BAB I
PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Internet of Things (IoT) adalah teknologi yang sangat populer di seluruh dunia, yang membantu menghubungkan objek-objek seperti sensor, kendaraan, instrumen rumah sakit, industri, dan peralatan rumah tangga melalui internet. Perangkat pintar yang ringkas merupakan bagian penting dari IoT [1]. Perangkat berbasis teknologi *Internet of Things* (IoT) saat ini telah banyak dimanfaatkan sebagai salah satu upaya meningkatkan pelayanan kesehatan. IoT dan integrasinya di bidang kesehatan diprediksi akan mendominasi tatanan dalam sistem kesehatan di masa depan [2]. IoT memungkinkan pengiriman data melalui jaringan tanpa interaksi manusia, serta mendukung identifikasi, pelacakan, dan pemantauan objek secara otomatis dan *real-time* dari jarak jauh. Teknologi ini telah banyak diterapkan dalam sektor kesehatan dan dikenal sebagai *Internet of Medical Things* (IoMT) [3].

Internet of Medical Things (IoMT) adalah *platform* cerdas yang terdiri dari sensor dan perangkat elektronik untuk memperoleh sinyal biomedis pasien, dilengkapi prosesor, perangkat jaringan, penyimpanan data, dan platform visualisasi berbasis kecerdasan buatan guna mendukung diagnosis dokter. Sistem pemantauan kesehatan jarak jauh berbasis IoMT kini dikembangkan sebagai alternatif untuk meningkatkan layanan kesehatan di rumah sakit [4]. IoMT menghubungkan pasien dan dokter melalui perangkat medis, memungkinkan pengumpulan serta pengiriman data medis secara aman, dan memfasilitasi

pemantauan kesehatan nirkabel yang membantu mengurangi rawat inap serta biaya kesehatan [5]. Namun, dengan berkembangnya penggunaan perangkat IoMT, muncul pula berbagai ancaman terhadap keamanan dan integritas data medis. Salah satu ancaman yang paling signifikan adalah serangan *reconnaissance* (recon), yang merupakan tahap awal dalam suatu serangan siber [6].

Serangan *Reconnaissance* adalah fase persiapan sebelum penyerang melakukan serangan, dengan tujuan utama mengumpulkan informasi sebanyak mungkin mengenai target. Teknik ini mencakup pemindaian jaringan, baik melalui jaringan internal maupun eksternal, yang dilakukan tanpa izin [7]. *Reconnaissance* merupakan upaya untuk memperoleh sebanyak mungkin informasi terkait target serangan. Contoh aktifitas ini adalah pencarian melalui *search engine*, *social website*, enumerasi dan *scanning* pada infrastruktur sistem informasi [8]. Serangan ini dapat dilakukan dengan dua pendekatan yaitu pasif dan aktif. Pengintaian pasif dilakukan dengan cara yang lebih ringan dan tidak mendalam tanpa memberi tahu target, sementara pengintaian aktif melibatkan pendekatan yang lebih mendalam, yang mungkin memberi tahu target bahwa serangan sedang terjadi [9].

Dampak serangan *reconnaissance* sangat signifikan dalam konteks keamanan siber karena serangan ini memungkinkan penyerang untuk mengidentifikasi kelemahan sistem secara mendalam, sehingga meningkatkan kemungkinan keberhasilan serangan lebih lanjut. Pengintaian, baik pasif maupun aktif, memberi informasi mengenai titik rentan target, seperti *port* terbuka, konfigurasi jaringan, dan perangkat yang tidak terlindungi [10]. Serangan *reconnaissance* dapat dilakukan dalam bentuk yang lebih sulit dideteksi, berkat

perkembangan teknologi dan teknik seperti penggunaan perangkat IoT dan alat pemindai otomatis. Hal ini memungkinkan penyerang untuk memperoleh informasi secara lebih cepat dan efektif, tanpa harus berinteraksi langsung dengan korban [11]. Selain itu, serangan *reconnaissance* seringkali tidak langsung mengarah pada kerusakan yang terlihat, sehingga sulit mendeteksi ancaman sebelum serangan utama terjadi. Pengintaian yang dilakukan dengan seksama memberikan keuntungan strategis besar bagi penyerang, mengurangi kemungkinan keberhasilan upaya pertahanan organisasi target [12].

