BAB I

PENDAHULUAN

1.1. Latar Belakang

Pendeteksian intrusi adalah proses memantau dan menganalisis peristiwa yang terjadi dalam sistem komputer secara berurutan untuk mendeteksi tanda-tanda masalah keamanan. Permasalahan saat ini deteksi intrusi berfokus pada masalah pemilihan fitur, karena beberapa fitur tidak relevan dan berlebihan yang menghasilkan proses deteksi yang panjang dan menurunkan kinerja sistem deteksi intrusi atau *intrusion detection system* (IDS). Sistem tersebut berfungsi untuk mengidentifikasi *traffic* atau lalu-lintas data pada sebuah jaringan komputer dimana IDS dapat menentukan apakah *traffic* aman, mencurigakan atau bahkan terindikasi merupakan serangan. Penelitian ini bertujuan untuk mengklasifikasi pendeteksian sistem serangan DoS pada sebuah jaringan perangkat IoT yang menggunakan Raspberry pi.

Internet of Things (IoT) dianggap menjadi investasi masa depan internet yang bekerja pada komunikasi *Machine to Machine* (M2M) dan *Radio Frequency Identification* (RFID) (Zawoad & Hasan, 2013). Tujuan utama dari IoT adalah untuk memungkinkan pertukaran data yang aman antara perangkat dunia nyata dan aplikasi. IoT telah menjadi cukup akrab dalam beberapa tahun terakhir. Banyaknya perangkat rutinitas sehari-hari semakin terhubung dengan Internet yang mencakup banyak kemampuan seperti penginderaan, otonomi dan kesadaran kontekstual. Perangkat IoT termasuk komputer pribadi, laptop, smartphone, tablet dan perangkat rumah yang tertanam lainnya (Hossain dkk., 2015). Perangkat ini terhubung satu dengan yang lain dan berbagi jaringan yang sama untuk saling berkomunikasi. Semua perangkat ini terhubung dengan sensor tertentu untuk mendeteksi kondisi sekitarnya dan bekerja sesuai dengan situasi. Perangkat ini juga diprogram untuk mengambil sebuah

keputusan secara otomatis atau menginformasikan sesuai dengan pengguna sehingga pengguna dapat membuat keputusan terbaik.

Jaringan interkoneksi pada IoT dapat menghubungkan berbagai objek yang memiliki identitas pengenal serta alamat IP, sehingga dapat saling berkomunikasi dan bertukar data. Obyek-obyek dalam IoT dapat menggunakan maupun menghasilkan layanan-layanan dan saling bekerjasama untuk mencapai suatu tujuan bersama. Dengan demikian dapat membawa banyak kemajuan di bidang teknologi aplikasi dan layanan yang dapat membawa manfaat bagi pengembangan bisnis global. Banyak perangkat IoT saling terhubung untuk berbagi informasi dan komunikasi secara umum memberikan masalah pada keamanan jaringan dalam IoT.

Denial of Service atau biasa disebut DOS adalah salah satu serangan yang menyerang sebuah komputer atau server pada sebuah traffic jaringan. Serangan ini bekerja dengan cara menghabiskan sumber daya yang dimiliki komputer atau *server* tersebut tidak dapat berjalan sebagaimana mestinya dan menyebabkan pengguna tidak dapat mengakses layanan komputer atau *server* yang diserang tersebut. *Distributed Denial of Service* atau disebut juga DDOS adalah jenis serangan terdistribusi dari DOS. Serangan ini yang menggunakan banyak penyerangan menggunakan komputer yang dikhususkan untuk melakukan penyerangan terhadap suatu *server* atau jaringan. Serangan DOS ini menyebabkan pengguna tidak dapat melakukan akses terhadap sistem atau jaringan yang dituju. Dalam serangan DOS terdapat bermacam-macam jenis serangan salah satunya adalah *Flood*. Target dari serangan DDOS sendiri biasanya adalah *Routing Device, Web, Electronic Mail* dan *Service Domain Name System*.

