Penggunaan *Dashboard* untuk Menampilkan Hasil *Detection of Wireless Router Impersonation*

1st Azhra Aufahadi Yasik
Fakultas Teknik Elektro
Telkom University
Bandung, Indonesia
azhraaufa@student.telkomuniversity.ac.id

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

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

***Abstrak* — Dalam era konektivitas yang semakin meningkat, keamanan jaringan nirkabel menjadi krusial, terutama dengan munculnya ancaman impersonasi router nirkabel. Penelitian ini bertujuan untuk mendeteksi impersonasi router nirkabel menggunakan algoritma *Machine Learning* (ML) yang diimplementasikan melalui *Feedforward Neural Network* (FNN). Data Wi-Fi dikumpulkan menggunakan airodump-ng, diolah dengan model ML, dan hasilnya divisualisasikan melalui *dashboard* interaktif. Dashboard ini memudahkan pemantauan dan identifikasi *Rogue Access Point* (RAP), serta *Trusted Access Point* sehingga memberikan perlindungan lebih terhadap jaringan. Pengujian performa *dashboard* dilakukan melalui CPU & *Memory Usage*, serta *User Experience Questionnaire* (UEQ). Hasil menunjukkan *dashboard* mampu beroperasi secara efisien dengan beban kerja yang bervariasi dan mendapatkan respon positif dari pengguna dalam aspek daya tarik, kejelasan, dan efisiensi.**

***Kata kunci*— impersonasi router nirkabel, *machine learning*, *Feedforward Neural Network* (FNN), *dashboard*, keamanan jaringan nirkabel, *Rogue Access Point (RAP)*.**

I. PENDAHULUAN

Dalam era konektivitas yang semakin meningkat, jaringan nirkabel menjadi infrastruktur penting bagi rumah tangga hingga perusahaan. Namun, meskipun terdapat keuntungan, terdapat juga resiko serangan, seperti *wireless router impersonation* yang dapat merugikan pengguna dengan mengakses data pribadi yang sangat sensitif.

Kepolisian Federal Australia baru-baru ini menangkap seorang pria yang diduga mengoperasikan *hotspot* Wi-Fi palsu di beberapa bandara besar, termasuk Perth, Melbourne, dan Adelaide. Jaringan Wi-Fi *Evil Twin Attack* (ETA) ini meniru jaringan yang sah untuk menarik pengguna agar memberikan data pribadi mereka, seperti akun email dan media sosial. Insiden ini menunjukkan resiko keamanan yang serius di lingkungan bandara karena konsentrasi orang yang tinggi dan kebutuhan untuk berkomunikasi menjadikannya target empuk bagi para penjahat siber. Kasus ini menunjukkan pentingnya upaya proaktif dalam mendeteksi dan mencegah kejahatan siber di lokasi-lokasi strategis, seperti bandara[1], [2].

Dengan meningkatnya ancaman terhadap keamanan jaringan nirkabel, *"Detection of Wireless Router Impersonation"* menjadi sangat penting. Implementasi solusi dalam sistem ini menggabungkan pendekatan *Machine Learning* (ML) dan *dashboard* sebagai media untuk menampilkan informasi dari hasil klasifikasi ML. Penggunaan *dashboard* dalam sistem ini memudahkan pengguna untuk memantau status jaringan dan mengambil tindakan yang diperlukan berdasarkan data yang telah ditampilkan. Hal ini dapat memberikan perlindungan yang lebih untuk melindungi data sensitif dan menjaga keamanan pengguna dalam mengakses 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. *Hardware*

