Rancang Bangun Pendeteksi Serangan Deauthentication Pada Jaringan WiFi Berbasis ESP8266

(*Design and Development of Deauthentication Attack Detection on ESP8266 Based WiFi Networks***)**

Muhamad Nurbayazi[1]*, Ahmad Zafrullah M.[1], Ariyan Zubaidi[1,2]
[1]Dept Informatics Engineering, Mataram University
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: muhamadnurbayazi@gmail.com, *[*zaf, zubaidi13]@unram.ac.id

Abstract

In the modern era that is so tied to the internet, network security is important because the internet is basically insecure. To connect to an internet network, you can use a wireless network that uses an access point to transmit signals from WiFi. By using WiFi, users can enjoy communication at home, in the office or while traveling without having to bother using cables, but there are drawbacks to this benefit. Because wifi communications occur over the air, they can be intercepted easily. A relatively easy attack on a WiFi network is a deauthentication attack. A deauthentication attack is an attack that occurs because too many deauthentication messages are sent. This deauthentication message can be sent by the user's device or access point to notify the receiving device that their communications should be terminated. Apart from causing communication disruption between connected devices, deauthentication attacks are also the beginning of other follow-up attacks, one of which is the evil twin attack. To prevent further attacks, a deauthentication attack detection tool is needed so that by detecting deauthentication attacks, users or admins can take preventive and security measures against the WiFi network. This research aims to improve network security, especially WiFi networks, by designing and building a tool that detects and provides warnings when deauthentication attacks occur in the form of visual and audio warnings to WiFi users, both users and admins, by utilizing buzzers and LEDs as well as notifications via the Telegram application so that they can Minimize the occurrence of deauthentication attacks on ESP8266 NodeMCU based WiFi networks. Based on tool testing on 10 access point samples, the tool's percentage of success in detecting deauthentication attacks is 100%.

Keywords: *Internet, WiFi, Deauthentication, Telegram, NodeMCU ESP8266*

**Corresponding Author*

1. PENDAHULUAN

Pada zaman modern atau milenial yang sudah begitu terikat dengan internet ini, keamanan jaringan menjadi suatu hal yang tidak bisa diabaikan dan menjadi begitu penting dalam melindungi informasi sensitif, data serta privasi pengguna dalam lingkungan digital, karena internet yang sifatnya global dan publik pada dasarnya tidak aman. Keamanan jaringan membantu mencegah akses yang tidak sah, manipulasi data, penyadapan informasi, dan kerugian finansial yang dapat ditimbulkan akibat serangan atau pelanggaran keamanan.

Untuk terhubung ke jaringan internet saat ini dapat didapatkan dengan mudah menggunakan jaringan nirkabel atau WiFi, jaringan nirkabel menggunakan suatu perangkat yang dinamakan *access point* untuk menyebarluaskan sinyal dari WiFi sehingga semakin banyak pengguna yang dapat menggunakan internet.

Dengan menggunakan jaringan nikabel atau WiFi pengguna dapat menikmati komunikasi tanpa gangguan di rumah mereka, kantor, perpustakaan, kedai kopi atau saat berpergian tanpa kerumitan tentang kabel. Namun dari semua manfaat tersebut tentu saja terdapat kekurangan. Pada saat komunikasi WiFi terjadi melalui udara, komunikasi tersebut dapat disadap dengan mudah hanya beberapa meter dari titik *access point* yang sebenarnya. Jaringan WiFi rentan terhadap sejumlah serangan seperti *man in the middle*, *authentication*, *deauthentication*, *rogue* WiFi, *evil twin* dan lain-lain[1]. Serangan yang tergolong mudah dan umum terjadi pada jaringan WiFi adalah *deauthentication attack*, *deauthentication attack* ini akan membuat perangkat yang terhubung ke jaringan WiFi akan terputus.

Deauthentication attack merupakan serangan yang terjadi karena terlalu banyak pesan *deauthentication* yang dikirim. Pesan *deauthentication* ini dapat dikirim oleh perangkat pengguna atau *access point* untuk memberitahu perangkat penerima bahwa komunikasi mereka harus dihentikan[2]. Pada saat *access point* dalam jaringan ingin memutuskan sambungan dari jaringan, *access point* akan mengirimkan *deauthentication frame*, *deauthentication frame* ini termasuk dalam kategori *frame* manajemen. Kondisi sah pengiriman *frame deauthentication* adalah ketika ada perubahan *password* WiFi ataupun *client* berada di luar jangkauan jaringan. *Frame* manajemen di jaringan WiFi 802.11 tidak dienkripsi sehingga inilah potensi kerawanan yang menjadi alasan adanya serangan *deauthentication*[3]. Jika serangan tersebut terus berlangsung dapat menyebabkan gangguan komunikasi antar perangkat yang terhubung. *Deauthentication attack* dapat dengan mudah dilakukan dengan menggunakan perangkat lunak yang tersedia secara bebas dan perangkat keras yang murah[2].

