DETEKSI PENIRUAN ROUTER NIRKABEL DENGAN PEMBELAJARAN MESIN

1st Muhammad Hidayah Ramadhan
Telkom University
Fakultas Teknik Elektro
Bandung, Indonesia
hidayahramadhan@student.telkomuniversity.ac.id

2nd Ida Wahidah
Telkom University
Fakultas Teknik Elektro
Bandung, Indonesia
wahidah@telkomuniversity.ac.id

3rd Fardan
Telkom University
Fakultas Teknik Elektro
Bandung, Indonesia
fardanfnn@telkomuniversity.ac.id

***Abstrak* — Deteksi Rogue Access Point (RAP) penting untuk mencegah serangan Evil Twin Attack (ETA) di lingkungan kampus, seperti di Telkom University. Penelitian ini mengembangkan model Machine Learning (ML) untuk mendeteksi RAP berdasarkan data yang dikumpulkan menggunakan airodump-ng. Data mencakup parameter jaringan seperti Channel, Speed, Privacy, Cipher, Authentication, Power, dan beacons. Data dikumpulkan dengan perangkat TP-Link WN821N. data digunakan untuk melatih model ML dengan algoritma Feedforward Neural Network (FNN).**

Kata kunci*— *Rogue Access Point, Evil Twin Attack, Machine Learning, Feedforward Neural Network, airodump-ng

I. PENDAHULUAN

Dalam era konektivitas yang semakin meningkat, jaringan nirkabel menjadi infrastruktur kunci, namun juga menghadirkan risiko serangan seperti wireless router impersonation yang dapat merugikan pengguna dengan mengakses data pribadi. Salah satu serangan ini adalah Evil Twin Attack (ETA), di mana penyerang menciptakan Rogue Access Point (RAP) dengan SSID yang sama untuk membajak koneksi nirkabel pengguna. Contoh nyata adalah penangkapan di Australia terkait hotspot Wi-Fi palsu di bandara, yang menunjukkan risiko serius di lokasi strategis.[1]

Para pakar keamanan siber memperingatkan bahaya Wi-Fi publik dan gratis, yang dapat digunakan untuk mencuri data pengguna melalui RAP. Serangan ini sering kali tidak terdeteksi oleh korban, dengan potensi pencurian data sensitif seperti nama pengguna dan kata sandi, serta risiko infeksi malware.[1]

Untuk menghadapi masalah ini, solusi Machine Learning (ML) menjadi semakin penting. ML menawarkan pendekatan cerdas untuk mendeteksi impersonasi router nirkabel dengan mengidentifikasi pola lalu lintas yang kompleks. Implementasi ML bersama teknik deteksi konvensional dapat meningkatkan perlindungan terhadap serangan, menjaga keamanan pengguna dan data sensitif dalam jaringan nirkabel.

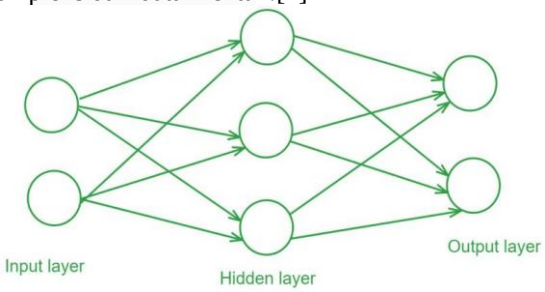
II. KAJIAN TEORI

A. *Machine Learning*

Dalam proses deteksi *Rogue Access Point* (RAP) dan AP yang sah, Algoritma *Feedforward Neural Network* (FNN) digunakan untuk melakukan klasifikasi antara keduanya berdasarkan data yang diterima dari airodump-ng dari jaringan Wi-Fi yang ada di sekitar. FNN akan belajar dari berbagai contoh dataset sinyal Wi-Fi yang diberikan, termasuk dataset dari RAP dan AP yang sah. Proses pembelajaran ini akan membantu FNN untuk mengidentifikasi pola yang membedakan antara sinyal yang berasal dari RAP dan AP yang sah.

