BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) terus berkembang dalam segi komunikasi antar perangkat, baik *software* maupun *hardware*. IoT membuat beragam perangkat dapat terhubung bersama ke internet. Selain itu, IoT merupakan koneksi unik perangkat komputasi yang dapat diidentifikasi, tertanam dan dapat mengirimkan data melalui jaringan tanpa interaksi antar pengguna atau perangkat. Jumlah perangkat yang terhubung ke internet dengan IoT semakin hari semakin berkembang. Teknologi IoT bisa menjadi sesuatu yang berharga dalam hal inovasi tetapi juga dapat menjadi ancaman keamanan siber yang signifikan bagi sistem yang rentan. Situasi ini adalah potensi risiko besar dalam hal keamanan siber, karena banyak titik masuk yang mungkin memiliki kerentanan keamanan. Kerentanan dalam rantai keamanan sistem dapat menimbulkan risiko keamanan untuk keseluruhan sistem dan memberikan peluang bagi penyerang untuk melancarkan aksinya. Terutama infrastruktur penting yang harus dilindungi dari risiko keamanan siber yang sangat besar (Da & Zekeriya Gündüz, 2019).

Salah satu tantangan yang harus diatasi untuk mendorong implementasi IoT secara luas adalah faktor keamanan. IoT merupakan sebuah sistem yang majemuk. Kemajemukannya bukan hanya karena keterlibatan berbagai entitas seperti data, mesin, RFID, sensor dan lain-lain, tetapi juga karena melibatkan berbagai peralatan dengan kemampuan komunikasi dan pengolahan data. Banyaknya entitas dan data

yang terlibat, membuat IoT menghadapi resiko keamanan yang dapat mengancam dan membahayakan penggunanya. Ancaman ini utamanya dilakukan dengan cara memungkinkan orang yang tidak berhak untuk mengkases data dan menyalahgunakan informasi personal, memfasilitasi serangan terhadap sistem yang lain, serta mengancam keselamatan personal penggunanya (Meutia, 2015). Jumlah penggunaan perangkat IoT (*Internet of Things*) telah meningkat dan tersebar luas. Ancaman keamanan pada perangkat IoT juga meningkat. Berbagai serangan siber dapat dilakukan pada perangkat IoT, mulai dari mengambil hak akses, merusak data, mencuri informasi penting, dan merekam aktivitas pribadi pengguna saat menggunakan perangkat IoT. Serangan siber ini memasuki sistem melalui *malware* yang berhasil ditanam di perangkat IoT (Jeremias Lewi Engel et al., 2020).

Malware merupakan perangkat lunak (*software)* yang memiliki tujuan negatif, seperti merusak data, mencuri informasi penting, mengganggu kinerja perangkat, dan mengambil alih sistem, ancaman ini terus meningkat setiap tahunnya. Pada tahun 2019 serangan siber menggunakan *malware* di Indonesia merupakan yang tertinggi di Asia Pasifik (KataData, 2020).

Salah satu aktivitas mencurigakan dari *malware* adalah penggunaan lalu lintas jaringan yang dapat dimanfaatkan sebagai media untuk mengirimkan informasi rahasia, informasi rekening bank, pesan pribadi, dan kata sandi. *Malware* juga bisa memanfaatkan lalu lintas jaringan sebagai pintu belakang untuk dapat dimasuki oleh *malware* lainnya (Jeremias Lewi Engel et al., 2020).

Penelitian berjudul *"Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics"* yang

dilakukan oleh Arther S dkk (2020) menyebutkan bahwa algoritma yang telah di evaluasi yaitu *K-Nearest Neighbor*, *Decision Tree, Logistic Regression*, dan *Random Forest* dapat disimpulkan bahwa algoritma K-NN memiliki performa yang paling baik di antara algoritma lainnya dengan hasil 95.51% *accuracy*, 89.42% *recall*, 89.42% *precision*, dan 0.212 RMSE untuk hasil *independent* sedangkan untuk hasil 10 *fold cross validation* memiliki hasil 93.61% *accuracy*, 85.05% *recall*, 85.25% *precision*, dan 0.251 RMSE dalam mendeteksi *malicious* dan *benign website* (Sandag et al., 2018).

Algoritma *K-Nearest Neighbour* (K-NN) adalah algoritma *supervised* yang memiliki hasil *query instance* baru yang didapat dengan klasifikasi dengan nilai mayoritas dari kategori. Algoritma K-NN memiliki tujuan untuk mengklasifikasi obyek baru berdasarkan atribut data dan *training sample* (Yudhana & Agus Jaka Sri Hartanta, 2020). Berdasarkan hasil paparan permasalahan maka fokus penelitian pada klasifikasi serangan *malware* terhadap lalu lintas jaringan IoT menggunakan algoritma *K-Nearest Neighbour* (K-NN).

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka rumusan permasalahannya adalah sebagai berikut:

1. Bagaimana melakukan klasifikasi serangan *malware* terhadap lalu lintas jaringan IoT menggunakan algoritma *K-Nearest Neighbour* (K-NN)?