Selain menyebabkan gangguan komunikasi antar perangkat yang terhubung, serangan *deauthentication* pada jaringan WiFi juga menjadi awal dari serangan lanjutan lainnya yang salah satunya adalah serangan *evil twin*[4]. Serangan *evil twin* merupakan teknik keamanan jaringan nirkabel di mana penyerang menciptakan *hotspot* WiFi palsu yang memiliki nama (SSID) yang sama dengan *hotspot* WiFi yang sah dan terpercaya yang sering digunakan pengguna dengan tujuan mencuri informasi sensitif seperti kata sandi, data kartu kredit, dan informasi pribadi lainnya. Untuk mencegah terjadinya serangan lanjutan yang berawal dari serangan *deauthentication* pada jaringan WiFi, diperlukan adanya alat deteksi serangan *deauthentication* sehingga dengan mendeteksi serangan *deauthentication* lebih awal, *user* ataupun admin dapat melakukan tindakan pencegahan dan pengamanan terhadap jaringan WiFi dengan cara memanggil tenaga ahli untuk memperkuat keamanan WiFi atau dengan cara mengganti *access point* dengan tipe terbaru yang sudah menerapkan enkripsi pada *frame* manajemen untuk mengatasi serangan *deauthentication*. Dengan adanya penelitian terkait rancang bangun pendeteksi serangan *deauthentication* pada jaringan WiFi berbasis ESP8266 yang dilengkapi dengan perangkat keras sederhana seperti *buzzer* dan LED, serta notifikasi melalui aplikasi pesan telegram, dengan mengintegrasikan *buzzer* dan LED pada NodeMCU ESP8266 dapat memberikan deteksi visual dan audio secara langsung terhadap serangan *deauthentication*. Selain itu, dengan menggunakan notifikasi melalui aplikasi pesan telegram, user maupun admin dapat menerima pemberitahuan terkait dengan serangan *deauthentication* yang terdeteksi sehingga memungkinkan untuk mengambil tindakan yang cepat dengan memanggil tenaga ahli untuk mengatasi serangan sehingga dapat mengurangi dampak dari serangan *deauthentication* maupun serangan yang berawal dari *deauthentication attack*.

Berdasarkan pemaparan di atas, penelitian ini bertujuan untuk meningkatkan keamanan jaringan khususnya pada jaringan WiFi dengan cara merancang dan membangun sebuah alat yang dapat mendeteksi dan memberikan peringatan ketika terjadinya serangan *deauthentication* berupa peringatan visual dan audio kepada pengguna WiFi baik itu user maupun admin dengan memanfaatkan *buzzer* dan LED serta notifikasi melalui aplikasi telegram sehingga bisa meminimalisir terjadinya serangan *deauthentication* pada jaringan WiFi berbasis NodeMCU ESP8266.

2. TINJAUAN PUSTAKA

Penelitian yang berjudul "*Pratically Detecting* WiFi *Deauthentication Attack*, 802.11 *Deauth Packets Using Python and Scapy Tech*". Penelitian tersebut melakukan deteksi serangan *deauthentication* dengan menggunakan beberapa *hardware* dan *software* seperti menggunakan sistem operasi linux karena memerlukan akses ke perangkat keras untuk mengubah kartu jaringan menjadi mode monitor, penelitian tersebut juga menggunakan kartu NIC dengan dukungan dalam mode monitor, *aireplay*-ng untuk melakukan serangan *deauthentication*, serta *scapy* yang digunakan untuk menganalisis semua paket Dot11 dengan *script python* kemudian mendeteksi serangan *deauthentication*[5]. Dalam beberapa hal, penelitian tersebut memiliki kesamaan dengan penelitian ini yaitu dalam hal melakukan deteksi serangan *deauthentication*, akan tetapi penelitian tersebut dan penelitian ini melakukan deteksi serangan *deauthentication* dengan cara serta alat yang berbeda. Penelitian ini melakukan deteksi serangan *deauthentication* menggunakan NodeMCU ESP8266 dengan tambahan *buzzer* dan LED serta notifikasi melalui aplikasi telegram sebagai tanda atau peringatan ketika adanya serangan *deauthentication* yang terdeteksi.

Penelitian yang berjudul "*An Automated Approach to Detect Deauthentication and*

*Disassociation Dos Attack*s *on Wireless* 802.11 *Networks*". Penelitian tersebut melakukan deteksi serangan *deauthentication* dan disassosiasi dengan menggunakan *script* yang ditulis dalam bahasa *python* dan dilakukan percobaan dengan menggunakan sistem operasi linux dan windows, untuk sistem operasi linux *script* yang digunakan berjalan dengan lancar, namun pada sistem operasi windows *script* tersebut tidak berjalan dengan baik karena keterbatasan perizinan untuk mode monitor[6]. Penelitian tersebut memiliki kesamaan dengan penelitian ini dalam hal jenis serangan yang akan dideteksi yaitu serangan *deauthentication*, namun memiliki perbedaan dalam melakukan deteksi serangan *deauthentication*, yaitu penelitian ini menggunakan alat berbasis NodeMCU ESP8266.

