BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital seluler saat ini telah memposisikan sistem operasi Android sebagai platform yang paling mendominasi pasar global, dengan pangsa pasar mencapai lebih dari 70% dan jumlah pengguna smartphone yang menembus angka 4,3 miliar pada tahun 2023 [1]. Meski demikian, popularitas yang sangat besar dan sifat platform yang terbuka (*open-source*) menjadikan Android sebagai target utama serangan siber global [2]. Ancaman ini tercermin nyata dalam laporan keamanan internasional yang mencatat adanya lebih dari 5,7 juta upaya serangan malware seluler ,walaupun akhirnya berhasil diblokir hanya dalam kurun waktu 3 bulan sekali [1]. Fenomena ini diperburuk oleh perilaku pengguna yang sering memasang aplikasi dari sumber pihak ketiga yang belum terverifikasi dengan asal usul yang tidak jelas , sehingga membuka celah besar bagi teknik *repackaging* atau penyisipan kode berbahaya ke dalam aplikasi sah untuk mencuri informasi sensitif[3].

Di Indonesia, penetrasi internet yang telah mencapai lebih dari 204 juta pengguna telah mendorong transformasi layanan publik ke arah *e-government* melalui aplikasi mobile guna meningkatkan efisiensi [4]. Namun, akselerasi transformasi ini sering kali tidak diikuti dengan audit keamanan yang memadai. Berdasarkan laporan ID-SIRTII, terdapat jutaan aktivitas malware yang menargetkan infrastruktur digital nasional, yang membuktikan bahwa aplikasi layanan publik memiliki profil risiko eksploitasi data yang sangat tinggi apabila tidak melalui proses pengujian yang ketat [5].

Dikarenakan kondisi keamanan di lapangan menunjukkan bahwa banyak aplikasi Android masih beroperasi tanpa perlindungan dasar seperti enkripsi lokal atau teknik pengaburan kode (*obfuscation*) [6]. Penelitian pada

aplikasi transportasi online populer bahkan menemukan kerentanan kritis berupa penggunaan izin akses berlebihan (*dangerous permissions*) dan algoritma kriptografi yang lemah, yang secara teknis memudahkan terjadinya interupsi data oleh pihak luar[7]. Permasalahan semakin kompleks karena pengujian keamanan sering kali mengabaikan interaksi jaringan dengan server, di mana kerentanan fatal seperti *Insecure Direct Object Reference* (IDOR) pada sisi *backend* sering kali luput dari deteksi standar [6]. OWASP menyebutkan bahwa proses security testing secara berkala sangat diperlukan untuk mendeteksi vulnerability pada sistem sebelum dimanfaatkan oleh pihak tidak bertanggung jawab, terutama pada aplikasi yang menangani data penting pengguna[8]

Aplikasi Jogja Istimewa (JOGIS) merupakan platform integrasi layanan publik resmi bagi masyarakat Yogyakarta yang menyediakan berbagai fitur strategis [9] Sebagai aplikasi *e-government*, JOGIS meminta izin akses ke berbagai sumber daya perangkat yang sensitif, seperti lokasi GPS secara *real-time* dan penyimpanan internal [9]. Aplikasi Jogja Istimewa (JOGIS) dikembangkan sebagai salah satu aplikasi layanan publik berbasis e-government di Daerah Istimewa Yogyakarta. Berdasar Google Playstore sendiri aplikasi Jogja Istimewa sudah di unduh lebih dari 100.000+ download ditambah dengan adanya pengelolaan data pengguna pada aplikasi tersebut, aspek keamanan menjadi hal yang perlu diperhatikan untuk menjaga kualitas layanan dan perlindungan data pengguna.[10]

Hingga saat ini, belum tersedia laporan audit teknis yang dipublikasikan secara terbuka mengenai profil risiko keamanan aplikasi JOGIS. Pengujian keamanan aplikasi Android dapat dilakukan menggunakan beberapa pendekatan, yaitu analisis statis ,analisis dinamis maupun kombinasi keduanya (*hybrid analysis*). Analisis statis dilakukan dengan menganalisis struktur aplikasi tanpa menjalankannya, sedangkan analisis dinamis dilakukan dengan mengamati perilaku aplikasi saat dijalankan. Namun, pada penelitian ini dipilih metode analisis statis menggunakan MobSF karena mampu mengidentifikasi

struktur aplikasi, konfigurasi *AndroidManifest.xml*, penggunaan *permission*, serta potensi kerentanan secara efisien melalui analisis berkas APK.

[11]. Analisis statis dipilih karena mampu mengidentifikasi struktur aplikasi, konfigurasi keamanan, source code, dan potensi kerentanan tanpa menjalankan aplikasi, sehingga sesuai dengan tujuan penelitian ini [12]. Oleh karena itu, pengujian keamanan melalui verifikasi berkas APK menjadi langkah krusial untuk mendeteksi potensi aplikasi berbahaya sebelum digunakan secara luas oleh masyarakat [13].