Salah satu cara untuk mengamankan sistem adalah dengan melakukan pengamanan pada infrastruktur jaringan. Selain itu, diperlukan juga pemantauan terhadap infrastruktur jaringan instansi pemerintah untuk memperoleh informasi mengenai ancaman dan serangan yang keluar masuk jaringan serta data terkini mengenai kondisi *host* atau server di dalam jaringan [13]. Sebagai perlindungan protokol komunikasi, protokol enkripsi WPA2 yang banyak digunakan untuk protokol enkripsi. Pengguna dapat mengakses *router* hanya dengan menggunakan kunci. Biasanya driver dapat dianggap sebagai bagian dari sistem operasi. Setelah mendaftar dengan *registry*, antarmuka driver komunikasi jaringan yang sesuai dapat dipanggil oleh program aplikasi komunikasi [14]. Salah satu metode dalam keamanan jaringan adalah dengan mendeteksi ancaman menggunakan pendekatan berbasis signature atau anomali. Pendekatan berbasis *signature* bergantung pada basis data tanda-tanda serangan yang diketahui untuk mengidentifikasi aktivitas mencurigakan. Namun, metode ini memiliki kelemahan dalam mendeteksi serangan baru jika *signature* belum tersedia atau basis datanya kedaluwarsa [15].

Untuk mendeteksi serangan pada jaringan internet telah dilakukan beberapa penelitian antara lain, yang di lakukan oleh F. Febriansyah, Z. Asti Dwiyanti, dan Diash Firdaus pada tahun 2023 dimana mendeteksi serangan *low rate* DDoS pada jaringan tradisional menggunakan *machine learning* dengan Algoritma *Decision Tree* mendapatkan hasil akurasi sebesar 99,74% [16]. Selain itu, penelitian yang dilakukan oleh N. Khairunnisa pada tahun 2024 dimana mendeteksi serangan pada protokol jaringan menggunakan Algoritma C4.5 mendapatkan hasil akurasi sebesar 91,2% [17]. Kemudian pada penelitian yang di lakukan oleh M. Pramana, Endang Setyati, and F.X. Ferdinandus pada tahun 2021 dimana mendeteksi serangan DoS dengan Algoritma *Decision Tree* C4.5 mendapatkan hasil akurasi sebesar 90,68% [18]. Penelitian lainnya yang di lakukan oleh E. Esterlin, V. Sihombing, and A. Putra Juled pada tahun 2024 dimana mendeteksi serangan dalam jaringan dengan Algoritma pohon keputusan C4.5 mendapatkan hasil akurasi sebesar 90% [19]. Dari beberapa penelitian menunjukkan bahwa metode Algoritma C4.5 mendapatkan akurasi yang baik dalam mendeteksi serangan pada jaringan. Oleh karena itu, penelitian ini berfokus pada penerapan dan pengujian Algoritma C4.5 untuk mendeteksi serangan pada jaringan.

Dengan demikian, terlihat bahwa metode Algoritma C4.5 sangat efektif dalam mendeteksi serangan pada jaringan. *Decision tree* adalah teknik klasifikasi yang diakui secara luas dan sangat efektif. Fakta-fakta besar direpresentasikan sebagai aturan dengan pendekatan *decision tree*, yang membuat aturan tersebut mudah dimengerti oleh orang-orang. Metode *decision tree* memiliki algoritma, algoritma C4.5 adalah salah satu dari algoritma yang memiliki *decision tree* [20].

Algoritma C4.5 adalah salah satu jenis pohon keputusan yang paling populer. Pohon keputusan berguna untuk eksplorasi data, mencari hubungan tersembunyi antara beberapa *variabel* input kandidat dan variabel target. Algoritma C4.5 dapat menangani data digital dan diskrit menggunakan rasio *gain*. Objek menggunakan konsep *entropy* [21]. Sebagai data pendukung untuk penerapan metode ini, digunakan dataset IoMT 2024 dari *Canadian Institute for Cybersecurity (CIC)* yang dikembangkan oleh Universitas *New Brunswick (UNB)*, Kanada. Dataset ini mencakup rekaman serangan *reconnaissance*, yang secara khusus ditujukan untuk mendeteksi ancaman keamanan dalam lingkungan IoMT. Dataset ini terdiri dari 299.335 baris data dengan 46 atribut, yaitu *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, rst count, HTTP, HTTPS, DNS, TELNET, SMTP, SSH, IRC, TCP, UDP, DHCP, ARP, ICMP, IGMP, IPv, LLC, tot sum, min, max, AVG, std, tot size, IAT, number, magnitue, radius, covariance, variance, weight,* dan *class.* Dataset ini memberikan gambaran realistis mengenai lalu lintas jaringan yang mengalami serangan *reconnaissance*, dengan tujuan mengumpulkan informasi sebanyak mungkin tentang target sebelum melancarkan serangan lebih lanjut. Dalam konteks IoMT, data ini sangat berguna untuk mengembangkan dan mengevaluasi algoritma deteksi, seperti Algoritma C4.5 yang diterapkan dalam penelitian ini. Algoritma ini membantu dalam mengidentifikasi pola serangan, yang penting untuk meningkatkan keamanan siber di sektor kesehatan.

