BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Saat ini, berkat kemajuan teknologi, perangkat elektronik dapat terhubung ke internet dan saling berkomunikasi secara langsung. Akibat dari perkembangan ini, munculah istilah baru dalam jaringan komunikasi data, yaitu Internet of Things (IoT)[1]. IoT memfasilitasi kemudahan dan memperkaya interaksi manusia dengan lingkungan, sosial, dan objek sehari-hari. Penerapannya sudah mencakup berbagai bidang, mulai dari kesehatan, otomotif, hiburan, hingga industri[2].

Inovasi perangkat IoT telah merubah berbagai segi kehidupan manusia, contohnya kota pintar, rumah pintar, jalan pintar, dan industri pintar, yang memanfaatkan internet untuk memantau informasi yang dibutuhkan. Namun, jaringan IoT yang kompleks itu sendiri menghadirkan tantangan untuk menjaga keamanan jaringan. Kaspersky menyatakan [3], pada kuartal pertama 2019, terjadi lebih dari 100 juta serangan terhadap IoT, jumlah ini meningkat tujuh kali lipat dibandingkan periode yang sama pada 2018 berdasarkan metode pengujian penetrasi.

Salah satu botnet besar yang paling berdampak adalah *mirai*, yang terdeteksi untuk pertama kalinya pada bulan agustus 2016[4]. *Mirai* adalah sebuah *malware* yang dirancang khusus untuk mengeksploitasi kerentanan pada perangkat *Internet Of Things* (IoT). Dimana *mirai* adalah botnet yang paling terkenal dalam

beberapa tahun terakhir, telah mampu mengeksploitasi kumpulan perangkat rentan ini untuk melakukan serangan DDoS yang besar[5]. Namun, dengan upaya bersama dari semua pemangku kepentingan keamanan IoT dapat ditingkatkan dan risiko serangan mirai dapat dikurangi dengan mengunakan IDS[6]. *Intrusion Detection System* (IDS) adalah salah satu solusi keamanan jaringan yang efektif dan banyak digunakan dalam jaringan saat ini.

Dimana, IDS merupakan suatu kemampuan perangkat keras untuk mencari, menganalisis, dan mendeteksi aktivitas yang mencurigakan[7]. Meskipun Intrusion Detection System (IDS) telah dipasang sebagai perangkat keamanan informasi, serangan tetap berpotensi menembus jaringan kita. Sistem strategis tentu akan menjadi sasaran menarik oleh para *attacker.* Dengan melakukan upaya penyusupan, baik secara coba-coba maupun dengan sengaja untuk tujuan jahat, ke dalam sistem.[8].

Mengingat sifat dari serangan ini, deteksi dini dan respons yang cepat terhadap serangan *mirai* sangat penting untuk menjaga keamanan perangkat IoT, memberikan solusi untuk menggunakan teknik *machine learning* untuk mendeteksi perangkat IoT yang terinfeksi. Penelitian yang dilakukan oleh M. Agus Syamsul Arifin dkk[9] dengan menerapkan teknik *Machine Learning(ML)* menggunakan algoritma *decision tree* dan *random forest* untuk deteksi serangan terhadap *internet of things(IoT)* dengan *accuracy* 99,90% dan 99,94% dimana algoritma *random forest* merupakan metode dengan akurasi paling tinggi.

Kemudian pada penelitian yang di lakukan oleh Julius Chandra dkk yang menerapkan teknik *Machine Learning (Ml)* seperti *Naive Bayes* deteksi serangan terhadap *internet of things(IoT),* dimana hasil akurasinya adalah *All-out attack* mencapai 99,10%, yang menunjukkan bahwa *Naïve Bayes* memiliki tingkat akurasi yang sangat baik dalam klasifikasi[10]. Dari beberapa penelitian menunjukkan bahwa berbagai metode yang telah digunakan untuk mendeteksi serangan *port scanning* dan *malware* memiliki akurasi yang baik.

Namun, dengan demikian metode *Naïve Bayes* dikenal sebagai metode klasifikasi probabilistik sederhana yang menghitung probabilitas berdasarkan frekuensi dan kombinasi nilai dalam dataset yang diberikan[11]. Algoritma *naïve bayes* memprediksi peluang di masa depan berdasarkan pengalaman sebelumnya, sehingga dikenal sebagai penerapan *Teorema Bayes*[12]. Dengan demikian, terlihat bahwa salah satu metode yang relatif sederhana yang memiliki tingkat akurasi yang tinggi dan dapat menangani data dalam jumlah besar[13] dalam mendeteksi serangan mirai pada lingkungan IoT adalah *naive bayes*.

Tetapi, penggunaan *naïve bayes* dalam mendeteksi serangan mirai pada jaringan IoT masih belum dimaksimalkan. Oleh karena itu, penelitian ini berfokus pada penerapan dan pengujian algoritma *naive bayes* untuk mendeteksi serangan mirai pada jaringan IoT, dengan tujuan meningkatkan akurasi deteksi sekaligus menambah alternatif metode keamanan siber untuk sistem berbasis IoT.

Sebagai data pendukung untuk penerapan metode ini, digunakan dataset CIC IoT *dataset* 2023 dari *Canadian Institute for Cybersecurity* yang

dikembangkan oleh Universitas New Brunswick (UNB), Kanada. Pada penelitian ini menggunakan *dataset mirai*(serangan) mencakup 33.597 *records* data dan 39 atribut dan *dataset benign*(normal) mencakup 362.361 *records* data dan 40 atribut. Dalam konteks IoT, dataset 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.