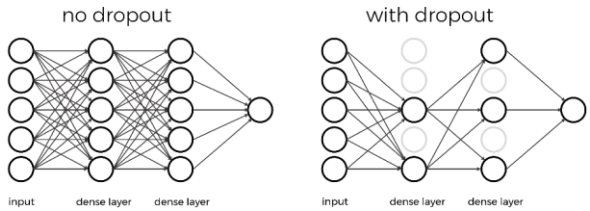
B. *Algoritma FNN*

Deep learning adalah subbidang dari ML yang menggunakan jaringan syaraf tiruan (neural networks) dengan banyak lapisan *(deep neural networks)* untuk menganalisis data dan membuat prediksi. Selain itu, deep learning memiliki kemampuan untuk mengekstraksi fitur-fitur kompleks dari data mentah.[2]



Gambar 1. *Feedforward Neural Network (FNN).*

Feedforward Neural Network (FNN) adalah jenis jaringan saraf tiruan yang meniru cara kerja otak manusia, di mana informasi mengalir satu arah dari input ke output tanpa aliran balik. FNN merupakan bentuk jaringan saraf yang sederhana dan sering digunakan untuk tugas-tugas klasifikasi dan prediksi. Model ini menggunakan arsitektur sequential yang menyusun lapisan-lapisan neural network secara berurutan, cocok untuk struktur jaringan yang sederhana.[2]



Gambar 2. *Perbedaan Arsitektur FNN dengan Dense (A) dan setelah di Dropout (B).*

Untuk mengatasi overfitting, teknik dropout digunakan dengan secara acak menghilangkan neuron selama pelatihan, memaksa jaringan belajar representasi yang lebih umum. Neuron sendiri adalah unit dasar pemrosesan yang menerima input, mengalikan dengan bobot, menambahkan bias, dan menerapkan fungsi aktivasi seperti ReLU atau sigmoid. ReLU (Rectified Linear Unit) adalah fungsi aktivasi populer yang memperkenalkan non-linearitas, membantu jaringan belajar dan merepresentasikan data yang lebih kompleks.

Inisialisasi bobot dengan metode he_normal digunakan untuk memastikan sinyal dan gradien tidak terlalu kecil atau besar, mendukung konvergensi yang cepat dan stabil. Selain itu, parameter use_bias=False dapat digunakan dalam lapisan neural network untuk menentukan apakah bias akan digunakan dalam perhitungan neuron, memberikan fleksibilitas tambahan pada model.

Fungsi aktivasi sigmoid juga umum digunakan dalam klasifikasi biner, mengubah input menjadi nilai antara 0 dan 1, meskipun rentan terhadap masalah vanishing gradient. Secara keseluruhan, FNN dan teknik-teknik terkaitnya memainkan peran penting dalam mengembangkan model pembelajaran mesin yang efektif untuk berbagai aplikasi klasifikasi.

C. Dataset

Dataset yang dihasilkan dari airodump-ng berisi informasi detail mengenai jaringan Wi-Fi yang terdeteksi selama pemindaian. Setiap entri mencakup atribut seperti kanal frekuensi (*Channel*), kecepatan data maksimum (*Speed*), jenis enkripsi (*Privacy*), algoritma enkripsi (*Cipher*), metode otentikasi (Authentication), kekuatan sinyal (Power), jumlah beacon frames (# *Beacons*), jumlah Initialization Vector (# IV), dan panjang identifikasi SSID (*ID-length*). Dataset ini dapat digunakan untuk analisis keamanan jaringan, mengidentifikasi jaringan rentan, dan memetakan topologi jaringan nirkabel di suatu area.

