BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Sistem operasi Android telah berkembang pesat dan menjadi salah satu platform paling dominan di pasar global. Pada tahun 2020, pangsa pasar Android untuk perangkat ponsel cerdas mencapai 36,6%. Sebagai sistem operasi sumber terbuka yang dikembangkan oleh Google menggunakan bahasa pemrograman Java, Android menawarkan fleksibilitas tinggi sehingga menjadikannya platform pilihan bagi pengguna ponsel cerdas di seluruh dunia [1]. Hingga tahun 2023, jumlah pengguna ponsel global mencapai 7,33 miliar, dengan Android menguasai 70,93% pangsa pasar [2]. Di Indonesia, penggunaan smartphone juga menunjukkan pertumbuhan signifikan, dari 54 juta pengguna pada tahun 2015 menjadi 209,3 juta pada tahun 2023. Fakta ini memperlihatkan kontribusi besar Android dalam mendorong transformasi digital masyarakat [3].

Seiring berkembangnya ekosistem Android, aplikasi seluler memainkan peran penting dalam berbagai aktivitas sehari-hari, mulai dari e-commerce, e-health, hingga e-payment. Pada September 2019, tercatat 2,7 juta aplikasi tersedia di Google Play Store dan 2,46 juta di Apple App Store. Pertumbuhan aplikasi ini sejalan dengan meningkatnya jumlah perangkat seluler, yang diperkirakan mencapai 20 miliar pada tahun 2023 [4]. Namun, penggunaan aplikasi sering kali membutuhkan izin akses terhadap informasi pribadi pengguna. Kondisi ini menimbulkan risiko serius terkait privasi dan keamanan data, terutama ketika aplikasi dimanfaatkan oleh pihak yang tidak bertanggung jawab [4].

Meningkatnya jumlah aplikasi juga beriringan dengan peningkatan serangan siber terhadap perangkat seluler. Sebuah studi pada tahun 2021 mencatat keberadaan 45.000 aplikasi berbahaya yang menginfeksi 18 juta perangkat [4]. Salah satu ancaman utama adalah adware, yang pada tahun 2023 menyumbang 40,8% dari total ancaman yang terdeteksi [5]. Adware tidak hanya menampilkan iklan yang mengganggu, tetapi juga berpotensi mengumpulkan data pengguna

tanpa izin, melakukan klik otomatis, hingga menjadi pintu masuk bagi aktivitas berbahaya lain seperti pencurian data atau pengendalian perangkat secara ilegal [6].

Di Indonesia, serangan adware termasuk dalam tiga besar insiden keamanan pada kuartal keempat tahun 2023 [7]. Tingkat kesadaran masyarakat mengenai risiko keamanan siber pun masih rendah. Hanya 66% pengguna memahami bahaya penyalahgunaan data pribadi, dengan tingkat pemahaman yang lebih rendah pada kelompok tertentu seperti perempuan, pengguna dengan pendidikan menengah, serta mereka yang tidak bekerja di bidang teknologi [8]-[11]. Kondisi ini menjadikan sebagian pengguna lebih rentan terhadap ancaman adware.

Ancaman yang terus berkembang tersebut menuntut adanya mekanisme deteksi yang lebih adaptif dan efektif. Metode deteksi tradisional berbasis tanda tangan (*signature-based*) atau aturan (*rule-based*) memiliki keterbatasan dalam menghadapi variasi adware baru yang dinamis [12]. Oleh karena itu, diperlukan pendekatan berbasis analisis pola data yang lebih fleksibel.

Teknologi *machine learning* menawarkan solusi dengan kemampuan mengidentifikasi pola dan melakukan klasifikasi aplikasi berbahaya secara lebih akurat. Dengan memanfaatkan fitur-fitur aplikasi Android, *machine learning* mampu membedakan aplikasi normal dengan aplikasi berbahaya. Dari berbagai algoritma yang tersedia, *Extreme Gradient Boosting* (XGBoost) menonjol karena kinerja tinggi dalam klasifikasi data tabular, efisiensi pelatihan, serta kemampuannya menangani data tidak seimbang. Sejumlah penelitian sebelumnya juga menunjukkan bahwa XGBoost dapat mencapai akurasi kompetitif dalam mendeteksi aplikasi berbahaya pada perangkat Android [13], [14].

Selain pemilihan algoritma, aspek platform implementasi juga menjadi pertimbangan penting. Baik aplikasi native maupun aplikasi berbasis web memiliki keunggulan masing-masing sesuai kebutuhan. Aplikasi native unggul dalam performa tinggi dan integrasi mendalam dengan hardware. Sementara itu, aplikasi web atau *Progressive Web App* (PWA) menjadi alternatif efektif untuk konsumsi konten dan layanan lintas platform dengan biaya pengembangan yang lebih rendah. Penelitian menunjukkan bahwa web apps tidak selalu kalah dari native apps[15], [16]. Bahkan dalam lebih dari 31% kasus, web apps dapat mengungguli performa

native. Hal ini semakin didukung dengan hadirnya teknologi WebAssembly (WASM) yang mampu mendekati atau bahkan melampaui native code[17], [18].

Berdasarkan uraian tersebut, penelitian ini berfokus pada rancang bangun sistem deteksi adware pada aplikasi Android berbasis web dengan algoritma XGBoost. Integrasi model ke dalam aplikasi web diharapkan menghasilkan sistem yang mudah diakses, responsif, serta mampu meningkatkan keamanan pengguna Android sebagai upaya pencegahan terhadap ancaman adware di era digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalah pada penelitian ini antara lain:

1. Bagaimana mengimplementasikan model XGBoost ke dalam platform berbasis web untuk mendeteksi adware pada aplikasi Android?
2. Bagaimana performa model XGBoost dalam mendeteksi adware berdasarkan pengujian pada dataset dan file APK nyata?

1.3 Tujuan Penelitian

Tujuan dalam penelitian ini adalah:

1. Mengimplementasikan model XGBoost ke dalam aplikasi berbasis web yang dapat digunakan untuk mendeteksi adware pada aplikasi Android secara praktis dan interaktif.
2. Mengevaluasi performa model deteksi adware berbasis XGBoost melalui pengujian pada dataset dan file APK asli, sehingga diperoleh gambaran akurasi dan kemampuan generalisasi model.

1.4 Manfaat Penelitian

Manfaat yang diharapkan dalam penelitian ini adalah:

1. Memberikan kontribusi dalam meningkatkan keamanan perangkat Android melalui pengembangan model deteksi adware berbasis XGBoost yang efektif.
2. Memberikan informasi dan referensi kepada masyarakat maupun peneliti tentang pentingnya deteksi dini adware sebagai upaya pencegahan kebocoran data pribadi dan ancaman keamanan perangkat Android

1.5 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini dibatasi hanya mencakup hal-hal berikut:

1. Penelitian ini hanya membahas penggunaan algoritma XGBoost untuk mendeteksi adware pada aplikasi Android dengan pendekatan static analysis berbasis fitur permission dari file APK.
2. Penelitian ini mengimplementasikan model XGBoost ke dalam aplikasi berbasis website yang memungkinkan pengguna mengunggah file APK untuk dilakukan ekstraksi fitur permission dan klasifikasi secara otomatis.
3. Penelitian ini hanya berfokus pada dua kategori klasifikasi, yaitu adware dan benign, serta tidak mencakup jenis malware lain seperti spyware, ransomware, trojan, dan sejenisnya.