Hardware adalah perangkat keras pendeteksi yang diperlukan untuk mengidentifikasi *Rogue Access Point* (RAP). Dalam perangkat keras mencakup beberapa komponen, antara lain ESP32, Router sebagai *Access Point* (AP), *Adaptor* Wi-Fi TL-WN821N sebagai pendeteksi Wi-Fi di sekitar, dan Laptop sebagai sensor. TP-Link WN821N untuk mendeteksi sinyal Wi-Fi menggunakan airodump-ng. Pendeteksian sinyal Wi-Fi dilakukan menggunakan laptop dengan sistem operasi Linux Ubuntu dan perangkat lunak aircrack-ng. Aircrack-ng merupakan rangkaian perangkat lunak jaringan yang memiliki berbagai fungsi, termasuk sebagai alat deteksi, *packet sniffer*, *cracker* WEP, dan WPA/WPA2-PSK, serta alat analisis untuk jaringan LAN nirkabel 802.11. Subsistem ini menggunakan airodump-ng untuk mengumpulkan paket data Wi-Fi yang terdeteksi di sekitar alat. Dengan menggunakan airodump-ng, subsistem ini dapat mengidentifikasi dan merekam

berbagai informasi penting dari jaringan Wi-Fi yang dijadikan dataset untuk *Machine Learning* (ML).

C. Firebase Realtime Database

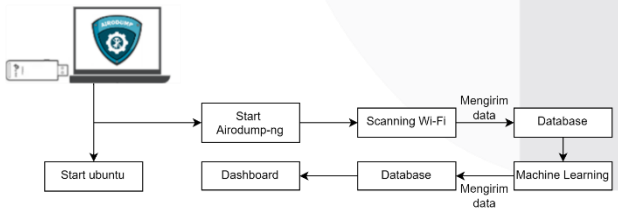
Firebase Realtime Database berfungsi sebagai pusat penyimpanan dan pendistribusian data secara *real-time*. *Database* ini menyediakan data yang diperlukan untuk proses klasifikasi menggunakan model *Machine Learning* (*Feedforward Neural Network*/FNN) di Google Colab untuk menentukan apakah jaringan yang dipindai merupakan *Rogue Access Point* (RAP) atau bukan. Hasil klasifikasi kemudian dikirim kembali dan disimpan di Firebase Realtime Database yang bertindak sebagai repositori utama. Data ini dapat diakses melalui *dashboard* untuk memantau kondisi jaringan Wi-Fi secara *real-time*. Dengan kemampuan sinkronisasi waktu nyata, Firebase Realtime Database memastikan bahwa setiap perubahan pada data dapat segera diperbarui dan dilihat di *dashboard* tanpa perlu penyegaran manual atau penundaan yang berarti, sehingga menjadikannya elemen penting dalam integrasi dan penyelarasan data di seluruh sistem.

D. Dashboard

Dashboard pada sistem ini berperan sebagai antarmuka pengguna yang memungkinkan pemantauan, analisis, dan respon cepat terhadap aktivitas jaringan nirkabel. Fungsinya mencakup visualisasi data deteksi yang disajikan dalam bentuk grafik, tabel, dan elemen visual lainnya. *Dashboard* menyediakan gambaran komprehensif tentang status keamanan jaringan dengan merinci deteksi impersonasi, identifikasi *Rogue Access Point* (RAP), dan aktivitas mencurigakan lainnya. Data yang dikirimkan dari Firebase secara *real-time* dan *update* di *dashboard* memungkinkan respon cepat terhadap ancaman yang mungkin muncul. Selain itu, *dashboard* juga dapat memberikan laporan yang terstruktur untuk memudahkan analisis.

III. METODE

A. Desain Sistem



GAMBAR 1.
IMPLEMENTASI UMUM TERKAIT WIDS

Pada gambar 1. menjelaskan beberapa langkah penting untuk memastikan keamanan jaringan nirkabel. Pengguna memulai dengan menghidupkan komputer dan masuk ke sistem operasi Ubuntu. Setelah itu, airodump-ng dijalankan di terminal Ubuntu untuk mulai memantau jaringan Wi-Fi. Airodump-ng dikonfigurasi untuk menyimpan output dalam format yang dapat dibaca oleh skrip Python. Dalam tahap scanning Wi-Fi, airodump-ng memindai jaringan Wi-Fi yang tersedia dan mengumpulkan data yang relevan. Skrip Python berjalan secara bersamaan untuk membaca *output* airodump-ng dan mengirimkan data tersebut ke *server backend*. *Server backend* bertanggung jawab untuk menerima dan menyimpan data ini di dalam database untuk analisis lebih lanjut.