Penelitian yang berjudul "*Detection and Prevention of De-authentication Attack in Real-time Scenario*". Penelitian tersebut melakukan deteksi dengan menggunakan *Medium Access Control Spoof Detection and Prevention* (MAC SDP) *DoS alghoritm* yang telah dimodifikasi dari penelitian lain dengan judul "*Medium Access Control Spoof Detection and Prevention Alghorithm* (MAC SDP *DoS*) *for Spoofing Attacks in* WLAN" algoritma tersebut digunakan untuk mendeteksi dan mencegah serangan *deauthentication* yang diluncurkan dengan memalsukan alamat MAC dari klien yang sah. Penelitian tersebut memanfaatkan *access point* untuk membuat kunci sandi 8-bit dan dienkripsi dengan algoritma *Rivest-Shamir-Adleman* (RSA) untuk dikirimkan ke korban. Kesamaan penelitian tersebut dan penelitian ini yaitu dalam hal tujuan penelitian untuk mendeteksi serangan *deauthentication* namun dengan cara yang berbeda.

Penelitian yang berjudul "*Analysis of Deauthentication Attack on* IEEE 802.11 *Connectivity Based on IoT Technology Using External Penetration Test*". Penelitian ini melakukan analisis menggunakan metode *external penetration test* atau juga dikenal sebagai *black box penetration test* untuk menilai dan mengevaluasi nilai keamanan jaringan informasi. Penelitian tersebut melakukan serangan *deauthentication* pada IP *camera* dengan menggunakan modul ESP8266, alat NodeMCU dan juga Lua *programming*[7]. Terdapat kesamaan untuk penggunaan alat IoT pada penelitian tersebut dengan penelitian ini, yaitu menggunakan alat IoT NodeMCU ESP8266, namun terdapat perbedaan fungsi dan tujuan dalam menggunakan NodeMCU ESP8266 tersebut. Penelitian tersebut menggunakan NodeMCU ESP8266 untuk melakukan skema penyerangan *deauthentication*, sedangkan pada penelitian ini menggunakan NodeMCU ESP8266 untuk mendeteksi serangan *deauthentication*.

Penelitian yang berjudul "*Deauthentication* of IP *Drones and Cameras that Operate on* 802.11 WIFI *Stantards Using* ESP8266". Penelitian tersebut melakukan skema serangan *deauthentication* menggunakan NodeMCU ESP8266 pada IP *drone* dan kamera yang beroperasi pada 802.11 WiFi standar[8]. penelitian tersebut dan penelitian ini memiliki kesamaan pada alat yang digunakan yaitu NodeMCU ESP8266, namun berbeda pada penggunaan NodeMCU ESP8266, penelitian ini menggunakan NodeMCU ESP8266 untuk melakukan deteksi serangan *deauthentication*.

Berdasarkan tinjauan pustaka yang ada, terdapat beberapa kesamaan dan perbedaan antara penelitian terkait yang telah dilakukan dengan penelitian yang diajukan. Kesamaan terdapat pada jenis serangan yang dideteksi yaitu serangan *deauthentication* pada jaringan WiFi, namun terdapat perbedaan dalam hal metode serta alat yang digunakan untuk mendeteksi serangan *deauthentication* pada jaringan WiFi. Penelitian yang diajukan melakukan deteksi serangan *deauthentication* dengan menggunakan alat berbasis NodeMCU ESP8266 dengan tambahan *buzzer* dan LED serta notifikasi melalui aplikasi telegram sebagai tanda atau peringatan ketika mendeteksi adanya serangan *deauthentication* yang terjadi.

3. METODE PENELITIAN

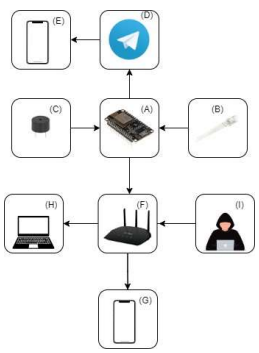
Analisi yang Memuat penjelasan tentang deskripsi sistem dan tahapan proses penelitian dengan urutan logis untuk mendapatkan hasil penelitian sesuai dengan harapan. Jika penjelasan proses penelitian menggunakan gambar dan tabel, maka gambar dan tabel harus disajikan dengan judul tabel dan gambar disertai dengan nomor urut. Contoh tabel seperti pada Tabel 1. Setiap tabel diberikan judul tabel yang diletakkan di atas tabel dengan *style* rata kiri, sedangkan judul gambar diletakkan di bawah gambar dengan *style* rata tengah. Rujukan tabel dan gambar di dalam teks diketik dengan nomer urut tabel dan gambar dengan huruf awal kapital, seperti Tabel I yang menyatakan fokus dan scope dari JTIKA.