III. METODE

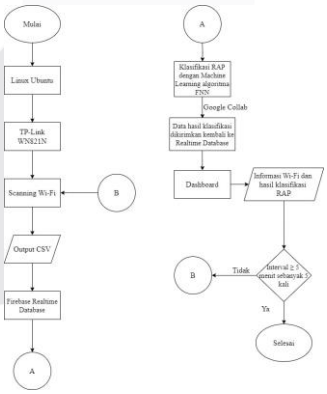
A. Alur Proses Sistem

Dalam penelitian ini, sistem dikembangkan untuk mendeteksi penyusupan jaringan Wi-Fi melalui beberapa tahap kritis. Tahap pertama melibatkan pengumpulan data Wi-Fi yang mencakup berbagai parameter seperti kanal frekuensi (Channel), kecepatan data maksimum (Speed), jenis enkripsi (Privacy), algoritma enkripsi (Cipher), metode otentikasi (Authentication), kekuatan sinyal (Power), jumlah beacon frames (# Beacons), jumlah Initialization Vector (# IV), dan panjang identifikasi SSID (ID-length). Selanjutnya, data yang dikumpulkan melalui tahap preprocessing, di mana dilakukan pembersihan dan pengolahan data, termasuk encoding, normalisasi, serta penghapusan fitur yang tidak relevan. Data yang telah diproses ini kemudian digunakan untuk melatih model machine learning (ML), yang dirancang untuk mengenali pola dalam jaringan yang aman serta jaringan yang berpotensi menjadi target penyusupan. Tahap akhir adalah pengujian model, di mana model diuji menggunakan data testing yang belum pernah dilihat sebelumnya, untuk memastikan kemampuannya dalam mengidentifikasi penyusupan berdasarkan karakteristik yang telah dikenali.

B. Implementasi Sistem

Dalam penelitian ini, sistem dikembangkan untuk mendeteksi penyusupan jaringan Wi-Fi melalui beberapa tahap kritis. Tahap pertama melibatkan pengumpulan data Wi-Fi yang mencakup berbagai parameter seperti kanal frekuensi (Channel), kecepatan data maksimum (Speed), jenis enkripsi (Privacy), algoritma enkripsi (Cipher), metode otentikasi (Authentication), kekuatan sinyal (Power), jumlah beacon frames (# Beacons), jumlah Initialization Vector (# IV), dan panjang identifikasi SSID (ID-length). Selanjutnya, data yang dikumpulkan melalui tahap preprocessing, di mana dilakukan pembersihan dan pengolahan data, termasuk encoding, normalisasi, serta penghapusan fitur yang tidak relevan. Data yang telah diproses ini kemudian digunakan untuk melatih model machine learning (ML), yang dirancang untuk mengenali pola dalam jaringan yang aman serta jaringan yang berpotensi menjadi target penyusupan. Tahap akhir adalah pengujian model, di mana model diuji menggunakan data testing yang belum pernah dilihat sebelumnya, untuk memastikan kemampuannya dalam mengidentifikasi penyusupan berdasarkan karakteristik yang telah dikenali.

C. Cara Kerja Deteksi Peniruan Router Nirkabel dengan Pembelajaran Mesin.



Gambar 3. Flowchart Cara Kerja Deteksi Peniruan Router Nirkabel dengan Pembelajaran Mesin

Cara Gambar di atas menunjukkan alur kerja sistem deteksi peniruan router nirkabel dengan menggunakan pembelajaran mesin. Sistem ini dimulai dengan inisialisasi perangkat pada Linux Ubuntu, yang kemudian melakukan proses pemindaian Wi-Fi menggunakan perangkat TP-Link WN821N. Hasil dari pemindaian ini disimpan dalam format CSV dan kemudian dimuat ke dalam Firebase Realtime Database.

Selanjutnya, data yang telah dimuat ke Firebase diambil dan digunakan untuk klasifikasi menggunakan algoritma machine learning Feedforward Neural Network (FNN) yang dijalankan di Google Collab. Hasil klasifikasi ini kemudian dikirim kembali ke Firebase Realtime Database dan ditampilkan pada dashboard yang berisi informasi terkait jaringan Wi-Fi dan hasil klasifikasi RAP (Rogue Access Point).

