BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Di era revolusi industri 4.0, kemajuan teknologi berkembang dengan sangat cepat. Perkembangan ini memberikan dampak nyata bagi manusia, terutama dalam mempermudah berbagai aktivitas melalui pemanfaatan teknologi. Salah satu teknologi yang mengalami pertumbuhan pesat adalah internet, yang menjadikan berbagai hal lebih mudah untuk diakses dan dijalankan. Kemajuan ini turut mendorong lahirnya teknologi Internet of Things (IoT)[1]. *IoT* merujuk pada jaringan perangkat fisik yang terhubung secara digital, seperti sensor, perangkat cerdas, dan peralatan elektronik lainnya, yang dapat berkomunikasi dan saling bertukar data melalui internet[2]. Perkembangan *IoT* ini dapat kita rasakakan salah satunya pada pelayanan bidang kesehatan yang disebut *Internet of Medical Things (IoMT)*[1]. Internet of *Medical Things (IoMT*) merupakan integrasi antara perangkat medis dan aplikasi yang terhubung dengan sistem teknologi informasi dalam layanan kesehatan melalui jaringan teknologi.[3].

Ancaman keamanan pada perangkat *IoT*, termasuk *IoMT*, semakin mengkhawatirkan. Serangan siber dapat mengakibatkan gangguan pada layanan medis, kebocoran data pasien yang sensitif, bahkan manipulasi perangkat medis. Serangan siber ini memasuki sistem melalui *malware* yang berhasil ditanam di perangkat *IoT* [4]. Keterbatasan sumber daya pada perangkat *IoMT*, seperti daya komputasi yang rendah dan koneksi jaringan yang terbatas,

semakin memperparah kerentanan perangkat terhadap serangan seperti *Distributed Denial of Service (DDoS), spoofing*, dan *man-in-the-middle attacks*[5].

Spoofing merupakan salah satu jenis serangan siber di mana pelaku menyamar sebagai individu atau entitas tertentu dengan tujuan mencuri data dari korban. Beberapa bentuk umum dari serangan spoofing antara lain *Address Resolution Protocol (ARP) spoofing* dan *Domain Name System (DNS) spoofing*.[6]. *Address Resulotion Protocol (ARP)* adalah protokol yang bertugas untuk menerjemahkan *ip address* menjadi *MAC address* [7]. *ARP* adalah protokol yang sangat rentan untuk di eksploitasi oleh *hacker*, karena kemungkinan setiap komputer memberikan paket *ARP* palsu. Kelemahan ini digunakan untuk melancarkan serangan yang dikenal sebagai *ARP spoofing* [8]. *ARP spoofing* merupakan teknik manipulasi terhadap pemetaan *ARP cache* dalam sebuah jaringan. Dalam serangan ini, pelaku secara terus-menerus mengirimkan paket *ARP reply* palsu ke perangkat target. Serangan ini sering kali disertai dengan upaya untuk menyadap atau mengambil alih komunikasi yang tidak terenkripsi atau tidak dilindungi oleh tanda tangan digital. *Address Resolution Protocol* (*ARP*) sendiri adalah protokol jaringan yang digunakan untuk menghubungkan alamat IP dengan alamat MAC dalam lingkungan jaringan lokal. *ARP spoofing* tergolong sebagai ancaman serius karena memungkinkan penyerang tidak hanya memantau lalu lintas data, tetapi juga mengubah isi data dan mencuri identitas pengguna[9].[9].

Oleh karena itu, diperlukan suatu sistem yang mampu mendeteksi dan menangani penyalahgunaan dalam jaringan maupun potensi ancaman dari pihak yang tidak berwenang, salah satunya melalui penerapan aplikasi *Intrusion Detection System* (IDS)[10]. *IDS* berguna sebagai pendeteksi aktivitas atau serangan yang tidak sah dan tidak normal[9].

Pada penelitian [11],terkait deteksi serangan menggunakan *random forest* didapatkan hasil dari algoritma *random forest* dengan tingkat akurasi mencapai 98%. Penelitian lainnya yang dilakukan oleh [12], didapatkan tingkat akurasi algoritma *random forest* mencapai 99,41%, *KNN* mencapai 99%, *SVM* mencapai 98,37%, dan *MLP* mencapai 93,97%. Berdasarkan penelitian diatas menunjukka bahwa akurasi algoritma *random forest* lebih baik dari beberapa algoritma lainnya.

Salah satu algoritma *machine learning* yang berpotensi untuk dapat meningkatkan keamanan perangkat *IoMT* adalah algoritma *random forest*. *Random Forest* adalah algoritma pembelajaran mesin yang fleksibel dan mudah digunakan. Algoritma *Random Forest* adalah salah satu algoritma yang paling sering digunakan karena sifatnya yang sederhana serta fleksibel, sehingga dapat diterapkan baik untuk tugas klasifikasi maupun regresi [13].

Penelitian ini bertujuan untuk mengimplementasikan algoritma *random forest* dalam deteksi serangan pada perangkat *IoMT*, khususnya serangan *ARP spoofing*. Dengan menerapkan algoritma ini, diharapkan dapat diperoleh sistem

deteksi yang efisien. Sehingga dapat tercapai perlindungan yang lebih baik terhadap peragkat *IoMT*.

Berdasarkan latar belakang yang sudah dijelaskan, maka peneliti tertarik untuk mengambil judul ***"IMPLEMENTASI ALGORITMA RANDOM FOREST UNTUK DETEKSI SERANGAN SPOOFING PADA IoMT"***.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang masalah yang telah dikemukakan diatas, beberapa penelitian telah mencoba mengimplementasikan beberapa algoritma machine learning dalam mendeteksi serangan, namun algoritma yang memiliki akurasi yang lebih tinggi adalah algoritma *random forest*. Maka dari itu peneliti mencoba mengimplementasikan algoritma tersebut dalam mendeteksi serangan *ARP spoofing* pada *IoMT*

Dari pernyataan masalah diatas maka peneliti dapat menuliskan pertanyaan masalah berikut :

1. Bagaimana cara mengimplementasikan algoritma *random forest* dalam mendeteksi serangan *ARP spoofing* pada *IoMT*?
2. Bagaimana kinerja algoritma *random forest* dalam mendeteksi serangan *ARP spoofing* pada *IoMT*?

1.3 BATASAN MASALAH

Agar dalam penelitian ini dapat berjalan dengan baik dan terarah penulis menetapkan ruang lingkup penelitian meliputi :

1. Nama dataset yang digunakan dalam penelitian ini adalah "*CIC IoMT dataset* 2024" yang bersumber dari https://www.unb.ca/ dengan 45 atribut dan 248.130 *record*.
2. Penelitian ini akan mengevaluasi model deteksi dengan *accuracy, recall, dan F1- score*.
3. Dalam penelitian ini tidak membahas bagaimana cara pencegahan serangan *spoofing* pada *IoMT*.
4. Penelitian ini menggunakan *google colab* sebagai alat bantu deteksi.

1.4 TUJUAN PENELITIAN

Berdasarkan pada permasalahan yang telah disampaikan sebelumnya yang terdapat di dalam penelitian ini. Memiliki tujuan-tujuan sebagai berikut :

1. Melakukan deteksi serangan *ARP spoofing* menggunakan metode *random forest.*
2. Mengetahui kinerja algoritma *random forest* dalam mendeteksi serangan *ARP spoofing*.

1.5 MANFAAT PENELITIAN

Adapun manfaat yang diperoleh dari penelitian ini adalah

1. Dapat menghasilkan output dari algoritma *random forest* pada serangan *ARP spoofing*.
2. Sebagai bahan referensi bagi peneliti yang sedang melakukan penelitian tentang serangan *ARP spoofing* pada *IoMT*.