Dari uraian di atas, maka penelitian akan berfokus pada penerapan klasifikasi dengan metode *naive bayes* untuk deteksi serangan mirai pada jaringan *Internet Of Things* (IoT). Dengan judul penelitian **"DETEKSI SERANGAN MIRAI TERHADAP JARINGAN *INTERNET OF THINGS* (IOT) MENGGUNAKAN ALGORITMA *NAIVE BAYES*".**

1.2 RUMUSAN MASALAH

Menurut penelitian yang sudah ada, metode *naive bayes* belum sepenuhnya dimanfaatkan dalam mendeteksi serangan mirai pada jaringan yang kompleks seperti IoT. Selain itu, tingkat akurasi yang dicapai masih memiliki peluang peningkatan, dan penerapan *naive bayes* pada lingkungan IoT masih belum mencapai hasil terbaik. Karena hal tersebut, riset ini berpusat pada pengembangan akurasi deteksi serangan *mirai* serta evaluasi kinerja metode *naïve bayes* dalam lingkungan IoT.

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

1. Bagaimana cara mendeteksi serangan *mirai* terhadap jaringan IoT menggunakan algoritma *naive bayes*?
2. Bagaimana performa *naïve bayes* dalam mendeteksi serangan *mirai* pada jaringan IoT?

1.3 BATASAN MASALAH

Agar pembahasan lebih terarah dan sesuai dengan tujuan, diperlukan pembatasan masalah dalam suatu topik. Oleh karena itu, batasan-batasan yang ditetapkan dalam penelitian ini adalah:

1. Mengembangkan model deteksi serangan *mirai* terhadap jaringan IoT menggunakan algoritma *naive bayes*.
2. Berfokus mengidentifikasi serangan *mirai* pada jaringan *Internet Of Things* (IoT).
3. Sumber data yang digunakan dalam penelitian ini berasal dari https://www.unb.ca/cic/datasets/iotdataset-2023.html. Dengan nama dataset *Mirai-greeth_flood.pcap.csv* yang mencakup 33.597 *records* data dan 39 atribut/fitur dan *dataset BenignTraffic.pcap.csv* yang mencakup 362.361 *records* data dan 40 atribut.
4. Bahasa pemrograman yang digunakan adalah *Python* dengan menggunakan *Google Colab*.

5. Pengukuran performa untuk mencari nilai *Accuracy, Presisi, F1-Score, Recall.*

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Berdasarkan latar belakang yang telah diuraikan, penelitian ini bertujuan untuk mengembangkan metode yang efektif dalam mengidentifikasi dan mengklasifikasikan serangan Mirai pada jaringan Internet of Things (IoT) dengan menggunakan algoritma Naive Bayes. Berikut adalah rincian tujuan penelitian:

1. Menerapkan algoritma *naive bayes* mengidentifikasi serangan *mirai* dalam perangkat *Internet Of Things* (IoT).
2. Mengevaluasi kinerja *naive bayes* untuk mengidentifikasi serangan *mirai* pada jaringan *Internet Of Things* (IoT).

1.4.2 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam memperkuat keamanan jaringan IoT dan melindungi perangkat dari ancaman siber yang semakin canggih. Adapun manfaat dari penelitian ini adalah:

1. Memberi peran dalam meningkatkan keamanan jaringan IoT terhadap ancaman serangan dan pengembangan metode *machine learning*, khususnya dalam deteksi serangan *mirai*.
2. Menjadi acuan penelitian di bidang keamanan siber dalam jaringan IoT, terkhusus serangan *mirai.*

1.5 SISTEMATIKA PENULISAN

Penulis menyajikan sistematika penulisan untuk memberikan gambaran yang jelas mengenai alur pembahasan dalam laporan penelitian ini:

BAB I : PENDAHULUAN

Bab ini memuat pengantar penelitian, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan alur penulisan. Latar belakang mengemukakan alasan di balik penelitian ini, sementara rumusan masalah merinci masalah yang akan diselesaikan. Tujuan penelitian menjelaskan hasil yang diinginkan, dan manfaat penelitian menguraikan kontribusi yang diharapkan dari studi ini. Batasan masalah menentukan batasan dan lingkup penelitian.

BAB II : LANDASAN TEORI

Penulis memaparkan berbagai definisi teoretis yang mendukung penelitian dalam bab ini, yang diambil dari buku dan jurnal, guna memperjelas pemahaman dan memberikan landasan teoretis yang kuat untuk menjawab permasalahan penelitian.

BAB III : METODOLOGI PENELITIAN

Bab ini menyajikan penjelasan mengenai metodologi yang digunakan oleh penulis, termasuk kerangka penelitian, cara pelaksanaan penelitian, teknik pengumpulan data, dan pendekatan pengembangan model deteksi serangan Mirai menggunakan Naïve Bayes, serta perangkat lunak yang mendukung pengembangan model tersebut.

BAB IV : ANALISIS DAN HASIL

Di bagian ini, penulis menguraikan hasil implementasi model Naive Bayes, mencakup hasil pengujian performa model yang dilakukan selama penelitian, serta tingkat akurasi yang dicapai. Bab ini juga membahas interpretasi dari hasil tersebut dan diskusi mengenai temuan penelitian.

BAB V : PENUTUP

Di bagian ini, penulis merangkum temuan penelitian dan memberikan rekomendasi yang relevan untuk penelitian lanjutan atau penerapan praktis dari hasil yang diperoleh.