BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Evolusi teknologi telah memungkinkan setiap perangkat elektronik terhubung ke internet dan saling berkomunikasi secara *realtime*. Hal ini mendorong lahirnya terminologi baru pada jaringan komunikasi data yang dikenal dengan *Internet of Things* (IoT). Hadirnya IoT telah memberikan berbagai kemudahan, dan memperkaya cara interaksi manusia dengan lingkungan, sosial, dan objek. IoT telah diaplikasikan pada berbagai bidang seperti bidang kesehatan, otomotif, hiburan, industri[1]. *Internet of Things* (IoT) telah menjadi bagian integral dari kehidupan *modern*, menghubungkan berbagai perangkat pintar untuk meningkatkan efisiensi dan kenyamanan. Dengan IoT, berbagai perangkat seperti lampu, termostat, kunci pintu, dan bahkan peralatan rumah tangga dapat dikendalikan dan dipantau dari jarak jauh[2].

Serangan DDoS (Distributed Denial of Service) merupakan salah satu ancaman utama dalam dunia keamanan cyber saat ini. Serangan DDoS memanfaatkan kelemahan infrastruktur jaringan target, seperti bandwidth atau sumber daya komputasi, dengan cara membanjiri target tersebut dengan permintaan lalu lintas yang melebihi kapasitas normalnya [3].

Teknik DDoS ini memanfaatkan penyerang menggunakan komputer zombie yang dibuat dengan perangkat lunak berbahaya yang ditempatkan di komputer korban untuk mengirim paket dalam jumlah besar. Serangan DDoS menyebabkan lalu lintas jaringan yang tinggi dengan paket yang dikirim di

jaringan, menyebabkan pengguna biasa yang ingin menerima layanan tidak menanggapi permintaan mereka [4].

Serangan seperti itu dapat datang dalam berbagai bentuk, seperti serangan fisik terhadap sistem IT, melebihi kapasitas koneksi jaringan, atau menggunakan kelemahan aplikasi. Sebagian besar serangan cyber ditujukan untuk mengganggu keamanan dengan membajak data dan informasi penting [5]. Serangan ini akan mengakibatkan mesin atau sumber daya jaringan tidak dapat diakses atau digunakan oleh pengguna. Serangan DDoS biasanya berasal dari beberapa mesin yang dioperasikan oleh pengguna atau bot [6].

Beberapa tahun terakhir, serangan Distributed Denial-of-Service (DDoS) telah menyebabkan kerugian yang signifikan untuk pengguna Internet of Things (IoT) dalam bidang industri dan pemerintahan. Adanya serangan DDoS dapat menyulitkan organisasi seperti terganggunya aktivitas online, data cloud organisasi, dan perangkat yang terhubung dengan internet [7].

Naive Bayes Classifier adalah algoritma klasifikasi probabilistik yang didasarkan pada teorema Bayes. Algoritma ini mengasumsikan bahwa setiap fitur yang ada dalam data independen satu sama lain. Naive Bayes Classifier sangat populer dalam deteksi ancaman keamanan jaringan karena kinerja yang baik dan kecepatan komputasi yang tinggi. Dengan menggunakan metode ini, dapat dilakukan klasifikasi pada data yang masuk ke jaringan dan mengidentifikasi apakah data tersebut merupakan ancaman atau tidak [8].

Naïve Bayes adalah salah satu metode yang dapat digunakan untuk melakukan klasifikasi data. Naive Bayes adalah metode algoritma klasifikasi sederhana yang dapat berkontribusi pada keputusan akhir. Pengoperasian metode Naive Bayes menggunakan parameter yang menghitung peluang dalam statistik serta menghitung probabilitas satu kelas dari setiap kelompok [9].

Dataset yang digunakan dalam penelitian ini adalah CICIoT2023, yang berisi berbagai jenis lalu lintas jaringan IoT. Dataset ini mencakup beberapa kelas, yaitu Benign Traffic (lalu lintas normal), Mirai-greeth_flood, Mirai-greip_flood, dan Backdoor_Malware. Kelas-kelas ini mewakili berbagai jenis serangan malware yang umum terjadi pada jaringan IoT [10].