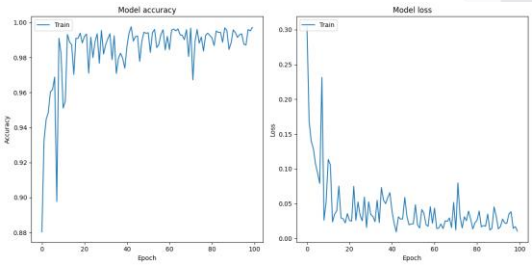
Proses ini diulang secara berkala dengan interval waktu yang telah ditentukan. Apabila proses telah dilakukan sebanyak lima kali dengan interval lima menit, maka sistem akan menghentikan pengulangan dan proses dianggap selesai. Dengan demikian, sistem ini memastikan bahwa deteksi peniruan router dilakukan secara terus-menerus dan hasilnya diperbarui secara real-time, memberikan informasi yang akurat dan terkini kepada pengguna..

IV. HASIL DAN PEMBAHASAN

Untuk menguji akurasi model dalam mendeteksi Wireless Router Impersonation, dilakukan pengujian dengan dua skenario pembagian dataset pelatihan dan pengujian dan pengujian menggunakan data test yang tidak ada di dataset. Pengujian ini bertujuan untuk memastikan bahwa model Machine Learning dapat memberikan klasifikasi dan prediksi yang akurat dalam mendeteksi router palsu. Parameter yang diuji meliputi Channel, Speed, Privacy, Cipher, Authentication, Power, beacons, dan ID-length. Dengan pengujian yang cermat, performa model dapat dievaluasi untuk memastikan keandalannya dalam membedakan antara router asli dan penyamaran, sehingga meningkatkan keamanan jaringan nirkabel..

A. *Pembagian Dataset: 75% untuk Pelatihan dan 25% untuk Pengujian*

Model dilatih menggunakan dataset yang disiapkan untuk mendeteksi RAP. Proses pelatihan berlangsung selama 100 epoch, di mana setiap epoch melibatkan iterasi penuh melalui dataset. Hasil pelatihan menunjukkan peningkatan akurasi model secara bertahap, dari 88.04% pada epoch pertama hingga mencapai 99.72% pada epoch terakhir. Nilai loss juga mengalami penurunan yang signifikan, menunjukkan bahwa model semakin baik dalam memprediksi data pelatihan.

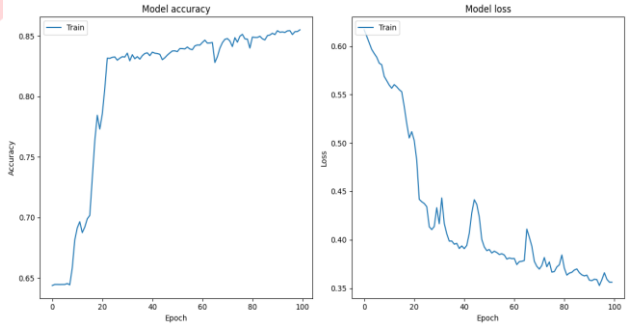


Gambar 4. Grafik Akurasi dan Nilai Loss Model Ml 75% pelatihan dan 25% pengujian.

Menampilkan grafik akurasi dan nilai loss model ML selama 100 epoch. Dari hasil pelatihan ini, dapat disimpulkan bahwa model menunjukkan kinerja yang sangat baik dalam klasifikasi data pelatihan. Model secara konsisten meningkatkan akurasinya dan mengurangi nilai *loss* seiring berjalannya epoch. Meskipun terdapat beberapa anomali pada beberapa epoch, model berhasil mempertahankan akurasi yang tinggi secara keseluruhan. Secara keseluruhan, model menunjukkan kemampuan yang kuat dalam klasifikasi dan deteksi penyamaran router nirkabel, memberikan dasar yang kuat untuk aplikasi lebih lanjut dalam lingkungan jaringan yang lebih luas. Peningkatan akurasi dan penurunan nilai *loss* yang konsisten menunjukkan bahwa model memiliki potensi yang baik untuk digunakan dalam skenario dunia nyata, di mana deteksi yang akurat dan cepat dari RAP sangat penting untuk keamanan jaringan .

