BAB I
PENDAHULUAN

1.1 Latar Belakang

Hingga awal tahun 2025, dominasi sistem operasi *android* di pasar perangkat seluler global tetap tak tergoyahkan, dengan pangsa pasar mencapai 71.85% (StatCounter, 2025). Skala adopsi yang masif ini telah memacu inovasi aplikasi di sektor sektor krusial yang mengelola data sensitif, seperti perbankan, *e-commerce*, dan layanan kesehatan. Namun, ketergantungan yang mendalam ini juga membuka vektor serangan baru, menjadikan keamanan aplikasi dan privasi data pengguna sebagai tantangan utama yang harus dihadapi oleh para pengembang.

Salah satu celah keamanan paling fundamental pada *android* berasal dari praktik *rooting*. Meskipun memberikan keuntungan bagi pengguna untuk melakukan kustomisasi penuh, *rooting* secara esensial membongkar model keamanan sistem operasi. Laporan dari Zimperium (2024) mengonfirmasi bahwa perangkat yang telah di *root* memiliki kemungkinan sepuluh kali lebih besar untuk terinfeksi *malware*. Ancaman ini mencakup *rootkit* pada level *kernel* yang sulit dideteksi oleh mekanisme tradisional (Guri dkk., 2015). Kondisi ini menjadikan perangkat sebagai target utama pencurian data, karena aplikasi berbahaya dapat dengan mudah melewati batasan keamanan dan mengakses data pribadi aplikasi lain, sebuah risiko yang secara spesifik diidentifikasi dalam OWASP Mobile Top 10.

Di samping risiko pada level sistem, keamanan pada level antarmuka visual juga menjadi prioritas. A*ndroid* menyediakan mekanisme *flag secure* yang

direkomendasikan untuk mencegah pengambilan tangkapan layar (*screenshot*) atau perekaman layar pada konten sensitif. Namun, implementasinya masih sering diabaikan oleh pengembang. Ancaman ini bukanlah teoretis, laporan dari *Kaspersky* (2025) menyoroti peningkatan serangan *trojan* Perbankan yang secara aktif mengeksploitasi kelemahan ini. *Malware* tersebut secara diam-diam mengambil tangkapan layar saat pengguna memasukkan kredensial, membuktikan adanya risiko nyata ketika praktik keamanan dasar ini tidak diterapkan dengan disiplin.

Tantangan keamanan ini semakin rumit karena metode pertahanan yang ada saat ini terbukti tidak memadai. Banyak metode deteksi *root* yang ada dapat dielakkan dengan teknik yang relatif sederhana, seperti yang ditunjukkan oleh penelitian Soewito & Suwandaru (2022) mengenai *Java function hooking*. Kelemahan ini dieksploitasi secara luas oleh *framework modern* seperti *Magisk*, yang dirancang khusus untuk menyembunyikan status *root*, dan *frida*, yang memungkinkan manipulasi *runtime* untuk menonaktifkan fungsi deteksi. Di sisi lain, tidak ada solusi terpadu yang praktis bagi pengembang untuk mengatasi deteksi *root* yang canggih sekaligus memvalidasi *flag secure*.

Mengingat skala ancaman yang masif, kelemahan pada pertahanan yang ada, serta ketiadaan alat bantu yang efisien bagi pengembang, maka pengembangan sebuah pustaka terintegrasi menjadi sebuah kebutuhan yang sangat mendesak. Pustaka semacam ini dapat menyederhanakan implementasi langkah-langkah keamanan yang kompleks, sehingga meningkatkan perlindungan privasi dan integritas data pengguna secara signifikan. Oleh karena itu, penelitian ini bertujuan

merancang dan membangun sebuah pustaka keamanan *android* yang komprehensif, guna menyediakan lapisan pertahanan yang solid dan mudah diadopsi untuk meminimalkan risiko keamanan pada ekosistem *android*.

Berdasarkan pada konteks yang telah dijelaskan di atas, peneliti memutuskan untuk melakukan penelitian dengan judul: "*Library* Deteksi *Root* Dan *Flag Secure* Pada Perangkat *Android* Menggunakan Metode *Mobile D*".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang menguraikan adanya ancaman aktif, metode pertahanan yang dapat ditembus, dan ketiadaan alat bantu yang efisien, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan mengembangkan sebuah metode yang efektif dan akurat untuk mendeteksi status *root* pada perangkat *android* melalui sebuah *library*?
2. Bagaimana cara mengembangkan dan mengintegrasikan sebuah mekanisme di dalam *library* yang dapat secara efektif memvalidasi implementasi *flag secure* pada aktivitas aktivitas krusial aplikasi?
3. Bagaimana memastikan desain dan implementasi *library* selaras dengan prinsip-prinsip keamanan yang relevan dalam *OWASP Mobile Application Security Verification Standard* (MASVS) untuk menjamin kualitas dan keandalannya?