Untuk mendeteksi serangan DDoS pada IoT sendiri telah dilakukan oleh beberapa peneliti sebelumnya antara lain, yang dilakukan oleh Muhammad Kana Riskilah, Fazmah Arif Yulianto dan Erwid M Jadied pada tahun 2022 dimana mereka memprediksi serangan DDoS menggunakan algoritma *Naïve Bayes* dengan metode *Intrusion Detection System (IDS)* dengan nilai akurasi sebesar 99.30%, sebaliknya penelitian yang dilakukan oleh Aditya Dwi Afifaturahman dan Firmansyah MSN menggunakan algoritma *K- Nearest Neighbor* mempunyai tingkatan akurasi yang lebih rendah yaitu 94.44%. Berdasarkan dari paparan permasalahan maka akan berfokus pada klasifikasi *dataset anomaly network traffic* pada *Intrusion Detection System (IDS)* dengan membandingkan algoritma *K-Nearest Neighbour (KNN)* dan *Naïve Bayes* dengan parameter metric *accuracy*, *sensitivity*, dan *specificity* sehingga akan menghasilkan nilai *gmeans* untuk studi perbandingannya[11]. Dari beberapa penelitian menunjukkan bahwa berbagai

metode yang telah digunakan untuk mendeteksi serangan DDoS memiliki akurasi yang baik. Namun, dengan demikian metode *Naive Bayes* yang dikenal memiliki efisiensi tinggi dan kecepatan komputasi baik, dalam mendeteksi serangan DDoS pada IoT masih belum dimaksimalkan. Dengan demikian, studi ini berfokus pada penerapan dan evaluasi algoritma Naive Bayes dalam mendeteksi serangan DDoS di IoT, bertujuan untuk meningkatkan ketepatan deteksi dan sekaligus memperluas pilihan metode keamanan siber bagi sistem jaringan komputer berbasis IoT

Dengan demikian, terlihat bahwa salah satu metode yang efektif dalam mendeteksi serangan DDoS pada IoT adalah *Naive Bayes*. *Naive Bayes Classifier* merupakan pengklasifikasi probabilitas sederhana berdasarkan pada teorema Bayes. Teorema Bayes dikombinasikan dengan “*Naive*” yang berarti setiap atribut/variabel bersifat bebas (*independent*)[12]. Klasifikasi *Naive Bayes* tidak memerlukan sejumlah besar data sebelum pembelajaran dimulakan serta ketika membuat keputusan berbanding dengan jenis pengklasifikasian lain. *Naive Bayes Classifier* sangat populer dalam deteksi ancaman keamanan jaringan karena kinerja yang baik dan kecepatan komputasi yang tinggi. Dengan menggunakan metode ini, dapat dilakukan klasifikasi pada data yang masuk ke jaringan dan mengidentifikasi apakah data tersebut merupakan ancaman atau tidak.[13]

Sebagai data pendukung untuk penerapan metode ini, digunakan *dataset* IoT 2023 yang dikembangkan oleh *Canadian Institute for Cybersecurity (CIC)* di Universitas New Brunswick (UNB), Kanada. *Dataset* ini merekam aktivitas serangan DDoS pada jaringan dengan protokol TCP/IP dan UDP, yang dirancang khusus untuk

mendeteksi ancaman keamanan dalam lingkungan IoT. *Dataset* ini mencakup 238.644 baris data dan 48 atribut, diantaranya *flow_duration*; *Header_Length*; *Protocol Type*; *Duration*; *Rate* ; *Srate*; *Drate*; *fin_flag_number*; *syn_flag_number*; *rst_flag_number*; *psh_flag_number*; *ack_flag_number*; *ece_flag_number*; *cwr_flag_number*; *ack_count*; *syn_count*; *fin_count*; *urg_count*; *rst_count*; HTTP, HTTPS, DNS; *Telnet*; SMTP, SSH, IRC, TCP, UDP, DHCP, ARP, ICMP, Ipv, LLC, *Tot sum*, *Min*, *Max*, *AVG*, *Std*, *Tot size*, *IAT*, *Number*, *Magnitue*, *Radius*, *Covariance*, *Variance*, dan *Weight label*.

Dataset ini memberikan gambaran realistis mengenai lalu lintas jaringan yang mengalami serangan DDoS, dengan tujuan membanjiri jaringan untuk menghabiskan sumber daya yang tersedia. Dalam konteks IoT, data ini sangat berguna untuk mengembangkan dan mengevaluasi algoritma deteksi, seperti algoritma *Naive Bayes* yang diterapkan dalam penelitian ini. Algoritma ini membantu dalam mengidentifikasi pola serangan, yang penting untuk meningkatkan keamanan siber di sektor jaringan komputer. Berdasarkan uraian di atas maka penelitian akan berfokus pada penerapan klasifikasi dengan metode *Naive Bayes* untuk deteksi serangan DDoS pada *Internet of Things* (IoT). Dengan judul penelitian **“DETEKSI SERANGAN DDOS PADA INTERNET OF THINGS (IoT) MENGGUNAKAN ALGORITMA NAIVE BAYES”**.

1.2 RUMUSAN MASALAH

Berdasarkan penelitian yang sudah ada, metode *Naive Bayes* belum sepenuhnya dimanfaatkan dalam mendeteksi ancaman pada jaringan yang kompleks seperti IoT. Selain itu, tingkat akurasi yang dicapai masih memiliki peluang peningkatan, dan penerapan *Naive Bayes* pada lingkungan IoT belum optimal. Oleh karena itu, penelitian ini difokuskan untuk meningkatkan akurasi deteksi serangan DDoS serta mengevaluasi kinerja metode *Naive Bayes* dalam konteks IoT.