B. *Pembagian Dataset: 60% untuk Pelatihan dan 40% untuk Pengujian*

Model dilatih menggunakan dataset yang disiapkan untuk mendeteksi RAP. Proses pelatihan berlangsung selama 100 epoch, di mana setiap epoch melibatkan iterasi penuh melalui dataset. Berdasarkan grafik akurasi dan *loss*, terlihat bahwa model mengalami peningkatan akurasi dan penurunan loss yang signifikan selama pelatihan.



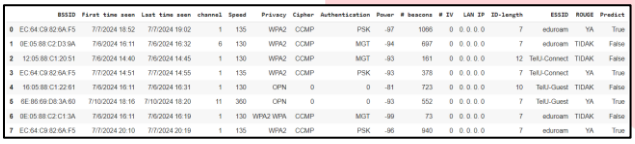
Gambar 5. Grafik Akurasi dan Nilai Loss Model ML 60% Pelatihan dan 40% pengujian

Model mencapai akurasi sebesar 64.38% dengan nilai *loss* 0.6169. Akurasi model meningkat secara bertahap, mencapai sekitar 73% pada epoch ke-10, dan terus meningkat hingga sekitar 85% pada epoch terakhir. Nilai *loss* juga menunjukkan penurunan yang signifikan selama pelatihan, mencapai nilai terendah sekitar 0.35 pada epoch ke-100. Grafik akurasi menunjukkan bahwa model terus belajar dan meningkatkan performanya seiring bertambahnya epoch. Meskipun terdapat beberapa fluktuasi kecil pada nilai akurasi, tren keseluruhannya adalah peningkatan yang stabil. Grafik *loss* juga menunjukkan penurunan yang konsisten, dengan beberapa fluktuasi kecil, yang menunjukkan bahwa model semakin mampu meminimalkan kesalahan selama pelatihan.

Analisis ini menunjukkan bahwa model mampu belajar dengan baik dari data pelatihan, meningkatkan akurasinya, dan mengurangi *loss* secara signifikan. Namun, penting untuk melakukan validasi lebih lanjut menggunakan data uji untuk memastikan bahwa model tidak mengalami *overfitting* dan mampu menggeneralisasi dengan baik pada data baru.

C. *Pengujian Model Machine Learning dengan Data Testing*

Pada tahap ini, dilakukan analisis terhadap pengujian model machine learning menggunakan data uji untuk menilai seberapa baik model mampu mengenali dan memprediksi pola pada data baru yang tidak termasuk dalam dataset pelatihan. Dalam konteks *Wireless Router Impersonation*, metode yang digunakan adalah dengan menyamakan SSID (*Service Set Identifier*) antara akses poin yang sah dengan akses poin palsu. Model diuji untuk memastikan kemampuannya dalam mengidentifikasi perbedaan antara SSID yang sah dan yang telah dipalsukan. Hasil pengujian dievaluasi melalui metrik performa seperti akurasi. Analisis ini penting untuk memastikan bahwa model tidak hanya efektif dalam mengenali pola pada data pelatihan, tetapi juga memiliki kemampuan yang baik dalam menggeneralisasi prediksi pada data uji, yang sangat penting dalam penerapan di lingkungan jaringan yang lebih luas.