3.1. Analisis Alat dan Bahan Penelitian

Pada tahap analisa kebutuhan, dilakukan analisa terhadap alat dan bahan yang dibutuhkan oleh sistem baik itu meliputi perangkat keras dan perangkat lunak, adapun alat dan bahan yang dibutuhkan sebagai berikut:

a. Laptop yang digunakan sebagai media dalam proses membuat codingan yang diperlukan untuk melakukan deteksi serangan *deauthentication* menggunakan NodeMCU ESP8266.
b. Sistem operasi yang digunakan adalah windows 8.1.
c. Aplikasi Arduino IDE untuk memprogramkan alat yang digunakan pada penelitian.
d. *Smarthpone* yang sudah terinstall aplikasi telegram untuk mendapatkan notifikasi dari hasil pemindaian dengan memanfaatkan bot dari aplikasi telegram.
e. NodeMCU ESP8266 digunakan sebagai media utama untuk melakukan deteksi serangan *deauthentication* pada jaringan WiFi. NodeMCU eso8266 juga nantinya akan dihubungkan dengan *buzzer* dan LED.
f. *Buzzer* digunakan sebagai media peringatan berupa suara ketika serangan *deauthentication* terdeteksi.
g. LED RGB digunakan sebagai media peringatan berupa visual, nantinya LED akan menyala dengan warna yang berbeda tergantung dari hasil deteksi yang didapatkan, jika serangan terdeteksi maka LED akan berwarna merah, sedangkan LED akan berwarna biru pada saat deteksi sedang dilakukan, kemudian LED akan berwarna hijau pada saat serangan telah berhenti.
h. Kabel jumper digunakan untuk menghubungkan komponen *buzzer* dan LED RGB pada NodeMCU ESP8266.

3.2. Rancangan Arsitektur Sistem



Gambar 1. Rancangan Arsitektur Sistem

Berikut merupakan penjelasan dari masing-masing proses serta hubungan setiap proses yang terdapat pada gambar1. di atas:

a. *Buzzer* (C) dihubungkan dengan NodeMCU ESP8266 sebagai media peringatan dalam bentuk suara ketika serangan *deauthentication* terdeteksi.
b. LED RGB (B) dihubungkan dengan NodeMCU ESP8266 digunakan sebagai media peringatan dalam bentuk visual ketika serangan terjadi maka LED akan menyala.
c. NodeMCU ESP8266 (A) sebagai media utama dalam melakukan pendeteksian serangan *deauthentication*. Pada saat NodeMCU ESP8266 (A) diaktifkan maka NodeMCU ESP8266 (A) akan langsung mencoba terhubung ke jaringan WiFi dari *hotspot smartphone* (E) yang telah diatur, kemudian NodeMCU ESP8266 (A) melakukan deteksi pada jaringan WiFi sekitar yang disebarkan menggunakan *access point* (F), pada saat NodeMCU ESP8266 (A) melakukan deteksi maka NodeMCU ESP8266 (A) akan mengaktifkan LED dengan warna biru sebagai tanda bahwa NodeMCU ESP8266 (A) sedang melakukan deteksi, kemudian jika NodeMCU ESP8266 (A) mendeteksi adanya serangan *deauthentication* maka NodeMCU ESP8266 akan memerintahkan *buzzer* (C) dan LED (A) untuk memberikan peringatan dalam bentuk suara dan visual LED berwarna merah, jika serangan telah berlangsung lebih dari 10 detik maka NodeMCU ESP8266 (A) akan menghentikan monitoring kemudian mematikan *buzzer* (C) dan menghidupkan LED berwarna hijau (B) serta mencoba untuk terhubung ke WiFi dari *hotspot smartphone* (E) untuk mengirimkan notifikasi melalui aplikasi telegram (D) yang sudah terinstall pada *device smartphone* (E). Namun, jika serangan yang terdeteksi berlangsung kurang dari 10 detik maka NodeMCU ESP8266 (A) tidak akan mengirimkan notifikasi melalui aplikasi telegram (D) dan hanya memberikan peringatan melalui LED berwarna merah (B) dan *buzzer* (C). Selanjutnya jika NodeMCU

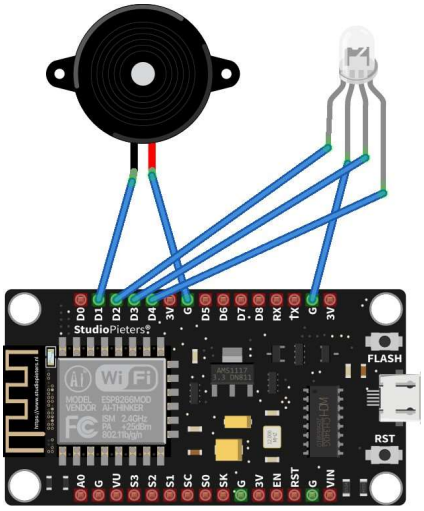
ESP8266 (A) telah mendeteksi serangan berhenti maka NodeMCU ESP8266 (A) akan menonaktifkan *buzzer* (C) dan mengaktifkan LED berwarna hijau (B).

