BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi merupakan salah satu hal yang terus mengalami perkembangan yang pesat setiap tahunnya untuk mempermudah kehidupan manusia, salah satu perkembangannya adalah manusia dapat saling terhubung melalui internet menggunakan perangkat Android. Android merupakan sistem operasi mobile yang paling banyak digunakan pada saat ini. Android menjadi kontributor utama pada pasar seluler dengan lebih dari 2 miliar perangkat aktif. Android memegang lebih dari 74% total pengguna *smartphone* dunia pada tahun 2019. Dengan popularitas yang dimiliki oleh Android dan ini memunculkan dampak negatif salah satunya adalah serangan Malware [1].

Malware atau *Malicious Software*, merupakan program jahat dengan maksud dan tujuan merugikan pihak lain. Sistem Android menjadi target utama malware seluler karena sistem operasi Android memungkinkan pengguna untuk menginstal aplikasi yang diunduh dari pasar pihak ketiga. Android malware menyerang dengan berbagai cara dan salah satunya dengan menggunakan fitur permission yang ada pada aplikasi android. Banyak pengguna yang tidak mengerti apa arti dari setiap permission dan memberikan permission tersebut tanpa memikirkan resiko yang memungkinkan aplikasi tersebut mengakses informasi sensitif pengguna[2].

Banyak metode dan pendekatan yang digunakan dalam mengidentifikasi dan mendeteksi malware android salah satunya adalah dengan menggunakan bantuan *Machine Learning*. *Machine Learning* merupakan serangkaian teknik yang dapat membantu dalam menangani dan memprediksi data dengan cara mengajarkan komputer untuk memiliki kecerdasan layaknya manusia, machine learning memiliki cabang algoritma yang mengambil inspirasi dari otak manusia bernama Deep Learning[3]. Salah satu algoritma *Deep Learning* yang paling umum digunakan dalam menyelesaikan masalah adalah algoritma *Convolutional Neural*

Network. *Convolutional Neural Network* ini adalah hasil pengembangan algoritma saraf jaringan yang dirancang untuk mengelola data dua dimensi[4].

Convolutional Neural Network memiliki algoritma turunan bernama *Convolutional Neural Network 1-Dimension*. Pembeda utamanya terletak pada dimensi nya, dimana *Convolutional Neural Network 1-Dimension* menggunakan array 1D untuk menggantikan matriks 2D pada CNN pada umumnya. Keunggulan utama dari Convolutional Neural Network 1-Dimensi dibanding *Convolutional Neural Network 2-Dimension* adalah mengurangi kompleksitas komputasi karena hanya menggunakan urutan data. Karena persyaratan komputasinya yang rendah inilah *Convolutional Neural Network 1-Dimension* cocok untuk di implementasikan pada aplikasi perangkat seluler[5].

Berdasarkan latar belakang di atas, penelitian ini akan mencoba untuk mengimplementasikan algoritma *Convolutional Neural Network 1-Dimension* untuk mengidentifikasi malware berdasarkan permissionnya, dan mengetahui seberapa efektifkah penerapan algoritma ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dirumuskan sebuah permasalahan yaitu :

1. Seberapa efektifkah implementasi algoritma *Convolutional Neural Network 1-Dimension* untuk identifikasi malware berdasarkan permissionnya?
2. Berapakah tingkat akurasi, *recall* dan *precision* yang dihasilkan algoritma *Convolutional Neural Network 1-Dimension* dalam identifikasi malware android?

1.3 Batasan Masalah

Agar penelitian ini terarah dan sesuai dengan tujuan peneliti, serta permasalahan yang dihadapi tidak terlalu luas, maka ditetapkan batasan terhadap masalah yang sedang diteliti. Adapun batasan masalah penelitian sebagai berikut:

1 Proses dekompilasi menggunakan tool JDAX sehingga tidak semua aplikasi android dapat dilakukan proses dekompilasi.

2 Lama waktu proses dekompilasi tergantung terhadap ukuran file APK.

3 Output dari program ditentukan dengan nilai 1 atau 0, 1 berarti Malware dan 0 berarti aplikasi jinak.

4 Hanya dapat untuk memprediksi aplikasi APK dan bukan XAPK.

5 Dataset yang digunakan berupa dataset dari website kaggle ditambah dengan dataset yang peneliti buat sendiri dengan jumlah total 510 sample.

6 Untuk mengunduh apk dari Playstore menggunakan cara manual.

7 Untuk mengunduh apk dari ApkPure menggunakan selenium webdriver.

1.4 Tujuan Penelitian

Adapun maksud dan tujuan dari penelitian ini adalah :

1 Untuk mengimplementasikan model *Convolutional Neural Network* 1 Dimension dalam mengidentifikasi malware dengan aplikasi jinak android berbasis *permission*-nya.

2 Untuk mengetahui hasil akurasi algoritma *Convolutional Neural Network* 1 Dimension dalam mengidentifikasi malware dengan aplikasi jinak android berbasis *permission*-nya.

1.5 Manfaat Penelitian

Penelitian ini tentunya diharapkan dapat memberikan manfaat secara teoritis dan praktis sebagai berikut:

1.5.1 Manfaat Teoritis

Menambahkan wawasan dan memperbanyak ilmu pengetahuan yang didapatkan dalam bidang *Artificial Intelligence*, khususnya dalam perkembangan teknologi *Machine Learning* dan *Deep Learning* pada bidang malware analisis.

1.5.2 Manfaat Praktisi

1. Peneliti

   Dapat memberikan pengetahuan baru mengenai *Convolutional Neural*

Network 1 Dimensi dan dapat dijadikan bahan referensi untuk penelitian-penelitian ke depan.

2. Pembaca

   Bagi pembaca terkhususnya untuk yang ingin membuat sistem aplikasi untuk deteksi malware pada android. Penelitian ini diharapkan dapat membantu atau memberi pengetahuan dan wawasan para pembaca untuk mengembangkan sistem atau aplikasi tersebut.

3. Masyarakat

   Diharapkan penelitian ini juga bisa diterapkan oleh masyarakat umum yang mempunyai perangkat android untuk bisa berhati-hati dalam menginstall suatu aplikasi pada perangkat android dan lebih bijak dalam menggunakannya.

1.6 Sistematika Penulisan

Berikut adalah sistematika penulisan naskah yang dilakukan penulis dalam penelitian ini :

BAB I PENDAHULUAN, berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian.

BAB II TINJAUAN PUSTAKA, berisi Penelitian yang relevan, dan teori dasar.

BAB III METODE PENELITIAN, didalamnya terdapat alur penelitian, variabel penelitian, metode penelitian, metode analisis, alat dan bahan penelitian.

BAB IV HASIL DAN PEMBAHASAN, bab ini merupakan tahapan yang penulis lakukan dalam merancang model hingga menjadi hasil yang meliputi beberapa pembahasan yaitu proses pengumpulan data, preprocessing data, pembuatan arsitektur model, proses *training*, proses evaluasi dan hasil, proses implementasi model.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.