1.2 Rumusan Masalah

Pemanfaatan aplikasi mobile berbasis Android dalam layanan *e-government* memberikan kemudahan bagi masyarakat dalam mengakses informasi dan layanan publik secara digital. Namun, penggunaan aplikasi tersebut juga memiliki potensi risiko keamanan yang berkaitan dengan pengelolaan data, penggunaan *permission*, serta interaksi aplikasi dengan sistem operasi Android. Aplikasi JOGIS sebagai salah satu aplikasi layanan publik memanfaatkan beberapa komponen sistem pada perangkat Android, seperti akses internet, penyimpanan data, dan layanan lokasi, sehingga memerlukan pengaturan keamanan yang tepat agar tidak menimbulkan potensi kerentanan. Permasalahan dalam penelitian ini adalah belum adanya analisis keamanan secara sistematis terhadap struktur aplikasi dan penggunaan permission pada aplikasi JOGIS. Kondisi tersebut dapat menimbulkan risiko seperti penyalahgunaan akses perangkat, kebocoran data pengguna, maupun eksploitasi sistem oleh pihak yang tidak bertanggung jawab, sehingga diperlukan analisis keamanan untuk mengetahui potensi kerentanan yang terdapat pada aplikasi JOGIS.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan sebelumnya, maka penelitian ini memiliki beberapa pertanyaan penelitian yang akan dijawab melalui proses analisis pada aplikasi yang diteliti. Pertanyaan penelitian tersebut disusun untuk mengidentifikasi potensi kerentanan keamanan yang mungkin terdapat pada aplikasi serta memahami karakteristik keamanan aplikasi Android yang digunakan dalam layanan *e-government*.

Adapun pertanyaan penelitian dalam penelitian ini adalah sebagai berikut:

1. Bagaimana karakteristik struktur aplikasi JOGIS berbasis Android ditinjau dari aspek keamanan aplikasi?
2. Apa saja potensi kerentanan keamanan yang terdapat pada aplikasi JOGIS berdasarkan hasil analisis aplikasi?
3. Bagaimana tingkat keamanan aplikasi JOGIS berdasarkan hasil analisis menggunakan Mobile Security Framework (MobSF)?

1.4 Batasan Masalah

Agar penelitian lebih terfokus, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian difokuskan pada analisis keamanan aplikasi Jogja Istimewa (JOGIS) dalam bentuk file APK menggunakan *Mobile Security Framework (MobSF)* berbasis Docker.
2. Analisis yang dilakukan terbatas pada metode Analisis Statis serta hasil laporan keamanan yang dihasilkan oleh MobSF.

3. Penelitian tidak membahas pengembangan maupun perbaikan kode sumber aplikasi, dan evaluasi keamanan dilakukan berdasarkan temuan teknis dari hasil analisis MobSF.

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisis tingkat keamanan aplikasi Jogja Istimewa (JOGIS) sebagai aplikasi layanan publik berbasis Android menggunakan Mobile Security Framework (MobSF). Analisis dilakukan untuk mengidentifikasi potensi kerentanan keamanan, konfigurasi tidak aman, serta tingkat risiko keamanan aplikasi berdasarkan hasil Analisis Statis yang dilakukan terhadap file APK aplikasi. Selain itu, penelitian ini juga bertujuan untuk memberikan rekomendasi teknis yang dapat digunakan sebagai upaya peningkatan keamanan aplikasi layanan publik berbasis Android.

1.6 Manfaat Penelitian

Penelitian ini diharapkan memberikan kontribusi baik secara akademis maupun praktis dalam bidang keamanan aplikasi mobile . Dengan adanya analisis kemanan yang terstuktur , penelitian ini dapat menjadi referensi dalam proses evaluasi dan verifikasi aplikasi Android sebelum digunakan secara luas , sehingga dapat meminimalkan potensi risiko kebocoran data maupun ancaman keamanan sistem.

1.6.1 Manfaat Akademis

a. Menambah referensi ilmiah dalam bidang keamanan informasi , khususnya terkait analisis keamanan aplikasi Android.

b. Memberikan pemahaman mengenai proses analisis keamanan aplikasi Android dalam mengidentifikasi potensi kerentanan serta risiko keamanan pada sistem aplikasi mobile.

c. Menjadi bahan kajian dan pengembangan penelitian selanjutnya yang berkaitan dengan pengujian keamanan aplikasi mobile .

1.6.2 Manfaat Praktis

a. Memberikan gambaran teknis kepada pengembang aplikasi mengenai potensi risiko keamanan yang dapat muncul pada file APK.

b. Membantu institusi atau organisasi dalam menerapkan proses analisis keamanan aplikasi secara terisolasi dan sistematis sebelum aplikasi digunakan.

c. Mengurangi risiko kebocoran data dan penyalahgunaan sistem akibat aplikasi yang tidak melalui proses pengujian keamanan yang memadai.

1.7 Bagan Keterikatan



Gambar 1.1 Bagan Keterikatan

Bagan keterkaitan penelitian menampilkan hubungan antara latar belakang penelitian, rumusan masalah, pertanyaan penelitian, tujuan penelitian, dan manfaat penelitian. Latar belakang menjelaskan fenomena meningkatnya penggunaan aplikasi Android serta pentingnya keamanan aplikasi pada layanan *e-government*. Permasalahan tersebut kemudian dirumuskan dalam bentuk rumusan masalah yang menjadi dasar penyusunan pertanyaan penelitianyang selanjutnya akan digunakan untuk menentukan tujuan penelitian yang ingin dicapai. Hasil penelitian diharapkan dapat memberikan manfaat baik secara akademis maupun praktis dalam bidang keamanan aplikasi mobile .