d. Aplikasi telegram (D) sebagai media informasi ketika NodeMCU ESP8266 (A) telah melakukan deteksi serangan *deauthentication* pada jaringan WiFi.
e. Device smartphone (E) sebagai *device* yang sudah terinstall aplikasi telegram (D) dan terhubung ke NodeMCU ESP8266 (A) melalui *hotspot smartphone* (E) untuk kebutuhan internet dari NodeMCU ESP8266 (A) untuk terhubung dan mengirimkan notifikasi melalui aplikasi telegram (D) yang ada di *smartphone* (E).
f. *Access point* (F) merupakan salah satu perangkat yang dapat menyebarkan sinyal dari jaringan WiFi dan dapat di akses oleh banyak *device* seperti laptop (H), *smartphone* (G), maupun *device* lainnya, NodeMCU ESP8266 akan melakukan deteksi serangan *deauthentication* pada jaringan WiFi yang tersebar dengan bantuan perangkat keras seperti *access point* (F).
g. *Device* laptop (H) dan *smartphone* (G) merupakan *client* atau pengguna yang terhubung ke jaringan WiFi dari *access point* (F).
h. *Attacker* (I) atau penyerang merupakan seseorang yang melakukan serangan *deauthentication* pada jaringan WiFi dari *access point* (F), serangan *deauthentication* dapat membuat *client* (H) (G) yang terhubung ke jaringan WiFi melalui *access point* (F) menjadi terputus dan jika serangan *deauthentication* terus berlanjut maka *client* (H) (G) tidak akan bisa terhubung ke jaringan WiFi sampai serangan *deauthentication* berhenti.

3.3. Pembuatan Program Mikrokontroler

Pembuatan program mikrokontroler menggunakan *software* Arduino IDE dalam proses *coding* untuk program yang akan digunakan pada mikrokontroler NodeMCU ESP8266, pada tahap ini juga dilakukan konfigurasi sehingga nantinya mikrokontroler NodeMCU ESP8266 bisa terhubung ke telegram untuk mengirimkan hasil dari deteksi yang telah dilakukan dalam bentuk notifikasi chat.

3.4. Rancangan Perangkat Keras



Gambar 2. Rancangan Perangkat Keras

Pada gambar 2. di atas merupakan gambaran rancangan perangkat keras untuk alat yang dibuat, terdapat NodeMCU ESP8266 yang dihubungkan dengan *buzzer* dan LED RGB menggunakan kabel jumper. NodeMCU ESP8266 akan mencoba untuk terhubung ke jaringan WiFi yang telah diatur dan melakukan pendeteksian terhadap jaringan WiFi yang ada, NodeMCU ESP8266 akan mengaktifkan LED berwarna biru sebagai tanda bahwa NodeMCU ESP8266 sedang melakukan deteksi, jika NodeMCU ESP8266 mendeteksi serangan *deauthentication* maka NodeMCU ESP8266 akan mengaktifkan *buzzer* dan LED berwarna merah sebagai peringatan dalam bentuk suara dan visual sekaligus akan memberikan notifikasi melalui aplikasi telegram setelah serangan berlangsung selama lebih dari 10 detik bahwa terjadi serangan *deauthentication*. Jika serangan *deauthentication* yang telah terdeteksi sudah berhenti maka NodeMCU ESP8266 akan menonaktifkan *buzzer* dan mengaktifkan LED berwarna hijau

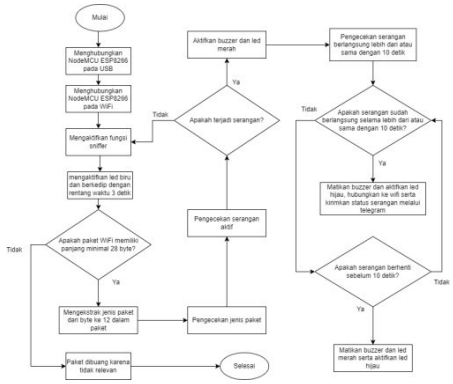
3.5. Pengujian dan Evaluasi Sistem

3.5.1. Pengujian Program Mikrokontroler

Pengujian program mikrokontroler dilakukan pada program yang telah dibuat sebelumnya menggunakan *software* Arduino IDE. Pengujian program mikrokontroler dilakukan untuk mengetahui

apakah program berhasil mendeteksi serangan *deauthentication* pada jaringan WiFi dengan cara melakukan skema serangan *deauthentication* menggunakan mikrokontroler NodeMCU ESP8266 lainnya. Pada pengujian ini juga sekaligus untuk mengetahui apakah mikrokontroler dapat terhubung ke aplikasi telegram.