Berdasarkan latar belakang yang telah dipaparkan, maka terdapat beberapa pertanyaan penelitian, yaitu:

1. Bagaimana menerapkan algoritma *Naive Bayes* untuk mendeteksi serangan DDoS pada *Internet of Things* (IoT)?
2. Bagaimana kinerja atau performa *Naive Bayes* dalam mendeteksi serangan DDoS pada IoT?

1.3 BATASAN MASALAH

Agar penelitian ini dapat berjalan dengan baik dan terarah, dibuatlah batasan terhadap ruang lingkup penelitian sebagai berikut:

1. Menggunakan metode *Naive Bayes* untuk mendeteksi serangan DDoS dalam lingkungan *Internet Of Things* (IoT).
2. Penelitian ini menggunakan *dataset* IoT 2023 dari *Canadian Institute for Cybersecurity* (CIC), yang berisi data serangan DDoS di lingkungan IoT dengan jumlah data sebanyak 238.644 baris dan 48 atribut.

3. Berfokus mendeteksi serangan DDoS pada *Internet Of Things* (IoT).
4. Bahasa pemrograman yang digunakan adalah *Python* dengan menggunakan *Google Collab*.
5. Pengukuran performa untuk mencari nilai *Accuracy*, *TPR*, *F1-Score*, *Recall*, dan *ROC*.

1.4 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini meliputi :

1. Mengimplementasikan algoritma *Naive Bayes* untuk mendeteksi serangan DDoS pada *Internet of Things* (IoT).
2. Mengevaluasi kinerja *Naive Bayes* dalam *Traffic Anomaly* pada serangan DDoS pada *Internet of Things* (IoT).

1.5 MANFAAT PENELITIAN

Manfaat yang didapat dari penelitian yaitu:

1. Penelitian ini menghasilkan solusi berbasis algoritma *Naive Bayes* untuk mengidentifikasi *Traffic Anomaly* pada *Internet of Things* (IoT).
2. Hasil penelitian ini dapat digunakan sebagai acuan bagi pengembang dan penyedia layanan *Internet of Things* (IoT) untuk meningkatkan sistem keamanan jaringan mereka melalui implementasi algoritma *Naive Bayes* sebagai alat deteksi dini yang efektif terhadap serangan DDoS berbasis *Traffic Anomaly*.

1.6 SISTEMATIKA PENULISAN

Penulisan karya ilmiah ini terdiri dari lima bab yang disusun secara sistematis untuk memberikan pemahaman yang komprehensif mengenai penelitian yang dilakukan.

BAB I : PENDAHULUAN

Memaparkan latar belakang masalah yang melandasi penelitian ini, tujuan penelitian, rumusan masalah, manfaat penelitian, dan sistematika penulisan. Pada bagian ini, penulis menjelaskan pentingnya penelitian terhadap keamanan *Internet of Things* (IoT), terutama dalam menghadapi serangan *Distributed Denial-of-Service* (DDoS).

BAB II : TINJAUAN PUSTAKA

Mengulas teori-teori dan hasil penelitian sebelumnya yang relevan dengan topik *Internet of Things* (IoT) dan keamanan siber. Bab ini mencakup penjelasan mengenai konsep dasar *Distributed Denial-of-Service* (DDoS), metode dan teknik keamanan, serta berbagai serangan yang sering terjadi pada sistem *Internet of Things* (IoT). Penulis juga membahas teknologi kecerdasan buatan dan *machine learning*, khususnya *Naive Bayes* (NB), yang digunakan dalam mendeteksi dan mencegah serangan.

BAB III : METODOLOGI PENELITIAN

Dalam bab ini menjelaskan metodologi yang digunakan penulis dan merinci kerangka penelitian, termasuk desain penelitian,

populasi dan sampel, teknik pengumpulan data, dan teknik analisis data serta data penelitian.

BAB IV : HASIL DAN PEMBAHASAN

Dalam bab ini penulis memaparkan analisis data yang diperoleh selama penelitian dan hasil dari analisis tersebut. Bab ini juga mencakup interpretasi hasil serta diskusi mengenai temuan penelitian yang diperoleh dari data yang telah dianalisis, serta membahas implikasi dari temuan tersebut dalam konteks keamanan *Internet of Things* (IoT).

BAB V : PENUTUP

Dalam bab ini penulis memberikan kesimpulan dari hasil penelitian dan menyampaikan saran-saran yang relevan untuk penelitian selanjutnya dan untuk praktik di lapangan dalam meningkatkan keamanan *Internet of Things* (IoT).