	BSSID	First time seen	Last time seen	channel	Speed	Privacy	Cipher	Authentication	Power	# beacons	# IV	LAN IP	ID-length	ESSID	ROUGE	Predict
0	EC:64:C9:82:6A:F5	7/7/2024 18:52	7/7/2024 19:02	1	135	WPA2	CCMP	PSK	-97	1066	0	0.0.0.0	7	eduroam	YA	True
1	0E:05:88:C2:D3:9A	7/6/2024 16:11	7/6/2024 16:32	6	130	WPA2	CCMP	MGT	-94	697	0	0.0.0.0	7	eduroam	TIDAK	False
2	12:05:88:C1:20:51	7/6/2024 14:40	7/6/2024 14:45	1	130	WPA2	CCMP	MGT	-93	161	0	0.0.0.0	12	TelU-Connect	TIDAK	False
3	EC:64:C9:82:6A:F5	7/7/2024 14:51	7/7/2024 14:55	1	135	WPA2	CCMP	PSK	-93	378	0	0.0.0.0	7	TelU-Connect	YA	True
4	16:05:88:C1:22:61	7/6/2024 16:11	7/6/2024 16:31	1	130	OPN	0	0	-81	723	0	0.0.0.0	10	TelU-Guest	TIDAK	False
5	6E:86:69:D8:3A:60	7/10/2024 18:16	7/10/2024 18:20	11	360	OPN	0	0	-93	552	0	0.0.0.0	7	TelU-Guest	YA	True
6	0E:05:88:C2:C1:3A	7/6/2024 16:11	7/6/2024 16:19	1	130	WPA2 WPA	CCMP	MGT	-99	73	0	0.0.0.0	7	eduroam	TIDAK	False
7	EC:64:C9:82:6A:F5	7/7/2024 20:10	7/7/2024 20:19	1	135	WPA2	CCMP	PSK	-96	940	0	0.0.0.0	7	eduroam	YA	True

Gambar 6. Menampilkan hasil klasifikasi model ML.

Hasil klasifikasi model machine learning pada Gambar di atas menunjukkan kinerja yang sangat baik dalam mendeteksi dan membedakan jaringan asli dari jaringan penyamaran. Pengujian dengan metode pencocokan SSID serupa menunjukkan bahwa model akurat mengidentifikasi jaringan "eduroam" sebagai penyamaran dan "TelU-Connect" sebagai jaringan asli. Akurasi tinggi ini menegaskan keandalan model dalam klasifikasi jaringan, berkontribusi signifikan pada deteksi ancaman keamanan siber dalam jaringan nirkabel.

V. KESIMPULAN

Berdasarkan Penelitian ini secara komprehensif membahas implementasi deteksi Rogue Access Point (RAP) menggunakan Machine Learning. Data dikumpulkan melalui pemindaian jaringan Wi-Fi dengan TP-Link WN821N dan airodump-ng, kemudian diolah dan disimpan di Firebase Realtime Database. Model Machine Learning yang dikembangkan berhasil mencapai akurasi 99.72% dalam mendeteksi RAP, dengan nilai loss yang menurun secara signifikan. Dashboard yang dibangun memudahkan visualisasi dan manajemen keamanan jaringan secara real-time. Implementasi ini tidak hanya meningkatkan keamanan jaringan Wi-Fi di Telkom University, tetapi juga memberikan dasar untuk aplikasi lebih lanjut dalam deteksi ancaman keamanan lainnya. Penelitian ini menunjukkan bahwa Machine Learning adalah metode yang efisien dan efektif untuk mendeteksi dan mengatasi ancaman penyamaran router nirkabel, dengan potensi penerapan luas di berbagai lingkungan.

VI. REFERENSI

[1] ezkalns, “Aussie Police Discover ‘Evil Twin’ Free Wifi Harvesting Personal Data at Airports,” commsrisk.com. Accessed: Jul. 11, 2024. [Online]. Available: https://commsrisk.com/aussie-police-discover-evil-twin-free-wifi-harvesting-personal-data-at-airports/

[2] J. Zou, Y. Han, and S.-S. So, “Overview of Artificial Neural Networks,” 2008. doi: 10.1007/978-1-60327-101-1_2.