3.5.2. Skenario Pengujian



Gambar 3. Skenario Pengujian

Pada tahap skenario pengujian akan dilakukan pengujian terhadap alat yang dirancang dengan melakukan serangan *deauthentication* terhadap *access point*. Pengujian ini bertujuan untuk mengetahui keberhasilan alat yang telah dirancang dalam mendeteksi serangan *deauthentication*. Adapun skenario pengujiannya sebagai berikut.

1. Langkah pertama dimulai dengan memasang NodeMCU ESP8266 pada usb, untuk usb yang digunakan merupakan usb *micro*, nantinya usb akan dihubungkan pada perangkat computer ataupun pada *powerbank* untuk mengaktifkan NodeMCU ESP8266.
2. Setelah NodeMCU ESP8266 aktif, mikrokontroler akan mencoba terhubung pada jaringan WiFi yang telah ditentukan kemudian mencoba koneksi ke server telegram.
3. Setelah koneksi ke jaringan WiFi dan server telegram berhasil, maka sesuai dengan program yang telah ada NodeMCU ESP8266 akan mengaktifkan fungsi *sniffer*, fungsi *sniffer* ini akan memeriksa setiap paket WiFi yang telah ditangkap.
4. Pada saat fungsi *sniffer* aktif, NodeMCU ESP8266 sedang melakukan monitoring sehingga akan mengaktifkan LED warna biru, LED akan berkedip dengan rentang waktu 3 detik aktif serta 3 detik tidak aktif.
5. Dalam fungsi *sniffer* ini ada beberapa hal yang dilakukan diantaranya adalah memeriksa apakah paket memiiki panjang yang memadai (minimal 28 *byte*), jika tidak, paket akan dibuang karena dianggap tidak relevan.
6. Langkah selanjutnya dalam fungsi *sniffer* juga akan mengekstrak jenis paket dari *byte* ke-12 dalam paket, yang merupakan separuh kedua dari *frame control field*.
7. Kemudian setelah jenis paket di ekstrak, program akan memeriksa apakah itu adalah jenis paket *deauthentication* atau *disassociation*. Dalam standar WiFi, jenis paket *deauthentication* memiliki kode 0xA0 dan jenis paket *disassociation* memiliki kode 0xC0.
8. Setelah program memeriksa jenis paket yang telah diekstrak, maka program melakukan pengecekan apakah terjadi serangan atau tidak, jenis paket yang diekstrak sebelumnya akan disimpan dalam sebuah variabel yang nantinya untuk menentukan terjadi serangan atau tidak program akan memeriksa apakah jumlah paket *deauthentication* yang ditangkap dalam interval waktu tertentu telah melebihi batas minimum yang ditetapkan. Jika ya, maka serangan dianggap aktif.
9. Jika serangan dianggap aktif, maka program akan mengaktifkan LED berwarna merah dan *buzzer*. Namun jika serangan dianggap tidak aktif maka program akan kembali menjalankan ulang dari mengaktifkan fungsi *sniffer*.
10. Langkah selanjutnya adalah ketika serangan dianggap aktif dan program mengaktifkan LED dan *buzzer*, program akan mengecek apakh serangan berlangsung lebih dari 10 detik.
11. Jika serangan telah berlangsung lebih dari 10 detik, maka program akan memaksa untuk mematikan *buzzer* dan mengaktifkan LED berwarna hijau serta mencoba untuk terhubung ke jaringan WiFi untuk mengirimkan notifikasi status serangan ke aplikasi telegram. Namun jika serangan berhenti sebelum melebihi rentang waktu 10 detik, maka program akan kembali melakukan pengecekan apakah serangan

berhenti sebelum melebihi rentang waktu 10 detik.

12. Jika iya, maka program akan mematikan *buzzer* dan LED warna merah kemudian mengaktifkan LED warna hijau sebagai tanda serangan telah berhenti. Namun jika serangan belum berhenti selama rentang waktu 10 detik, maka program akan kembali mengecek apakah serangan sudah berlangsung selama lebih dari 10 detik.

3.5.3. Pengujian *black box*

Pengujian *black box* dilakukan untuk mengetahui fungsi dari setiap fitur yang ada pada sistem pendeteksian serangan *deauthentication* pada jaringan WiFi, apakah sistem telah berjalan dengan baik.

