BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital saat ini, keamanan aplikasi seluler menjadi sangat krusial. Peningkatan penggunaan aplikasi seluler untuk berbagai transaksi dan pertukaran informasi pribadi menuntut perlindungan data yang lebih ketat. Aplikasi malware yang menyamar sebagai aplikasi legit dapat mengakibatkan pencurian data, kerugian finansial, dan kerusakan reputasi [1]. Salah satu contohnya adalah Malware 'Daam' yang merupakan sebuah program jahat yang menyerang perangkat Android untuk mencuri data sensitif, melakukan *screenshot*, mengubah *password*, membaca pesan, dan mengakses kamera pengguna. Malware jenis ini menyebar melalui situs dan aplikasi tidak resmi, sehingga pengguna harus waspada terhadap *link* dan aplikasi mencurigakan [2]. Oleh karena itu, mengamankan aplikasi seluler bukan hanya kebutuhan, tetapi suatu keharusan untuk melindungi privasi pengguna dan integritas data [3][4]. Apabila data pengguna diambil oleh pihak luar yang tidak bertanggung jawab, maka data tersebut dapat diperjualbelikan atau disalahgunakan.

Sandboxing adalah teknik keamanan yang digunakan untuk menjalankan aplikasi yang tidak dipercaya dalam lingkungan yang aman, sekaligus untuk mencegah penyebaran infeksi malware dari sebuah aplikasi sehingga kerusakannya tidak menyebar secara menyeluruh pada sistem yang dijalani. Teknik ini mencakup berbagai metode seperti Metode Sistem Operasi, Virtualisasi, Pembungkus Proses, dan Penulisan Ulang Biner. Solusi *sandbox* biasanya menggunakan kombinasi dari metode-metode ini untuk memastikan aplikasi yang tidak dipercaya berperilaku baik saat dieksekusi pada sistem *host*, dengan setiap pelanggaran kebijakan keamanan biasanya menghasilkan penghentian aplikasi segera [5]. Pada *cyber security*, *developer* dapat menemukan sekaligus melakukan penelitian terkait jenis malware yang beredar di dalam sistem melalui penerapan *Sandbox*, sehingga *developer* dapat menemukan dan menguji solusi antimalware di *Sandbox* lagi [6].

Bahasa pemrograman yang diterapkan ke dalam *Sandbox* adalah Kotlin, karena memiliki sintaks yang ringkas dan mudah dibaca, serta memiliki interopabilitas dengan *Java* sehingga dapat berinteraksi dengan baik. Keunggulan penggunaan Kotlin tersebut menjadi opsi bahasa pemrograman untuk membangun sebuah aplikasi [7]. Hal ini dibuktikan dengan hasil penelitian terkait performa

aplikasi Android pada Java dan Kotlin yang menyimpulkan bahwa Kotlin memiliki performa yang unggul dalam hal penggunaan memorinya yang tergolong kecil dengan pengeksekusian program yang cepat dibandingkan dengan Java [8].

Untuk meningkatkan keamanan aplikasi seluler, diimplementasikanlah teknologi *sandboxing* yang memungkinkan aplikasi berjalan dalam lingkungan yang terisolasi dengan pembatasan akses, sehingga mengurangi risiko kerusakan yang mungkin ditimbulkan oleh aplikasi yang tidak terpercaya. Dengan demikian, pengguna dapat merasa lebih aman dan terlindungi dari ancaman potensial dalam lingkungan *mobile*. Metode yang diterapkan dalam proses penciptaan sistem tersebut adalah metode *waterfall* yang dipaparkan oleh Herbert D. Benington pada 29 Juni 1956 yang menekankan langkah-langkah sistematis dan mencakup lima tahapan secara berurutan, yaitu *requirement analysis*, *design*, *implementation and unit testing*, *integration and system testing*, dan *maintenance* [9]. Metode *waterfall* digunakan karena memiliki alur kerja yang jelas, cocok untuk pengembangan *software* berskala besar dengan proses yang lebih terstruktur, sekaligus menghemat biaya [9].

1.2 Rumusan Masalah

Permasalahan yang hendak diselesaikan melalui penelitian ini adalah apakah *Sandbox* yang dibangun menggunakan kotlin efektif dalam hal mengisolasi aplikasi?

1.3 Batasan Permasalahan

Batasan permasalahan yang hendak diselesaikan dalam penelitian dijabarkan ke dalam poin-poin di bawah ini.

1. Penelitian ini akan difokuskan pada implementasi lingkungan *sandboxing* pada aplikasi seluler menggunakan bahasa pemrograman Kotlin.
2. Penelitian ini tidak akan mencakup pengembangan solusi otentikasi atau enkripsi data yang bersifat terpisah dari implementasi lingkungan *sandboxing*.

1.4 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai adalah untuk memastikan keamanan data dari pengguna Android dari serangan aplikasi yang mencurigakan melalui penerapan *Sandbox* dengan bahasa pemrograman Kotlin.

1.5 Manfaat Penelitian

Penelitian ini bertujuan untuk meningkatkan keamanan aplikasi seluler melalui implementasi sandboxing dengan *Kotlin*, memberikan perlindungan lebih terhadap risiko keamanan dan membuat pengguna merasa lebih aman. Selain itu, penelitian ini berpotensi mengembangkan solusi keamanan baru, memberikan kontribusi signifikan pada keamanan informasi dalam aplikasi seluler.

1.6 Sistematika Penulisan

Sistematika penulisan terkait penelitian ini dimulai dari Pendahuluan hingga Simpulan dan Saran yang diuraikan secara singkat sebagai berikut.

- Bab 1 PENDAHULUAN
  Bab 1 merupakan tahap perencanaan dalam menentukan tujuan penelitian terkait suatu permasalahan melalui 6 sub-bab, yaitu latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan laporan skripsi ini.
- Bab 2 LANDASAN TEORI
  Bab 2 merupakan kumpulan teori yang menjadi pondasi dalam keseluruhan proses penelitian yang dilakukan. Teori-teori tersebut yaitu teori Android, *sandbox*, *Package Manager*, *Kotlin*, dan *Mobile Application*.
- Bab 3 METODOLOGI PENELITIAN
  Bab 3 merupakan penjabaran dari langkah-langkah penelitian yang telah dilakukan dan disertai dengan dokumentasinya.
- Bab 4 HASIL DAN DISKUSI
  Bab 4 berisikan tentang hasil yang telah dicapai melalui serangkaian proses penelitian beserta masukan yang diterima terkait implementasi penelitian.

- Bab 5 KESIMPULAN DAN SARAN

  Bab 5 berisikan kesimpulan dari keseluruhan proses penelitian yang telah dilakukan beserta dengan saran terkait penelitian dan sebagainya.