2. Bagaimana menguji tingkat akurasi menggunakan algoritma *K-Nearest Neighbour* (K-NN) terhadap dataset *aposemat IoT-23*?

1.3 Batasan Masalah

Mengingat banyaknya perkembangan yang bisa ditemukan dalam permasalahan yang telah didefinisikan pada rumusan masalah, maka perlu adanya batasan-batasan masalah yang jelas. Adapun batasan-batasan permasalahannya adalah sebagai berikut:

1. Dataset *aposemat iot-23* di unduh pada *website* stratosphereips.org.
2. Pengunduhan *dataset* dilakukan pada 20 Januari 2020.
3. Jumlah *dataset* yang didapatkan pada *website* stratosphereips.org sebanyak 23 *dataset*, tetapi yang layak digunakan hanya 20 *dataset* karena 3 *dataset* lainnya tidak diinfeksi dengan serangan *malware*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, maka tujuan dari penelitian ini adalah untuk:

1. Melakukan klasifikasi terhadap dataset *aposemat iot-23* dengan menggunakan algoritma *K-Nearest Neighbour* (K-NN) serta *tools jupyter lab.*
2. Membagi dataset menjadi data *training* dan data *testing* lalu digunakan algoritma *K-Nearest Neighbour* (K-NN) untuk proses klasifikasi atau *training*

model, nilai akurasi akan didapatkan setelah proses klasifikasi atau *training* model.

1.5 Manfaat Penelitian

Berikut merupakan manfaat dari penelitian ini :

1. Dapat memprediksi serangan *malware* pada data lalu lintas jaringan IoT kedalam *benign* dan *malicious*.
2. Mengurangi data *missing value* pada proses *training* sehingga saat melakukan pengujian menggunakan algoritma *K-Nearest Neighbour* (K-NN) tidak banyak data yang *missing value*.

1.6 Metodologi Penelitian

Metodologi penelitian menjelaskan mengenai waktu dan tempat penelitian, tahapan atau prosedur penelitian, jenis penelitian, pendekatan penelitian, objek penelitian, serta variabel penelitian. Tahapan penelitian terdiri dari pengumpulan data, analisis permasalahan dan pencarian solusi, implementasi solusi, serta penarikan kesimpulan. Berikut merupakan penjelasan dari proses tahapan penelitian:

1. Tahap pengumpulan data, berisi telaah jurnal dan pencarian dataset.
2. Tahap analisis permasalahan dan pencarian solusi, berisi tentang analisis berbagai masalah yang sifatnya aktual dan faktual khususnya terkait serangan *malware* serta cara mengetahui sifat atau tipe serangannya.

3. Tahap implementasi solusi, berisi langkah-langkah guna menyelesaikan permasalahan yang dihadapi.
4. Tahap penarikan kesimpulan, merupakan tahapan akhir dari penelitian dimana hasil penelitian tersebut berupa model yang sudah melewati proses klasifikasi atau *training* dengan menggunakan *dataset* lalu lintas jaringan IoT yang bisa memprediksi apakah termasuk lalu lintas jaringan IoT bersifat *benign* atau *malicious*.

1.7 Sistematika Penulisan

Sistematika penulisan dibuat untuk mempermudah dalam menyusun penelitian. Sistematika penulisan yang digunakan pada penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi kajian dari penelitian terdahulu, beberapa teori yang ada, literatur review, penelitian yang relevan, serta matriks penelitian yang diperoleh berbagai sumber literatur seperti jurnal dan buku.

BAB III METODOLOGI PENELITIAN

Metodologi penelitian berisi waktu dan tempat penelitian, tahapan atau prosedur penelitian, jenis penelitian, pendekatan penelitian, objek penelitian serta variabel penelitian yang menggambarkan jalannya proses penelitian dari awal hingga akhir.

BAB IV HASIL DAN PEMBAHASAN

Tahap awal dari bab ini adalah proses pengumpulan data melalui studi literatur dan pencarian dataset terkait serangan *malware* terhadap lalu lintas jaringan IoT. Setelah data diperoleh, kemudian data tersebut dilakukan analisis terhadap permasalahan yang dihadapi dan bagaimana cara pemecahanan masalahnya yakni dengan menerapkan algoritma *K-Nearest Neighbour* (K-NN) untuk klasifikasi serangan *malware* terhadap lalu lintas jaringan IoT. Tahap akhir dari bab ini adalah penarikan kesimpulan dimana kesimpulan tersebut berisi nilai akurasi dari pemrosesan algoritma *K-Nearest Neighbour* (K-NN) terhadap serangan *malware* terhadap lalu lintas jaringan IoT beserta kategorinya bersifat *benign* atau *malicious*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan secara keseluruhan yang merupakan jawaban atas permasalahan yang dihadapi. Bagian saran berisikan *future work* yang berpotensi untuk dijadikan bahan dasar penelitian berikutnya.