Salah satu penelitian terkait yang telah dilakukan sebelumnya adalah penelitian penggunaan Rapsberry Pi sebagai IDS dengan memanfaatkan gabungan aplikasi honeypot, Snort, Kippo, dan Dionea (Bharathi, 2019). Penelitian lainnya juga menggunakan Rapsberry Pi sebagai IDS *web server* (Atmojo, 2018) dan membuktikan bahwa Raspberry Pi dapat menjalankan tugas sebagai IDS dengan baik walaupun memiliki *resource* yang terbatas. Namun, penelitian tersebut belum dapat menentukan apakah *traffic* tersebut aman atau mengindikasi sebuah serangan.

Menurut Witten dkk (Witten dkk., 2011) algoritma Naive Bayes merupakan algoritma yang menggunakan pendekatan statistik dalam mengambil keputusan. Kelebihan dari metode ini adalah algoritma yang sederhana dengan kompleksitas perhitungan yang rendah. Namun, metode Naive Bayes memiliki kelemahan terkait sifat independensi dari fitur Naive Bayes tidak dapat selalu diterapkan sehingga akan berpengaruh pada tingkat akurasi perhitungan. Namun, metode Naive Bayes dapat dioptimasi dengan cara menggunakan memberikan bobot pada masing-masing atribut. Dalam penelitian data dengan format KDD99 digunakan agar data jaringan dapat dirubah dalam bentuk angka yang setiap atributnya memiliki bobot.

Penelitian ini menggunakan dataset *training* dari NSLKDD dengan format KDD99 dan data *testing* didapatkan dari proses log IDS pada perangkat Raspberry Pi. Penelitian ini menggunakan dataset yang berbeda agar mengetahui dataset *training* yang banyak digunakan saat ini masih dapat bekerja dalam jaringan perangkat IoT. Dataset testing yang baru perlu dibangun karena NSLKDD bukan dataset yang dikhususkan pada jaringan IoT namun layak digunakan untuk data training awal untuk pembelajaran bagi sistem. Berdasarkan penjelasan di atas, maka dalam penelitian ini ditawarkan solusi dalam menentukan apakah sebuah *traffic* tersebut berupa serangan atau tidak pada perangkat IoT sebagai IDS dengan menggunakan metode Naive Bayes.

1.2. Rumusan Masalah

Dari latar belakang diatas dapat ditarik permasalahan untuk dijadikan perumusan masalah antara lain :

1. Bagaimana implementasi metode Naïve Bayes dalam mengklasifikasi pendeteksian jenis serangan berupa DoS pada sebuah jaringan yang menggunakan perangkat IoT, dalam hal ini Raspberry pi?
2. Bagaimana tingkat akurasi metode Naïve Bayes dalam memproses data serangan berupa DoS pada sebuah jaringan yang menggunakan perangkat IoT?

1.3. Batasan Masalah

Batasan-batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Serangan yang dilakukan hanya sebagai simulasi dengan menyerang server yang ada.
2. data *training* menggunakan data set NSL KDD yang dapat diperoleh di https://web.archive.org/web/20150604025119/http:/nsl.cs.unb.ca/NSL-KDD/
3. Analisis pengujian algoritma Naive Bayes untuk IDS tidak termasuk dalam hal implementasi ke dalam suatu sistem jaringan.
4. Metode yang digunakan pada klasifikasi serangan adalah metode Naïve Bayes.
5. Tidak melakukan monitoring serangan secara real time.

1.4. Tujuan Penelitian

Berdasarkan rumusan yang dibuat maka dapat diambil tujuan dari penelitian ini. Tujuan dari dibuatnya penelitian ini antara lain :

1. Mengimplementasi metode Naïve Bayes dalam mengklasifikasi pendeteksian jenis serangan berupa DoS pada sebuah jaringan menggunakan perangkat IoT, dalam hal ini Raspberry pi.
2. Mengukur tingkat akurasi metode Naïve Bayes dalam memproses data serangan berupa DoS pada sebuah jaringan yang menggunakan perangkat IoT

1.5. Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain :

1. Dapat membantu administrator jaringan apabila terdapat serangan Dos.
2. Mengenal dan memahami kinerja algoritma naïve bayes pada proses klasifikasi dalam IDS.