BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring berkembangnya teknologi komputer di zaman sekarang sudah menjadi bagian terpenting di dalam kehidupan sehari-hari. Teknologi komputer yang berkembangan cukup pesat sangat berperan serta dalam mempermudah pertukaran informasi antar pengguna mulai dari akademik, kesehatan, sampai dengan pengguna *internet* biasa. Perkembangan teknologi yang semakin pesat terutama teknologi komputer khususnya bidang teknologi komputer jaringan, permasalahan yang sering dihadapi adalah segi keamaanannya. Permasalahan keamanan komputer yang paling banyak dijumpai adalah penyebaran *Malware (malicious software)* melalui jaringan *internet* yang menyebabkan berbagai macam kerugian Setiawan (2016).

Malicous Software atau yang lebih dikenal sebagai *Malware* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti *Trojan, Virus, Spyware* dan *Exploit*. *Malware* dibuat khusus agar tersembunyi sehingga mereka bisa tetap berada di dalam sistem komputer pada periode waktu tertentu tanpa sepengetahuan pemilik sistem. Biasanya mereka menyamarkan diri sebagai program yang bersih. Dampak yang ditimbulkan *Malware* sendiri bias menyebabkan kerusakan dan gangguan yang meluas yang memerlukan upaya pemulihan intensif di dalam komputer. Penyebaran *Malware* di dunia maya terus meningkat Cahyanto, Wahanggara et al. (2018).

Beberapa kasus mengenai serangan *Malware* telah banyak meresahkan pengguna *internet*. Salah satu bentuk dari serangan tersebut yaitu dengan melakukan penyisipan file-file berbahaya atau malicious ke komputer. Contohnya seperti penyisispan *skrip web shell* yang di sisipkan ke komputer penyedia layanan *internet*. Apabila berhasil diunggah, *skrip web shell* dapat memberikan akses *shell* tidak sah kepada pengunggah *skrip* secara jarak jauh. Hal ini dapat berpotensi merusak aplikasi web dan juga komputer server yang menyediakan aplikasi tersebut Setiawan (2016).

Banyaknya aktifitas penyebaran *Malware* yang terjadi melalui jaringan *internet* membuat banyak pengguna menjadi resah, maka dari itu peneliti merasa perlu melakukan pendeteksian terhadap serangan *Malware* tersebut agar pengguna bisa mengetahui apakah data yang disimpan di internet aman dari penyisipan *Malware* atau tidak.

Dalam penelitian ini, peneliti menerapkan metode naïve bayes dalam melakukan pendeteksian. Algoritma naïve bayes didasarkan pada tingkat probabilitas nilai dari suatu atribut data terhadap kelasnya. Naïve bayes pada detection *Malware* dengan diskritisasi variabel memiliki nilai yang berbeda dalam suatu atribut, sebagai contoh penerapan pada *detection Malware* dataset yang digunakan adalah data dengan tipe kontinu, sehingga nilai probabilitas menunjukan kemungkinan nilai yang sama keluar pada suatu kelas namun pada sisi lain rentang nilai pada atribut tersebut sangat besar sehingga nilai probabilitas dari nilai tersebut muncul kembali dalam suatu kelas. Untuk mengatasi hal tersebut dilakukan pendekatan teknik diskritisasi dengan menggunakan *mean*/standar deviasi Wirawan and Eksistyanto (2015).

Berdasarkan latar belakang diatas maka peneliti ingin melakukan penelitian dengan judul **"Penerapan Naïve Bayes Pada Detection *Malware* Dengan Diskritisasi Variabel".**

1.2 Identifikasi Masalah

Karena banyaknya aktifitas-aktifitas berbahaya atau perusak perangkat lunak yang tersebar melalui jaringan *internet*, maka diperlukan adanya pendeteksian terhadap *Malware (malicious software)* tersebut.

1.3 Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari permasalahan yang ada, maka perlu adanya batasan masalah. Batasan masalah dalam penelitian ini yaitu :

a. *Dataset* yang digunakan dalam penelitian ini adalah dataset *Malware* yang didapat dari data nsaravana *(*sumber *:https://www.kaggle.com/nsaravana/Malware-detection)*
b. Algoritma yang digunakan yaitu Algoritma Naive Bayes Classifier

1.4 Rumusan Masalah

Berdasarkan latar belakang diatas maka peneliti merumuskan permasalahan dalam penelitian ini yaitu " Bagaimana menerapkan Naïve Bayes pada *detection malicious software (Malware)* dengan Dikritisasi Variabel?".

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk menerapkan algoritma naïve bayes dalam mendeteksi *Malware.*

1.6 Manfaat Penelitian

Dengan menggunakan algoritma naive bayes ini diharapkan dapat membantu mempermudah pengguna dalam menemukan metode yang tepat untuk mendeteksi serangan dari *Malware*.

1.7 Ruang Lingkup Penelitian

Dalam penulisan tesis ini, penulis akan membatasi ruang lingkup penelitian dengan menitik beratkan permasalahan yang akan dibahas, yaitu melakukan pendeteksian terhadap *Malware* dengan menggunakan algoritma naïve bayes.

1.8 Susunan dan Struktur Tesis

Susunan dan struktur tesis tesis ini maksudnya agar dapat memberikan garis besarnya secara jelas sehingga terlihat hubungan antara bab yang satu dengan bab yang lainnya. Susunan dan struktur tesis tesis dijabarkan di bawah ini sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian, ruang lingkup penelitian, serta susunan dan struktur tesis.

BAB II KAJIAN PUSTAKA

Pada bab ini membahas tentang kajian pustaka, penelitian terdahulu, kerangka berfikir, dan hipotesis penelitian yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

Pada bab ini pembahasannya yang terdiri dari desain dan jadwal penelitian, data penelitian meliputi jenis data, populasi dan sampel penelitian,

kemudian konsep dan metode penelitian yang digunakan, metode pengumpulan data serta teknik analisis data.

BAB IV ANALISA DATA

Pada bab ini akan dibahas tentang proses analisa data mulai dari pengambilan data sampai ke prapemrosesan data.

BAB V HASIL DAN PEMBAHASAN

Pada bab ini pembahasannya meliputi hasil dari penelitian dan pembahasannya.

BAB VI KESIMPULAN DAN SARAN

Bab ini menjelaskan tentang kesimpulan serta saran dari hasil penelitian

LAMPIRAN

Berisi lampiran pendukung daripada penelitian yang akan dilakukan.