1. Pendahuluan

Latar Belakang

Fintech adalah singkatan dari *financial technology* merupakan jenis perusahaan di bidang jasa keuangan yang digabungkan dengan teknologi. *Fintech* diubah menjadi sebuah aplikasi android untuk mempermudah dalam menghemat waktu yang dapat mengelola pajak secara otomatis, memperkecil risiko ketidakpatuhan pajak, menerima pembayaran lebih cepat dan banyak kemudahaan lainnya [15]. Aplikasi *fintech* memiliki banyak kemudahan tetapi tidak semua aplikasi *fintech* dapat dipercaya terbukti pada september 2020 ditemukan aplikasi *fintech* yang sengaja memanfaatkan kesulitan keuangan sebagian masyarakat di masa pandemi ini. Pinjaman dari *fintech* tersebut mengenakan suku bunga yang tinggi dan persyaratan pinjaman jangka waktu pendek serta meminta semua akses data di telepon genggam, yang digunakan untuk mengintimidasi saat penagihan [16]. Aplikasi *fintech* akan meminta akses izin yang tidak relevan seperti akses kontak, mikrofon, lokasi dan masih banyak lagi di ponsel pengguna sebagai cara konfirmasi data calon peminjam. Bahkan terdapat penggunaan aplikasi *fintech* yang memberikan akses terhadap data di ponsel dapat membuat riwayat transaksi bocor sehingga dapat digunakan pihak yang tidak bertanggung jawab [17].

Malware berasal dari kata *malicious* dan *software* dapat diartikan perangkat lunak yang digunakan untuk melakukan perusakan sistem, pencurian atau pengumpulan informasi, hingga mendapatkan akses terhadap suatu sistem [18]. Terdapat beberapa cara penyebaran *malware* seperti email *phising*, serangan rekayasa sosial, dan *downloader*. Tujuan dari penyebaran *malware* adalah untuk pencurian data rahasia, pengumpulan informasi seperti password dan email, serta *spamming* [18]. Analisis *malware* adalah sebuah metode untuk mengidentifikasi *malware* atau dapat diartikan suatu aktivitas yang dilakukan untuk mendeteksi dan mengamati perilaku *software* ketika dieksekusi serta metode pencegahan paling efektif terhadap *malware*. Penelitian mengenai deteksi *malware* telah banyak dilakukan oleh beberapa orang atau instansi di dunia umumnya dalam deteksi *malware* dapat menggunakan pendekatan tradisional seperti antivirus, namun menurut [1] dalam deteksi *malware* pada perangkat android dengan menggunakan pendekatan tradisional seperti antivirus tidaklah efektif dikarenakan *malware* di setiap tahunya selalu berbeda dan terus berkembang sehingga membutuhkan pembaruan database pada antivirus. Untuk mengatasi hal tersebut maka dibutuhkan *machine learning* untuk deteksi *malware* pada aplikasi android.

Dalam penelitian ini sistem yang dibangun bertujuan untuk deteksi *malware* aplikasi *fintech* berdasarkan permissionnya untuk dataset diambil dari ekstraksi fitur permission dari 160 sampel aplikasi *fintech* dengan 80 sampel aplikasi *fintech* yang terdaftar di OJK [19] dan 80 sampel aplikasi *fintech* yang tidak terdaftar di OJK [20]. Untuk metode klasifikasinya menggunakan algoritma naïve bayes dan random forest serta K-*fold Cross Validation* yang tersedia di *tool* WEKA [21].

Tujuan penelitian ini adalah menganalisa deteksi *malware* pada aplikasi android *fintech* berdasarkan permission dengan menggunakan klasifikasi naïve bayes dan random forest. Bagian penelitian selanjutnya yaitu bagian 2 studi terkait yang membahas penelitian sebelumnya dan gambaran tentang *malware* pada aplikasi android berdasarkan permission. Bagian 3 membahas perancangan sistem yang dibangun berdasarkan teori yang terkait. Pada bagian 4 membahas hasil dan analisanya. Selanjutnya bagian 5 membahas kesimpulan dan saran untuk penelitian selanjutnya.