BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi mobile yang pesat telah mengubah cara masyarakat berinteraksi dan melakukan berbagai aktivitas digital. Kemudahan yang ditawarkan oleh perangkat *smartphone* dan tablet mendorong pertumbuhan ekosistem aplikasi yang sangat masif, terutama pada platform Android melalui Google Play Store. Seiring dengan meningkatnya kebutuhan masyarakat terhadap layanan digital, banyak aplikasi yang dirilis untuk mempermudah aktivitas sehari-hari, termasuk dalam bidang kesehatan, pemerintahan, dan komunikasi.

Namun, di balik kemajuan tersebut, muncul tantangan baru dalam hal keamanan dan perlindungan data pengguna. Kasus peretasan yang menimpa aplikasi PeduliLindungi, yang kemudian berubah menjadi SatuSehat, menjadi contoh nyata bagaimana sistem keamanan digital masih rentan terhadap serangan siber. Insiden tersebut menyebabkan pengguna dialihkan ke laman judi daring dan menunjukkan lemahnya pengawasan serta pengelolaan keamanan ketika terjadi transisi pengelolaan aplikasi.

Fenomena seperti ini menggambarkan bahwa meskipun aplikasi digital menawarkan kemudahan dan efisiensi, risiko kebocoran data dan penyalahgunaan informasi pribadi tetap tinggi. Oleh karena itu, diperlukan penelitian dan analisis mendalam terhadap berbagai aplikasi di Play Store untuk mengidentifikasi izin berbahaya, potensi eksploitasi data, serta tingkat keamanan aplikasi secara menyeluruh agar dapat memberikan perlindungan yang lebih baik bagi pengguna di Indonesia.

Menanggapi isu peretasan laman PeduliLindungi yang dialihkan ke situs judi online, Kepala Biro Komunikasi dan Informasi Publik Kemenkes, Aji Muhawarman, menegaskan bahwa pihaknya tidak lagi bertanggung jawab atas keamanan sistem tersebut. Ia menjelaskan bahwa sejak transisi ke aplikasi SatuSehat pada Maret 2023, seluruh pengelolaan dan keamanan situs PeduliLindungi telah diserahkan sepenuhnya kepada pihak lain. [1]

Banyaknya aplikasi gratis di Google Play Store tidak selalu diiringi dengan jaminan keamanan yang memadai. Kurangnya kesadaran pengembang akan pentingnya aspek keamanan menjadi celah yang dimanfaatkan oleh pihak tidak bertanggung jawab. Kerentanan yang umum ditemukan meliputi:

1. Izin Akses (Permissions) Berlebihan: Aplikasi seringkali meminta izin akses yang tidak relevan dengan fungsionalitas utamanya, seperti meminta akses ke kontak atau lokasi padahal aplikasi tersebut hanya berfungsi sebagai kalkulator. Hal ini dapat menjadi pintu masuk bagi penyalahgunaan data pribadi.
2. Penggunaan Pustaka (Libraries) Pihak Ketiga yang Tidak Aman: Untuk mempercepat proses pengembangan, banyak pengembang menggunakan pustaka pihak ketiga. Jika pustaka ini memiliki kerentanan, maka seluruh aplikasi akan terdampak, membahayakan data pengguna.

Ancaman-ancaman tersebut menimbulkan kekhawatiran yang mendalam bagi privasi dan keamanan data pengguna. Oleh karena itu, diperlukan sebuah pendekatan yang sistematis untuk menganalisis dan mengidentifikasi potensi kerentanan keamanan pada aplikasi Android, khususnya yang tersedia secara gratis.

Data dari laporan Google menjadi alasan kuat mengapa peneliti memilih judul ini. Meskipun Google telah mencegah jutaan aplikasi jahat agar tidak rilis, angka 2,36 juta pelanggaran menunjukkan bahwa upaya penyisipan celah keamanan ke dalam Play Store masih sangat masif dilakukan oleh pihak-pihak tidak bertanggung jawab.[2]

Hal ini memicu pertanyaan penting: apakah aplikasi gratis yang saat ini sudah lolos dan digunakan sehari-hari terutama di kategori Game yang sangat

populer dan Productivity yang mengelola data pribadi benar-benar aman dari ancaman tersebut?