Data yang telah tersimpan diklasifikasikan menggunakan model *Machine Learning* (ML). Model tersebut menganalisis karakteristik router yang terdeteksi dan mengklasifikasikannya untuk mengidentifikasi mana yang merupakan *Rogue Access Point* (RAP). Setelah analisis, data yang telah diproses, termasuk potensi ancaman atau peristiwa yang ditandai oleh model pembelajaran mesin, dikirim kembali ke database. Hasil analisis ini kemudian ditampilkan di *dashboard* dengan menanmpilkan visualisasi data yang jelas tentang kondisi jaringan. *Administrator* jaringan dapat melihat laporan *real-time* dan historis untuk memastikan keamanan jaringan. Dengan demikian, keseluruhan proses ini mencakup pengumpulan data, pengiriman ke *database*, analisis menggunakan ML, dan visualisasi hasil di *dashboard* yang secara kolektif memastikan keamanan jaringan nirkabel melalui deteksi dini dan respon cepat terhadap ancaman.

B. Implementasi Sistem

Implementasi dari sistem kontrol ini adalah dengan membuat *dashboard* sebagai media yang membantu proses monitoring hasil deteksi. *Dashboard* ini di desain dengan menggunakan aplikasi Visual Studio Code dan dengan menggunakan bahasa JavaScript dan HTML. Framework yang digunakan pada pembuatan website ini adalah framework React JS. Pemilihan framework ini didasarkan karena framework React Js menggunakan bahasa yang sederhana dan dapat dikombinasikan dengan bahasa pemrograman JavaScript. *Dashboard* ini memiliki dua fitur utama, yaitu dapat menampilkan hasil terdeteksinya *Rogue Access Point* (RAP) dan *Trusted Access Point* atau *access point* yang dapat dipercaya. Berikut merupakan tampilan dan fitur yang ada pada *dashboard* sistem ini.

GAMBAR 2.
WIDS DASHBOARD MENDETEKSI KEBERADAAN RAP

Gambar 2. menampilkan daftar SSID yang terdeteksi, lengkap dengan informasi kekuatan sinyal dan *channel* yang digunakan, serta menyediakan detail informasi yang lebih spesifik untuk setiap SSID yang dipilih. Selain itu, fitur ini memungkinkan pengguna untuk mengidentifikasi RAP dengan tampilan yang sederhana dan informatif.

GAMBAR 3.
WIDS DASHBOARD MENDETEKSI KEBERADAAN TRUSTED AP

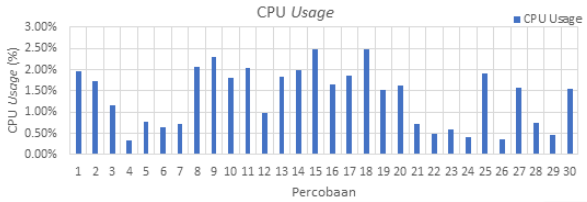
Gambar 3. menampilkan daftar SSID yang terdeteksi lengkap dengan informasi kekuatan sinyal dan *channel* yang digunakan. Saat sebuah SSID dipilih, detail informasinya akan ditampilkan di sebelah kanan, termasuk nama SSID, kekuatan sinyal, dan statusnya. Pengguna juga dapat menandai titik akses sebagai "*Trusted Access Point*" untuk membantu dalam pengelolaan dan keamanan jaringan.

IV. HASIL DAN PEMBAHASAN

Pada tahap ini dilakukan pengujian untuk memastikan bahwa *dashboard* berfungsi dengan baik. Terdapat dua pengujian yang dilakukan, yaitu pengujian CPU & *Memory Usage*, serta pengujian *User Experience Questionnaire* (UEQ).

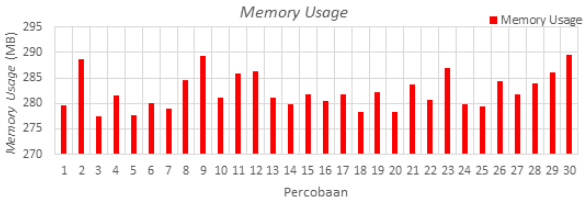
A. Pengujian CPU & *Memory Usage*

Pengujian CPU *Usage* dan *Memory Usage* merupakan langkah dalam memastikan bahwa *dashboard* yang telah dibuat mampu berkerja dengan baik dalam kondisi yang nyata. Pengujian ini bertujuan untuk mengevaluasi performa dari *dashboard*.