Pengujian dilakukan dengan simulasi serangan dan deteksi serangan *deauthentication* pada 10 sampel jaringan WiFi yang rentan terhadap serangan *deauthentication* sehingga didapatkan tingkat keberhasilan deteksi menggunakan alat yang telah dirancang. Adapun hasil pengujian yang telah dilakukan, selanjutnya dilakukan perhitungan persentase keberhasilan menggunakan perhitungan sebagai berikut

$$\frac{Jumlah\ pengujian\ yang\ berhasil}{Jumlah\ pengujian} \times 100\% = \ldots$$

4. HASIL DAN PEMBAHASAN

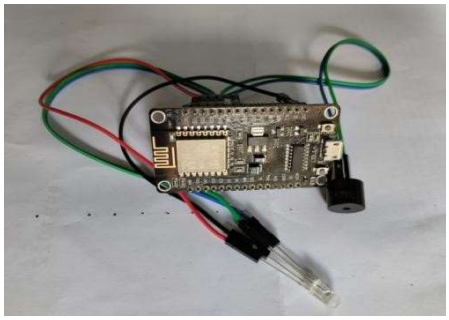
Bagian ini berisi hasil dan pembahasan penelitian. Hasil penelitian disajikan bentuk tabel atau grafik yang selanjutnya diberikan deskripsi dan pembahasan atas fakta yang diperoleh dikaitkan teori pendukung penelitian dan atau dibandingkan dengan hasil penelitian yang sangat terkait lainnya.

4.1. Realisasi Sistem

Realisasi sistem ini merupakan bagian yang akan membahas terkait dengan implementasi dari sistem yang telah dirancang serta hasil penelitian yang dilakukan tentang "Rancang Bangun Alat Pendeteksi Serangan *Deauthentication* pada Jaringan WiFi Berbasis ESP8266".

4.1.1. Realisasi penyusunan perangkat keras

Pembahasan pada sub bab ini membahas terkait dengan realisasi penyusunan perangkat keras dari pembuatan pendeteksi serangan *deauthentication* pada jarngan WiFi yang dibuat berdasarkan rancangan perangkat keras pada bab sebelumnya.



Gambar 4. Realisasi penyusunan perangkat keras

Gambar 4. adalah realisasi perangkat keras yang setiap alat dihubungkan untuk mendapatkan fungsi yang sesuai dengan tujuan penyusunan perangkat keras yang dibuat. Berikut merupakan fungsi dari setiap alat yang digunakan.

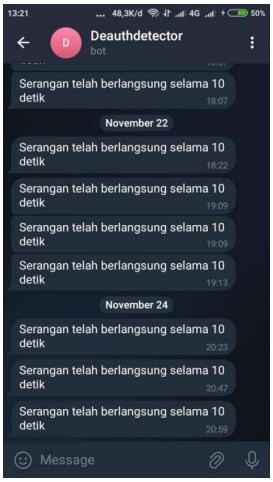
1. NodeMCU ESP8266 adalah perangkat yang digunakan sebagai mikrokontroler yang menjadi inti dan mengontrol keseluruhan kerja alat. NodeMCU ESP8266 digunakan sebagai alat untuk memonitoring jaringan WiFi yang ada dalam jangkauannya, selain untuk memonitoring NodeMCU ESP8266 juga digunakan untuk terhubung ke jaringan internet melalui koneksi WiFi yang kemudian NodeMCU ESP8266 akan terhubung ke server telegram untuk mengirimkan notifikasi melalui aplikasi telegram.
2. LED RGB, adalah alat yang dapat menghasilkan cahaya atau sinar dengan 3 warna yaitu merah, hijau dan biru. LED disini berfungsi untuk memberikan pemberitahuan secara visual ketika NodeMCU ESP8266 sedang bekerja, untuk cahaya yang dihasilkan akan berbeda sesuai dengan apa yang sedang dilakukan oleh NodeMCU ESP8266. LED warna merah untuk kondisi serangan *deauthentication* terdeteksi, LED warna hijau untuk kondisi serangan *deauthentication* telah berhenti, dan LED warna biru untuk kondisi NodeMCU ESP8266 sedang melakukan monitoring pada jaringan WiFi.
3. *Buzzer*, adalah alat yang dapat menghasilkan suara sebagai peringatan secara audio ketika NodeMCU ESP8266 mendeteksi adanya serangan *deauthentication* pada jaringan WiFi.

4.1.2. Realisasi program mikrokontroler

Realisasi program mikrokontroler menggunakan *software* Arduino IDE. Pada pemrograman mikrokontroler ini terdapat beberapa bagian program yang digunakan untuk melakukan monitoring pada jaringan WiFi sehingga dapat mendeteksi serangan *deauthentication* yang terjadi, terhubung ke server telegram untuk notifikasi adanya serangan.

4.1.3. Realisasi interface sistem

Pada bagian ini akan membahas terkait dengan realisasi *interface* sistem yang memanfaatkan aplikasi pesan telegram dengan salah satu fiturnya yaitu bot telegram. Berikut merupakan hasil dari realisasi *interface* sistem yang memanfaatkan aplikasi pesan telegram yang digunakan sebagai notifikasi dari alat deteksi serangan *deauthentication* pada jaringan WiFi berbasis NodeMCU ESP8266.



