1. Pendahuluan

Latar Belakang

Pada perkembangan teknologi masa kini, android menjadi salah satu sistem operasi yang paling terkenal dan populer di platform komunikasi seluler dengan tingkat pasar sebesar 75-80% [9]. Sistem operasi android memiliki fitur teknologi modern yang dapat membantu aktivitas manusia sehari-hari seperti belanja online, jualan online, media social, perbankan online dan aplikasi lainnya. Sehingga android dapat menjadi target malware untuk mengambil kendali atas perangkat. Penelitian tentang malware seluler menunjukkan bahwa malware di platform android terus meningkat pada tiap tahun [3]. Ada berbagai macam jenis-jenis malware yang tersebar saat ini seperti virus, worm, trojan, rootkit, ransomware, backdoor, adware dan spyware. Malware bisa disebut juga malicious software yang diciptakan untuk menyusup pada android seperti memata-matai pemilik tersebut, melacaknya, memonitori aktivitas telepon maupun SMS, memonitori email, dan melacak aktivitas pengguna saat web browsing [6].

Untuk mengatasi malware pada android umumnya cukup dengan menggunakan tools atau aplikasi antivirus yang sudah ada sebelumnya. Menggunakan tools maupun antivirus merupakan cara tradisional yang kurang efisien karena malware yang sifatnya dapat berubah menjadi lebih baru dalam waktu yang singkat demi menghindari berbagai macam pendeteksian. Semakin berkembangnya malware pada saat ini, maka diperlukan implementasi dan analisis terhadap malware untuk melihat bagaimana malware bekerja dan melihat sifat dari malware pada sistem android.

Dalam penelitian [2] menggunakan dataset dengan nilai biner dalam proses mendeteksi malware android menggunakan metode *Naïve Bayes* dengan akurasi yang baik. Dalam penelitian [6] mengatakan, bahwa *Naïve Bayes* sangat baik dalam mengolah data dalam bentuk biner. Dalam penelitian [4][3] dengan metode *Decision Tree* dipilih karena memiliki nilai akurasi yang baik dalam mendeteksi malware. Penelitian ini akan menggunakan dataset yang berbeda dari penelitian sebelumnya dengan menggunakan dataset android traffic dengan data nilai tidak biner yang diambil dari *website* Kaggle [17] untuk proses implementasi terhadap malware pada android dengan metode *Decision Tree* dan *Naïve Bayes*. Untuk mengolah dataset digunakanlah *Machine Learning* karena cara kerjanya yang dapat mempermudah dalam memperoleh data untuk melihat sebuah label dari dataset.

Pada peneliti tugas akhir ini, akan membuktikan apakah metode *Naïve Bayes* bisa memiliki akurasi yang lebih baik daripada *Decision Tree* ketika dataset yang dipakai tidak memiliki nilai biner.

Topik dan Batasannya

Rumusan masalah yang diselesaikan pada tugas akhir ini adalah sebagai berikut:

1. Bagaimana perbedaan nilai akurasi dari metode *Decision Tree* dan *Naïve Bayes* dalam mendeteksi malware pada android?

Batasan masalah yang digunakan pada tugas akhir ini adalah sebagai berikut:

1. Dalam proses analisis deteksi malware pada android diimplementasikan berdasarkan atribut Type dengan menggunakan metode *Decision Tree* dan *Naïve Bayes.*
2. Penelitian ini menggunakan data pelatihan dan data pengujian yang akan digunakan untuk mengelola data secara acak.

Tujuan

Tujuan penelitian tugas akhir ini untuk implementasikan sebuah algoritma *Machine Learning* supaya mendapatkan metode yang terbaik dalam mendeteksi malware pada android menggunakan dataset yang berbeda dari penelitian sebelumnya [2] [9][21] dengan melihat nilai akurasi dari setiap metode tersebut.

Organisasi Tulisan

Urutan penulisan pada tugas akhir ini adalah sebagai berikut : pada bagian BAB 2 akan dijelaskan tentang Studi Terkait, pada bagian BAB 3 dijelaskan tentang sistem yang dibangun diantaranya pembuatan model untuk *Machine Learning*, pada BAB 4 akan dijelaskan tentang evaluasi, dan pada BAB 5 dijelaskan kesimpulan dan saran.