GAMBAR 4.
MENAMPILKAN GRAFIK CPU USAGE

Gambar 4. menampilkan grafik dari penggunaan CPU *Usage* yang menunjukkan bahwa sistem dapat menyesuaikan dengan berbagai beban kerja, menandakan fleksibilitas dan adaptabilitas yang baik. Penggunaan CPU menunjukkan nilai terendah sekitar 0,5% dan nilai tertinggi mendekati 2,5%. Hal ini menunjukkan bahwa beban kerja pada CPU bervariasi di antara percobaan, variasi ini dapat diakibatkan oleh perbedaan dalam jenis dan jumlah tugas yang dijalankan selama setiap percobaan. Hal ini menunjukkan adaptabilitas sistem terhadap berbagai beban kerja dengan rata-rata penggunaan CPU adalah sekitar 1,363%.



GAMBAR 5.
MENAMPILKAN GRAFIK MEMORY USAGE

Gambar 5. menampilkan grafik dari penggunaan memori yang stabil dengan beberapa lonjakan menunjukkan bahwa sistem memiliki manajemen memori yang baik. Penggunaan memori menunjukkan nilai yang berkisar antara 277,5 MB hingga hampir 290 MB. Meskipun ada variasi dalam penggunaan memori, rentang ini tetap relatif stabil, menunjukkan bahwa sistem memiliki manajemen memori yang efisien. Stabilitas ini penting untuk memastikan bahwa sistem tetap responsif dan dapat menangani beban kerja yang beragam tanpa mengalami masalah performa. Penggunaan memori yang stabil juga menunjukkan bahwa sistem tidak mengalami kebocoran memori atau penggunaan memori yang tidak efisien, yang dapat menyebabkan penurunan kinerja dalam jangka panjang, Dengan rata-rata penggunaan memori adalah sekitar 282,379 MB.

B. Pengujian *User Experience Questionnaire (UEQ)*

Untuk menilai pengalaman pengguna terhadap *dashboard*, maka dilakukan pengujian performa menggunakan metode *User Experience Questionnaire* (UEQ). Proses pengujian dimulai dengan menyusun kuesioner yang terdiri dari 26 komponen pertanyaan dengan 7 pilihan jawaban yang mencakup berbagai aspek kualitas *dashboard*. Adapun enam skala penilaian dalam UEQ yang digunakan untuk mengukur performa dashboard adalah sebagai berikut :

1. Daya Tarik (Attractiveness)

Menilai kesan keseluruhan pengguna terhadap dashboard, apakah mereka menyukai atau tidak menyukai tampilannya. Skala ini mencakup penilaian tentang apakah dashboard tersebut menarik, menyenangkan, dan memberikan kesan positif secara umum[3].

2. Kejelasan (Perspicuity)

Menilai seberapa mudah pengguna memahami dan belajar menggunakan dashboard, termasuk fitur-fitur dan navigasinya. Skala ini mencakup penilaian tentang apakah dashboard mudah dipahami, tidak membingungkan, dan mudah dipelajari oleh pengguna baru.

3. Efisiensi (Efficiency)

Mengukur seberapa cepat dan efisien pengguna dapat menyelesaikan tugas mereka menggunakan dashboard tanpa usaha yang tidak perlu. Skala ini mencakup penilaian tentang apakah dashboard memungkinkan pengguna menyelesaikan tugas dengan cepat dan tanpa hambatan.

4. Ketepatan (Dependability)

Mengukur sejauh mana pengguna merasa bahwa interaksi dengan dashboard dapat diandalkan dan konsisten. Skala ini mencakup penilaian tentang apakah dashboard memberikan rasa aman, dapat diprediksi, dan mendukung pengguna dalam menyelesaikan tugas mereka.