Kekhawatiran ini semakin nyata melihat data bahwa ada 1,3 juta aplikasi yang terdeteksi mencoba meminta akses data sensitif secara berlebihan. Oleh karena itu, peneliti merasa perlu melakukan pengujian mandiri menggunakan pendekatan statis untuk membongkar "jeroan" kode aplikasinya dan pendekatan dinamis untuk memantau kelakuannya saat dijalankan. Dengan kata lain, penelitian ini bertujuan untuk membuktikan apakah sistem keamanan Google sudah cukup kuat, atau justru masih ada aplikasi yang diam-diam "mengintip" data user meskipun kelihatannya bermanfaat dan gratis untuk diunduh.

Laporan dari Google dan data statistik kerentanan menjadi alasan utama peneliti memilih judul tersebut. Meskipun Google sudah bekerja keras menjaga keamanan dengan memblokir 2,36 juta aplikasi nakal dan 158.000 akun pengembang bermasalah, ancaman ternyata masih banyak yang lolos ke publik. Faktanya, ada sekitar 1,3 juta aplikasi yang masih terdeteksi mencoba mengintip data pribadi user secara berlebihan. Hal ini menunjukkan bahwa sistem keamanan otomatis saja belum cukup, sehingga diperlukan analisis lebih dalam terhadap aplikasi yang sudah telanjur beredar.

Kekhawatiran ini semakin terbukti jika melihat data Ternyata, kategori Game menempati urutan pertama sebagai kategori aplikasi yang paling banyak memiliki konfigurasi keamanan (Firebase) yang rentan, yaitu mencapai 24,71%. Angka ini jauh lebih tinggi dibandingkan kategori lain seperti pendidikan atau bisnis. Karena Game adalah jenis aplikasi yang paling sering diunduh secara gratis, risiko kebocoran data di sana sangatlah besar.[3]

1.2 Rumusan Masalah

Permasalahan penelitian ini adalah: Informasi apa saja yang bisa diperoleh menggunakan pendekatan statis dan dinamis?

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan sesuai dengan rumusan masalah yang telah dipaparkan sebelumnya, peneliti membuat batasan masalah. Batasan masalah yang ditetapkan dalam penelitian ini adalah sebagai berikut:

1 Penelitian dibatasi pada top 5 chart aplikasi Android gratisan kategori *Game* dan *Productivity* yang diunduh dari Play Store.

2 Peneliti menganalisis secara statis menggunakan MobSF secara dinamis menggunakan JADX-GUI.

3 Aplikasi berbayar dan sistem operasi lain (iOS) tidak termasuk dalam ruang lingkup penelitian ini.

1.4 Tujuan Penelitian

Untuk menganalisis potensi kerentanan keamanan data pada aplikasi gratis di Play Store dengan dua metode yaitu metode dari Imam Himawan, Kevin Septianzah, Irawan Setiadi untuk penggunaan *tools* MobSF nya dan menggunakan teori dari Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, dan David Wagner untuk penggunaan *tools* JADX-GUI.

1.5 Manfaat Penelitian

1. Memberikan informasi kepada pembaca mengenai risiko keamanan dari aplikasi gratis.
2. Memberikan gambaran yang jelas dan terukur mengenai status keamanan aplikasi gratis di Play Store.

1.6 Sistematika Penulisan

Berisi sistematika penulisan skripsi yang memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab. Peneliti harus dapat mendeskripsikan (menggambarkan) apa saja isi masing-masing Bab yang akan disusun. Jelaskan secara singkat isi dari bab I, bab II, bab III, bab IV, dan bab V.

BAB I PENDAHULUAN, berisi Latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi tinjauan pustaka, dasar-dasar teori yang

digunakan.

BAB III METODE PENELITIAN, bab ini berisikan gambaran umum tentang alur dari penelitian, prosedur, dan mekanisme metode analisis yang diterapkan pada penelitian.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang peneliti lakukan dalam mengembangkan aplikasi, testing hingga penerapan aplikasi di objek penelitian.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum .