BAB 1
PENDAHULUAN

1.1. Latar Belakang

Perkembangan Teknologi Informasi (TI) di era digital saat ini menunjukkan pertumbuhan yang sangat pesat. Teknologi informasi memberikan berbagai manfaat, seperti kemudahan dalam mencari dan bertukar informasi, pengolahan data, serta mendorong inovasi bisnis. Teknologi informasi juga erat kaitannya dengan jaringan internet. Menurut laporan terbaru, jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221,56 juta orang, meningkat dari 215,63 juta orang pada tahun 2022-2023. Dari jumlah tersebut, sekitar 22,4% adalah pengguna Wi-Fi [1]. Penggunaan Wi-Fi di Indonesia semakin meluas, terutama di tempat-tempat umum seperti kafe, restoran, dan ruang publik lainnya. *Wireless Local Area Network* (WLAN) menjadi pilihan karena kemudahan akses tanpa kabel fisik yang memberikan fleksibilitas tinggi bagi pengguna. Namun, di balik keunggulan tersebut, keamanan WLAN menjadi perhatian serius karena jaringan ini rentan terhadap berbagai serangan siber.

Salah satu ancaman yang umum terjadi pada WLAN adalah *Address Resolution Protocol* (ARP) *poisoning*. Serangan ini dilakukan dengan mengirimkan paket ARP palsu ke jaringan untuk memanipulasi tabel ARP perangkat lain, sehingga memungkinkan penyerang mengalihkan lalu lintas data ke perangkatnya sendiri [2]. Serangan ini dapat mengakibatkan pencurian data sensitif, modifikasi lalu lintas, atau bahkan penghentian koneksi pada perangkat yang terhubung. Dampaknya tidak hanya merugikan individu, tetapi juga dapat menimbulkan kerugian finansial dan kerusakan reputasi bagi individu atau organisasi [3].

Penting untuk memiliki sistem deteksi yang mampu mengenali serangan *ARP poisoning* secara dini. Penelitian sebelumnya menunjukkan bahwa Machine Learning dapat menjadi solusi efektif dalam mendeteksi serangan siber, termasuk ARP Poisoning, dengan memanfaatkan analisis pola lalu lintas jaringan secara mendalam. Pendekatan ini memungkinkan pengenalan pola mencurigakan dengan tingkat akurasi yang tinggi sambil mempertimbangkan aspek kompleksitas dan efisiensi [4]. Salah satu algoritma yang sering digunakan untuk mendeteksi serangan jaringan adalah Random Forest. Algoritma ini mampu mengklasifikasikan data berdasarkan struktur pohon keputusan yang kompleks dan dikenal handal dalam mengelola data besar serta

anomali yang terjadi dalam jaringan [5]. Kedua, penelitian ini menggunakan algoritma AdaBoost. AdaBoost merupakan teknik pengembangan dari *Decision Tree* seperti Random Forest, namun algoritma tersebut berfokus pada teknik *boosting*, berbeda dengan Random Forest yang menggunakan teknik *Bagging* (*bootstrap* dan *aggregating).* Tujuannya adalah membandingkan *ensemble learning* mana yang memiliki performa lebih baik.

Menurut penelitian dari Ahuja et al. [6], serangan ARP *poisoning* dapat menyebabkan kerentanan signifikan pada jaringan, termasuk kebocoran data, gangguan layanan, dan ancaman keamanan lainnya. Penelitian tersebut menunjukkan bahwa algoritma Random Forest dapat meningkatkan deteksi serangan dengan analisis pola lalu lintas jaringan yang lebih efisien. Algoritma ini berhasil mencapai akurasi deteksi hingga 97,2% pada dataset lalu lintas jaringan yang dihasilkan menggunakan emulator. Penelitian tersebut juga mengidentifikasi bahwa serangan *ARP poisoning* dilakukan dengan mengirimkan paket ARP palsu, baik dalam bentuk permintaan maupun balasan, yang mengarah pada manipulasi tabel ARP perangkat target.

Dari peneliti terdahulu, kami melakukan pengembangan yaitu sistem deteksi ARP *poisoning* yang memanfaatkan kombinasi *machine learning* dan scapy. Scapy merupakan sebuah pustaka Python yang kuat untuk manipulasi paket jaringan. Scapy memungkinkan perekaman dan analisis lalu lintas secara langsung, yang kemudian dapat diolah menggunakan algoritma Random Forest dan AdaBoost untuk mendeteksi pola serangan [7]. Dengan menggabungkan kemampuan scapy dan algoritma Random Forest dan AdaBoost, diharapkan sistem ini dapat memberikan deteksi terhadap ancaman ARP *poisoning*.

Untuk proses pengambilan dataset dilakukan di *coffee shop* Gelateria yang berlokasi di jalan tunjungan Surabaya, kemudian juga terdapat aktivitas perekaman data menggunakan simulasi serangan statis yang nantinya akan di *merge* atau integrasikan. Tools perekaman dataset menggunakan wireshark yang perannya adalah untuk merekam lalu lintas jaringan yang terkoneksi secara *real time*. Wireshark memiliki beberapa keunggulan, yaitu kemampuannya untuk menangkap paket data secara *real time* dari antarmuka jaringan fisik. Dari penelitian ini sendiri peneliti menemukan celah mengenai adanya kekurangan pada sistem yaitu adanya kesalahan dari menemukan letak kondisi duplikasi atau identitas penyerang sebenarnya. Oleh karena itu pada penelitian ini selain melakukan deteksi ARP *Poisoning* juga dapat

mengidentifikasi identitas penyerang sebenarnya yang dipelajari oleh model *machine learning* Random Forest dan AdaBoost.

Dapat disimpulkan bahwa skripsi ini bertujuan untuk melakukan *testing* mengenai model Random Forest dan AdaBoost (*hybrid*) apakah terbukti baik secara *confusion matrix* dan penerapan pada *real time* nya dibandingkan dengan beberapa skenario *machine learning* lainnya. Untuk *output* atau luaran dari penelitian ini adalah berupa bot telegram yang bisa mendeteksi secara *real time* kemudian dapat mengirimkan notif secara berkala. Sistem yang dihasilkan diharapkan dapat meningkatkan keamanan jaringan WLAN dan memberikan solusi efektif bagi pengguna serta penyedia layanan dalam menghadapi risiko serangan siber. Dengan kontribusi ini, diharapkan mendukung pengembangan teknologi keamanan jaringan sekaligus memberikan wawasan baru dalam penerapan *machine learning* untuk mitigasi ancaman keamanan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, diperoleh rumusan masalah yaitu bagaimana merancang sistem deteksi serangan ARP *Poisoning* pada jaringan WLAN menggunakan algoritma *machine learning* yang efektif? dan apakah algoritma Random Forest x AdaBoost (*hybrid*) terbukti optimal untuk dimodelkan?

1.3. Batasan Masalah

Agar penelitian lebih fokus lebih fokus dan terarah, terdapat beberapa batasan masalah yang diterapkan, yaitu sebagai berikut:

1. Skripsi ini berfokus pada deteksi ARP *poisoning* pada jaringan WLAN dan tidak mencakup metode pencegahan atau mitigasi serangan secara langsung.
2. Deteksi serangan ARP dibatasi pada jenis paket manipulasi ARP *reply*.
3. Algoritma *machine learning* yang digunakan untuk membangun sistem deteksi adalah Random Forest dan AdaBoost
4. Data yang digunakan untuk melatih dan menguji model diambil dari hasil monitoring lalu lintas jaringan pada *coffee shop* di Surabaya yaitu Gelateria dan data dari simulasi serangan menggunakan wireshark.
5. Model deteksi yang dirancang mengevaluasi performa menggunakan confusion matrix yaitu *accuracy, precision, recall, dan F1-score.*

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk merancang sistem deteksi serangan ARP *Poisoning* pada jaringan WLAN dengan memanfaatkan algoritma Random Forest dan AdaBoost. Selain itu, penelitian ini juga bertujuan untuk mengevaluasi kinerja algoritma Random Forest dan AdaBoost apakah terbukti optimal dibandingkan dengan 4 skenario kombinasi lainnya.

1.5. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat bagi berbagai pihak. Bagi peneliti, penelitian ini memperluas wawasan tentang penerapan algoritma Random Forest dan AdaBoost dalam mendeteksi serangan ARP *poisoning*. Bagi praktisi keamanan jaringan, penelitian ini menyediakan sistem deteksi serangan ARP *Poisoning* yang dapat diimplementasikan pada jaringan WLAN dan memberikan informasi perbandingan kinerja antara algoritma Random Forest, AdaBoost, dan 4 skenario kombinasi lainnya untuk menentukan algoritma yang optimal. Bagi dunia akademik, penelitian ini berkontribusi pada pengembangan ilmu keamanan jaringan berbasis *machine learning* dan dapat menjadi referensi bagi penelitian selanjutnya terkait evaluasi kinerja algoritma deteksi serangan jaringan.