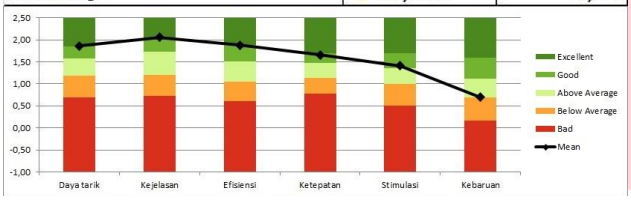
5. Stimulasi (Stimulation)

Mengukur sejauh mana dashboard memberikan kesan yang menarik dan menyenangkan bagi pengguna. Skala ini mencakup penilaian tentang apakah dashboard membuat pengguna merasa tertarik, termotivasi, dan terhibur saat menggunakannya.

6. Kebaruan (Novelty)

Mengukur sejauh mana dashboard dianggap inovatif dan menawarkan fitur atau desain yang baru dan menarik.

UEQ Scales (Mean and Variance)		
Attractiveness	1,859	0,82
Perspicuity	2,053	0,85
Efficiency	1,879	1,06
Dependability	1,659	0,64
Stimulation	1,409	0,64
Novelty	0,697	1,30



GAMBAR 6.
SKALA DAN GRAFIK UEQ

Berdasarkan gambar 6. hasil pengujian dengan metode *User Experience Questionnaire* (UEQ), analisis performa *dashboard* menunjukkan bahwa pengguna memberikan penilaian positif dalam beberapa aspek kunci. *Attractiveness* mendapat skor rata-rata 1,859 dengan variansi rendah 0,82 menunjukkan bahwa *dashboard* ini dianggap cukup menarik secara keseluruhan. *Perspicuity* mencatat skor tertinggi dengan rata-rata 2,053 dan variansi 0,85 menunjukkan bahwa pengguna merasa *dashboard* mudah dipahami dan dipelajari. *Efficiency* juga dinilai positif dengan skor 1,879 meskipun variansi yang sedikit lebih tinggi 1,06 menunjukkan adanya sedikit variasi dalam penilaian pengguna. *Dependability dashboard* mendapat skor 1,659 dengan variansi rendah 0,64 yang mencerminkan kepercayaan pengguna terhadap konsistensi kinerja *dashboard*. *Stimulation* dinilai cukup baik dengan skor 1,409 dan variansi 0,64 meskipun tidak setinggi aspek lainnya. Sementara itu, pada skala *novelty*, *dashboard* mendapatkan skor 0,697 dengan variansi yang cukup tinggi 1,30 menunjukkan bahwa pengguna merasa dashboard ini cukup inovatif dan terdapat perbedaan pendapat di antara pengguna.

V. KESIMPULAN

Penelitian ini menunjukkan bahwa *dashboard* yang dikembangkan untuk mendeteksi impersonasi router nirkabel mampu beroperasi dengan efisien dalam berbagai beban kerja. Berdasarkan pengujian CPU & *Memory Usage*, sistem menunjukkan adaptabilitas yang baik terhadap variasi beban kerja dengan penggunaan CPU rata-rata sekitar 13,63%. Selain itu, analisis performa menggunakan *User Experience Questionnaire* (UEQ) membuktikan bahwa pengguna memberikan penilaian positif terhadap dashboard ini, khususnya dalam aspek daya tarik, kejelasan, dan efisiensi. Pengguna merasa bahwa dashboard ini mudah dipahami dan cukup inovatif, meskipun terdapat sedikit variasi dalam penilaian terhadap efisiensinya. Keseluruhan hasil ini memperlihatkan bahwa dashboard yang diimplementasikan tidak hanya mendukung deteksi ancaman keamanan jaringan, tetapi juga memberikan pengalaman pengguna yang memuaskan .

REFERENSI

[1] E. Priezkalns, “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] Nur Fitriatus Shalihah, “Bahaya Asal Pakai Wifi Gratis di Publik, Ini Cara Aman dari Ahli,” Kompas.com. Accessed: Nov. 19, 2023. [Online]. Available: https://www.kompas.com/tren/read/2021/08/21/150000465/bahaya-asal-pakai-wifi-gratis-di-publik-ini-cara-aman-dari-ahli?page=all

[3] Schrepp Martin, “User Experience Questionnaire Handbook,” in User Experience Questionnaire (UEQ), 2023, pp. 1–16. [Online]. Available: www.ueq-online.org