Dari uraian di atas, maka penelitian akan berfokus pada penerapan klasifikasi dengan metode Algoritma C4.5 untuk deteksi serangan *reconnaissance* pada lingkungan *Internet Of Medical Things* (IoMT). Dengan judul penelitian **"DETEKSI SERANGAN RECONNAISSANCE PADA LINGKUNGAN INTERNET OF MEDICAL THINGS (IOMT) MENGGUNAKAN ALGORITMA C4.5".**

1.2 RUMUSAN MASALAH

Berdasarkan penelitian yang sudah ada, metode *Algoritma C4.5* belum sepenuhnya dimanfaatkan dalam mendeteksi ancaman pada jaringan yang kompleks seperti IoMT. Penelitian [16] mengatakan bahwa tingkat akurasi yang dicapai masih memiliki peluang peningkatan. Oleh karena itu, penelitian ini difokuskan untuk meningkatkan akurasi deteksi serangan pada jaringan serta mengevaluasi kinerja metode *Algoritma C4.5* dalam konteks IoMT.

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

1. Bagaimana mengoptimalkan metode Algoritma C4.5 untuk meningkatkan akurasi dalam mendeteksi serangan *reconnaissance* pada lingkungan IoMT?
2. Bagaimana performa Algoritma C4.5 dalam mendeteksi serangan *reconnaissance* pada lingkungan IoMT?

1.3 BATASAN MASALAH

Agar nantinya permasalahan sesuai dengan rumusan masalah dan tidak meluas, permasalahan perlu dibatasi sebagai berikut :

1. Menggunakan metode Algoritma C4.5 untuk mendeteksi serangan *reconnaissance* dalam lingkungan *Internet Of Medical Things* (IoMT).
2. Data yang digunakan dalam penelitian ini adalah serangan *reconnaissance* pada lingkungan *Internet Of Medical Things* (IoMT).
3. Berfokus mendeteksi serangan *reconnaissance* pada lingkungan *Internet Of Medical Things* (IoMT).
4. Penelitian ini menggunakan dataset IoMT 2024 dari *Canandian Institute for Cybersecurity (*CIC), yang berisi data serangan *reconnaissance* di lingkungan IoMT dengan jumlah data sebanyak 299.335 baris data dan 46 atribut.
5. Bahasa pemrograman yang digunakan adalah *Python* dengan menggunakan *Google Colab.*
6. Pengukuran performa untuk mencari nilai *Accuracy*, *Precision* , *F1-Score*, *Recall*, AUC dan TPR.

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Menerapkan Algoritma C4.5 untuk mendeteksi serangan *reconnaissance* dalam lingkungan *Internet Of Medical Things* (IoMT).

2. Mengevaluasi kinerja Algoritma C4.5 dalam mengklasifikasi lalu lintas jaringan dan mendeteksi adanya serangan *reconnaissance* yang terjadi pada lingkungan *Internet Of Medical Things* (IoMT).
3. Menghasilkan model klasifikasi yang dapat memberikan informasi akurat dalam mendeteksi serangan *reconnaissance* pada lingkungan *Internet Of Medical Things* (IoMT) dengan akurasi yang tinggi.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut :

1. Memberikan kontribusi dalam meningkatkan keamanan jaringan IoMT terhadap ancaman *reconnaissance* dan pengembangan metode *Machine Learning* dalam bidang kesehatan, khususnya dalam deteksi serangan *reconnaissance.*
2. Membantu melindungi data dan layanan medis, sehingga meningkatkan kepercayaan terhadap layanan kesehatan berbasis IoMT.
3. Menjadi acuan penelitian di bidang keamanan siber dalam lingkungan IoT, khususnya di sektor medis yang sangat penting seperti IoMT.

1.5 SISTEMATIKA PENULISAN

Sistematika penulisan ini menggambarkan secara umum mengenai apa yang akan penulis bahas dalam setiap bab dari laporan ini. dimana sistematika penulisan ini terdiri dari (5) bab meliputi :

BAB I : PENDAHULUAN

Dalam bab ini dijelaskan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini penulis membahas beberapa definisi dari beberapa teori-teori yang berhubungan dengan masalah yang diteliti bersumber dari buku dan jurnal-jurnal, untuk mendukung pemahaman terhadap penulis. Dan digunakan sebagai landasan untuk menjawab masalah penelitian serta membantu penulis agar memiliki landasan teori yang baik mengenai penelitian yang dilakukan.

BAB III : METODOLOGI PENELITIAN

Bab ini berisi metode pengumpulan data, prosedur penelitian, dan metode analisis berupa pendekatan penyelesaian masalah yang dilakukan untuk mendukung penelitian.

BAB IV : HASIL ANALISIS 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.

BAB V : PENUTUP

Bab terakhir ini berisikan kesimpulan dan saran-saran yang merupakan bab penutup agar dapat bermanfaat untuk para pembaca.