1.3 Tujuan

Sejalan dengan rumusan masalah yang telah disederhanakan, penelitian ini bertujuan untuk:

1. Merancang dan membangun sebuah *library* yang mampu mendeteksi status *root* pada perangkat *android* dengan tingkat efektivitas dan akurasi yang tinggi.
2. Mengembangkan sebuah modul fungsional yang mudah digunakan oleh pengembang untuk memvalidasi penerapan *flag secure*, guna memastikan konten visual sensitif pada aplikasi terlindungi dari tangkapan layar.
3. Mengimplementasikan *library* dengan mengikuti praktik terbaik dan kontrol keamanan yang diuraikan dalam *OWASP Mobile Application Security Verification Standard* (MASVS), khususnya pada aspek arsitektur dan kualitas kode.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini, yaitu:

1. Bagi pengembang aplikasi menyediakan sebuah *library D*yang praktis dan andal (*reliable*) untuk diintegrasikan, mempermudah pengembang dalam menerapkan mekanisme deteksi *root* yang akurat dan proteksi *flag secure* tanpa memerlukan keahlian keamanan yang mendalam.
2. Bagi pengguna akhir meningkatkan perlindungan data pribadi dan finansial saat menggunakan aplikasi, dengan mengurangi risiko yang timbul dari penggunaan aplikasi pada perangkat yang integritas keamanannya telah ter kompromikan (*compromised*).
3. Bagi komunitas keamanan siber menambah referensi dan wawasan mengenai implementasi metode deteksi *root* yang efektif dalam format *library* yang dapat diadopsi, serta mendorong praktik pengembangan aplikasi yang lebih aman di kalangan komunitas.

1.5 Batasan Masalah

Penelitian ini memiliki beberapa batasan agar fokus pada tujuan yang ingin dicapai, yaitu:

1. Lingkup deteksi *root*, penelitian berfokus pada perancangan dan implementasi metode deteksi *root* berbasis perangkat lunak (*software based*). Penelitian ini tidak akan membahas metode deteksi yang memerlukan akses fisik atau analisis perangkat keras.
2. Implementasi *flag secure*, pembahasan terbatas pada pengembangan fungsi untuk memvalidasi penerapan *flag secure* sebagai upaya pencegahan pengambilan tangkapan layar dan perekaman layar, tanpa mencakup fitur keamanan antarmuka lainnya.
3. Standar keamanan, verifikasi kualitas dan keamanan *library* akan mengacu secara spesifik pada kontrol yang relevan dalam OWASP *Mobile Application Security Verification Standard* (MASVS).
4. Versi *Android library* akan dikembangkan dan diuji untuk perangkat yang menjalankan sistem operasi *android* mulai dari API Level 27 (*Android* 8.1 Oreo) ke atas, hingga versi stabil terkini yang didukung saat penelitian berlangsung.
5. Keterbatasan akses, *library* akan dirancang untuk berfungsi menggunakan izin standar aplikasi *android* dan tidak akan meminta akses yang bersifat *invasif* atau melampaui batas wajar privasi pengguna.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun sebagai berikut:

BAB I Pendahuluan

Bab ini menyajikan latar belakang mengenai pentingnya keamanan perangkat *android*, dengan fokus pada risiko *rooting* dan *flag secure*. Di dalamnya dijelaskan rumusan masalah, tujuan penelitian, manfaat baik secara teoretis maupun praktis, serta ruang lingkup yang membatasi penelitian.

BAB II: Tinjauan Pustaka

Bab ini menguraikan teori teori dasar yang berkaitan dengan *rooting*, *flag secure*, dan pengembangan *library* keamanan *android*. Selain itu, bab ini meninjau penelitian terdahulu untuk memberikan kerangka konseptual serta menemukan kelebihan dan kekurangan dari pendekatan yang ada.

BAB III: Metode Penelitian

Bab ini menjelaskan pendekatan penelitian yang menggunakan metode *Mobile D*, termasuk teknik pengumpulan data, instrumen yang digunakan, serta tahapan mulai dari analisis kebutuhan, perancangan, pengembangan *library*, hingga pengujian.

Bab IV: Hasil dan Pembahasan

Bab ini menyajikan temuan dari pengujian *library*, dilengkapi dengan data dan ilustrasi. Bab ini juga menginterpretasikan hasil penelitian dengan

membandingkannya dengan kajian penelitian terdahulu untuk menilai keefektifan dan kelemahan dari solusi yang dikembangkan.

Bab V: Kesimpulan dan Saran

Bab ini merangkum seluruh hasil penelitian, menyoroti kontribusi penelitian terhadap peningkatan keamanan aplikasi *android*, serta mengidentifikasi keterbatasan yang ada. Selain itu, bab ini memberikan saran dan rekomendasi untuk pengembangan lebih lanjut guna mengoptimalkan keamanan perangkat.