TUGAS AKHIR

ANALISIS KEAMANAN APLIKASI SMART PROVINCE MENGGUNAKAN FRAMEWORK MASVS-PRIVACY



Disusun Oleh :

Malvin Sandi 221711854

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2026

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

ANALISIS KEAMANAN APLIKASI SMART PROVINCE MENGGUNAKAN FRAMEWORK MASVS-PRIVACY

yang disusun

oleh Malvin

Sandi 221711854

dinyatakan telah memenuhi syarat pada tanggal 23 Juli 2026

		Keterangan Dosen
Pembimbing 1	: Emanuel Ristian Handoyo, S.T., M.Eng.	Telah Menyetujui
Dosen Pembimbing 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng., Ph.D.	
Tim Penguji		
Penguji 1	: Emanuel Ristian Handoyo, S.T., M.Eng.	Telah Menyetujui
Penguji 2	: Rangga Perwiratama S.T., M.Kom.	Telah Menyetujui
Penguji 3	: Paulus Mudjihartono, S.T., M.T., Ph.D.	Telah Menyetujui

Yogyakarta, 23 Juli 2026 Universitas Atma Jaya

Yogyakarta Teknologi Industri

Dekan ttd.

Prof. Dr. Ir. Parama Kartika Dewa SP., S.T., M.T., IPU,

ASEAN En

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Tugas Akhir yang berjudul **"ANALISIS KEAMANAN APLIKASI SMART PROVINCE MENGGUNAKAN FRAMEWORK MASVS-PRIVACY"** dengan baik.

Tugas Akhir ini disusun sebagai salah satu syarat dalam memenuhi tahapan penyusunan Tugas Akhir pada Program Studi Sistem Informasi. Penyusunan ini bertujuan untuk merancang penelitian yang berfokus pada analisis keamanan aplikasi Android guna mengidentifikasi potensi risiko keamanan dengan memanfaatkan *Mobile* Security Framework (MobSF) yang dijalankan pada lingkungan Docker dengan standar OWASP MASVS PRIVACY.

Penulis menyadari bahwa penyusunan ini tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa atas rahmat dan penyertaan-Nya.
2. Bapak/Ibu dosen pembimbing yang telah memberikan arahan, bimbingan, serta masukan selama proses penyusunan ini.
3. Bapak/Ibu dosen Program Studi Sistem Informasi yang telah memberikan ilmu dan pengetahuan selama masa perkuliahan.

Penulis menyadari bahwa Tugas Akhir ini masih memiliki keterbatasan dan kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi penyempurnaan ini. Semoga ini dapat memberikan manfaat bagi penulis maupun pihak lain yang membacanya.

Yogyakarta, 11 Februari 2026

Mahasiswa Sistem Informasi



Malvin Sandi

ABSTRAK

Meningkatnya penggunaan Android dan aplikasi Android di berbagai sektor, termasuk layanan pemerintah seperti aplikasi Jogja Istimewa (JOGIS), menimbulkan risiko terhadap keamanan sistem dan perlindungan data pengguna. Sebagai salah satu platform yang banyak digunakan dalam layanan digital, aplikasi Android berpotensi menjadi target berbagai ancaman keamanan seperti kebocoran data, penyalahgunaan izin akses, serta eksploitasi kerentanan pada aplikasi. Oleh karena itu, diperlukan analisis keamanan untuk mendeteksi potensi kerentanan sebelum aplikasi digunakan atau didistribusikan secara luas. Sebagai solusi, penelitian ini menganalisis keamanan aplikasi JOGIS menggunakan Mobile Security Framework (MobSF) yang dijalankan dalam lingkungan terisolasi berbasis Docker dengan mengacu pada standar OWASP MASVS-Privacy. Metodologi penelitian meliputi instalasi dan konfigurasi MobSF pada Docker, proses pemindaian aplikasi menggunakan metode analisis statis terhadap berkas APK, evaluasi hasil analisis berdasarkan parameter permission, konfigurasi keamanan, potensi kerentanan, dan risiko kebocoran data, yang kemudian diverifikasi melalui pemeriksaan manual terhadap hasil dekompilasi kode.

Hasil analisis menunjukkan bahwa aplikasi JOGIS memperoleh Security Score sebesar 51 dari 100 dengan risk rating grade B, yang menempatkan aplikasi pada kategori keamanan menengah (medium risk). Dari seluruh temuan yang teridentifikasi, terdapat 2 temuan berkategori high, 19 temuan berkategori medium, 2 temuan berkategori info, 2 indikator secure, 1 hotspot potensial, serta 2 user/device tracker yang terdeteksi pada aplikasi. Temuan tersebut antara lain berupa penggunaan weak cryptography, raw SQL query, penyimpanan pada external storage, dan penggunaan temporary file, sehingga dapat disimpulkan bahwa aplikasi JOGIS belum berada pada kondisi kritis namun tetap memerlukan perbaikan untuk mengurangi potensi eksploitasi dan risiko kebocoran data pengguna.

Kata kunci: *keamanan aplikasi; Android; MobSF; Docker; Analisis Statik APK*

ABSTRACT

The increasing use of Android devices and Android applications across various sectors, including government services such as the Jogja Istimewa (JOGIS) application, has raised concerns regarding system security and user data protection. As one of the most widely used platforms for digital services, Android applications are potential targets of security threats such as data breaches, misuse of access permissions, and exploitation of application vulnerabilities. Therefore, security analysis is required to identify potential vulnerabilities before an application is deployed or widely distributed.

As a solution, this study analyzes the security of the Jogja Istimewa (JOGIS) application using the Mobile Security Framework (MobSF), deployed in an isolated Docker-based environment and conducted with reference to the OWASP MASVS-Privacy standard. The methodology includes the installation and configuration of MobSF on Docker, a static analysis scan of the APK file, and an evaluation based on parameters such as permissions, security configurations, potential vulnerabilities, and data leakage risks, which is further verified through manual inspection of the decompiled code.

The analysis results show that the JOGIS application obtained a Security Score of 51 out of 100 with a risk rating of grade B, placing it in the medium-risk security category. Among all the findings identified, there were 2 high-severity findings, 19 medium-severity findings, 2 info-level findings, 2 secure indicators, 1 potential hotspot, and 2 user/device trackers detected in the application. These findings include the use of weak cryptography, raw SQL queries, external storage usage, and temporary files, indicating that the JOGIS application is not in a critical condition but still requires improvement to reduce potential exploitation and the risk of user data leakage.

Keywords: *application security; Android; MobSF; Docker; APK static analysis*

DAFTAR ISI

HALAMAN PENGESAHAN..... Error! Bookmark not defined.

KATA PENGANTAR i

ABSTRAK.....ii

ABSTRACT iii

DAFTAR ISI iv

DAFTAR GAMBAR.....vii

DAFTAR TABEL.....viii

BAB I PENDAHULUAN.....1

1.1 Latar Belakang..... 1

1.2 Rumusan Masalah..... 3

1.3 Pertanyaan Penelitian..... 4

1.4 Batasan Masalah..... 4

1.5 Tujuan Penelitian..... 5

1.6 Manfaat Penelitian..... 5

1.6.1 Manfaat Akademis..... 5

1.6.2 Manfaat Praktis..... 6

1.7 Bagan Keterikatan..... 6

BAB 2.....7

TINJAUAN PUSTAKA.....7

2.1 Penelitian Terdahulu..... 7

2.2 Gap Penelitian 11

2.3 Dasar Teori..... 12

2.3.1 Keamanan Aplikasi *Mobile* 12

2.3.2 Android Application Package (APK) 13
2.3.3 Analisis Statis 14
2.3.4 *Mobile* Security Framework (MobSF) 15
2.3.5 Docker 15
2.3.6 OWASP *Mobile* Top 10 16
2.3.7 OWASP MASVS Privacy 17
2.3.8 Android Permission dan Klasifikasinya 18
2.3.9 AndroidManifest.xml 18
2.3.10 Kerentanan (Vulnerability) pada Aplikasi Android 19
2.4 Kerangka Pemikiran 19
BAB 3 21
METODOLOGI PENELITIAN 21
3.1 Tahapan Penelitian 21
3.2 Metode pengumpulan data 23
3.3 Desain Penelitian 24
3.4 Metode Analisis Statis 26
BAB 4 28
HASIL DAN PEMBAHASAN 28
4.1 Deskripsi Objek Penelitian 28
4.2 Hasil Analisis Statis 30
4.2.1 Hasil Analisis Izin Aplikasi (*Permission*) 32
4.2.2 Analisis Manifestasi (*Analisis Manifest*) 37
4.2.3 Analisis Kode Sumber (*Source Code*) dan Keamanan Perilaku (*Behaviour Analysis*) 40
4.2.4 Identifikasi Kerentanan 42

4.3 Analisis Tingkat Risiko 44
4.4 Analisis Berdasarkan Owasp Mobile Top 10 45
4.5 Analisis Permission Berdasarkan MASVS-Privacy 46
4.6 Rekomendasi Perbaikan 50
4.7 Pembahasan 51
BAB 5 53
KESIMPULAN DAN SARAN 53
5.1 Kesimpulan 53
5.2 Saran 54
5.3 Keterbatasan Penelitian 55
5.4 Saran Untuk Penelitian Selanjutnya 55
DAFTAR PUSTAKA 56
LAMPIRAN 59

DAFTAR GAMBAR

Gambar 1.1.Bagan Keterikatan.....17
Gambar 2.1.Komponen APK File.....25
Gambar 3.1.Tahapan Penelitian.....31
Gambar 4.1.Aplikasi Jogja Istimewa.....40
Gambar 4.2.Hasil Analisis Statis..... 40
Gambar 4.3.Informasi Aplikasi..........41
Gambar 4.3.Hasil Analisis Izin(Permission).....43
Gambar 4.4.Analisis Izin..........42
Gambar 4.5.Hasil Analisis Manifestasi.......47
Gambar 4.6.Allow Backup False.....49
Gambar 4.7.Hasil Analisis Kode Sumber.....50
Gambar 4.8.Hasil Analisis Behavior.....51

DAFTAR TABEL

Tabel 2.1.Penelitian Terdahulu.....19
Tabel 2.2.Gap Penelitian..........22
Tabel 4.1.Hasil Analisis Izin Aplikasi.....43
Tabel 4.2.Hasil Analisis AndroidManifest.....48
Tabel 4.3.Identifikasi Kerentanan..... 53
Tabel 4.4.Analisis JOGIS Menggunakan OWASP MASVS-PRIVACY.....57
Tabel 4.5.Pemetaan Temuan Terhadap OWASP MASVS-PRIVACY.....58
Tabel 4.6.Rekomedasi Perbaikan..........59