. S. Parihar, and A. H. Lanje, "Digital Forensics," *Int. J. Oral Care Res.*, vol. 5, no. 4, pp. 335–337, 2017, doi: 10.5005/jp-journals-10051-0127.

[6] H. Wijayanto, D. Daryono, and S. Nasiroh, "Analisis Forensik Pada Aplikasi Peduli Lindungi Terhadap Kebocoran Data Pribadi," *J. Teknol. Inf. dan Komun.*, vol. 9, no. 2, p. 11, Nov. 2021, doi: 10.30646/tikomsin.v9i2.572.

[7] A. Eka Dewi Melania, I. Gunawan, J. Teknik Elektro Jurusan Informatika ab Sekolah Tinggi Teknologi Ronggolawe, and P. Korenspondensi, "Analisis Keamanan Aplikasi Android Non Playstore Dengan Metode Digital Forensik Pendekatan Statis Dan Dinamis," vol. 15, no. 2, pp. 29–34, 2021, [Online]. Available: https://m.apkpure.com.

[8] V. Baryamureeba, F. Tushabe, K. Penelitian, and F. Digital, "Proses Investigasi Digital yang Disempurnakan Model," 2004.

[9] H. Dalziel and A. Abraham, *Automated Security Analysis of Android and iOS Applications with Mobile Security Framework*. Waltham: Syngress Publication, 2015.

[10] G. Koala, D. Bassolé, A. Zerbo/Sabané, T. F. Bissyandé, and O. Sié, "Analysis of the impact of permissions on the vulnerability of mobile applications," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 311 LNICST, no. February, pp. 3–14, 2020, doi: 10.1007/978-3-030-41593-8_1.

[11] G. Leurent and T. Peyrin, "From collisions to chosen-prefix collisions application to full SHA-1," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11478 LNCS, pp. 527–555, 2019, doi: 10.1007/978-3-030-17659-4_18.

[12] F. Kurniawan, A. Kusyanti, and H. Nurwarsito, "Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 803–812, 2017, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/247

[13] H. Sibyan, "Implementasi Enkripsi Basis Data Dengan Algoritma Dengan Algoritma MD5 (Message Digest Algorithm 5) dan Vigenere Cipher," *Ppkm I*, vol. 5, pp. 114–121, 2017.

Submitted: **07/09/2024**; Accepted: **26/09/2024**; Published: **08/03/2025**