Gambar 5. Realisasi *Interface* Sistem

Gambar 5. merupakan realisasi *interface* sistem yang memanfaatkan aplikasi pesan telegram untuk notifikasi dari alat deteksi serangan *deauthentication* pada jariingan WiFi berbasis NodeMCU ESP8266. *Interface* dari sistem hanya untuk menampilkan notifikasi bahwa serangan telah berlangsung selama 10 detik, jika alat mendeteksi serangan namun berhenti sebelum 10 detik maka alat tidak akan mengirimkan notifikasi namun tetap memberikan peringatan secara audio dan visual menggunakan *buzzer* dan LED.

4.2. Pengujian Sistem

Pada sub bab ini merupakan tahap pengujian sistem untuk mengetahui apakah sistem yang dibangun berupa perangkat keras dan perangkat lunak dapat berjalan sesuai dengan yang direncanakan.

4.2.1. Pengujian *black box*

Pengujian *black box* dilakukan untuk mengamati serta menganalisa terkait fungsionalitas dari fitur yang terdapat pada alat deteksi serangan *deauthentication* pada jaringan WiFi. Hal tersebut dilakukan untuk memastikan apakah semua fitur yang ada pada alat yang telah dirancang dapat berjalan sesuai dengan yang diharapkan. Berikut merupakan hasil pengujian *black box*.

TABEL 1. PENGUJIAN BLACK BOX

No	Kondisi	Hasil yang diharapkan	Ya	Tidak
1.	NodeMCU ESP8266 aktif	NodeMCU ESP8266 berhasil terhubung ke jaringan WiFi	√	
		NodeMCU ESP8266 berhasil terhubung ke server telegram	√	
2.	NodeMCU ESP8266 memonitoring serangan *deauthentication*	NodeMCU ESP8266 mengaktifkan LED berwarna biru dan berkedip dengan durasi 3 detik	√	
3.	NodeMCU ESP8266 mendeteksi serangan *deauthentication*	NodeMCU ESP8266 mengaktifkan *buzzer*	√	
		NodeMCU ESP8266 mengaktifkan LED berwarna merah	√	
4.	NodeMCU ESP8266 mendeteksi serangan berhenti sebelum melebihi rentang waktu 10 detik	NodeMCU ESP8266 menonaktifkan *buzzer*	√	
		NodeMCU ESP8266 menonaktifkan LED merah	√	
		NodeMCU ESP8266 mengaktfikan LED hijau	√	
5.	NodeMCU ESP8266 setelah mendeteksi serangan *deauthentication* berlangsung selama 10 detik	NodeMCU ESP8266 menonaktifkan *buzzer*	√	
		NodeMCU ESP8266 menonaktifkan LED merah	√	
		NodeMCU ESP8266 mengaktifkan LED hijau	√	
		NodeMCU ESP8266 terkoneksi ke jaringan WiFi	√	
		NodeMCU ESP8266 mengirimkan notifikasi ke apliasi telegram	√	

4.2.2. Hasil Pengujian Keseluruhan Sistem

Pengujian keseluruhan sistem dilakukan pada tanggal 19 November 2023 – 24 November 2023. Pengujian dilakukan pada 13 fungsi yang ada pada alat yang telah dirancang, dilakukan pada 10 *access point* yang berlokasi di beberapa dusun di daerah desa Labulia Lombok tengah dan Kuripan Lombok barat. pengujian dilakukan dengan melakukan skema serangan *deauthentication* pada access point. Adapun hasil dari pengujian yang telah dilakukan adalah sebagai berikut:

TABEL 2. HASIL PENGUJIAN KESELURUHAN SISTEM

No	Jenis Access Point	Hasil Pengujian					
		Durasi pengujian	*Buzzer*	LED			Notif
				R	G	B	
1.	TENDA AC 6	3 menit	✓	✓	✓	✓	✓
2.	ZTE ZXHN F609	2 menit	✓	✓	✓	✓	✓
3.	Huawei HG8245H	5 menit	✓	✓	✓	✓	✓
4.	Huawei HG8245H	2 menit	✓	✓	✓	✓	✓
5.	Net1 LOG U-270	3 menit	✓	✓	✓	✓	✓
6.	ZTE ZXHN F609	2 menit	✓	✓	✓	✓	✓
7.	FiberHome HG6243C	2 menit	✓	✓	✓	✓	✓
8.	Huawei HG8245H	6 menit	✓	✓	✓	✓	✓
9.	ZTE ZXHN F609	3 menit	✓	✓	✓	✓	✓
10.	FiberHome HG6243C	2 menit	✓	✓	✓	✓	✓

Berdasarkan Tabel 2. Didapatkan hasil pengujian terhadap 10 *access point* yang tealh diujikan. Semua serangan *deauthentication* yang terjadi dapat terdeteksi sehingga dapat disimpulkan bahwa alat yang telah dirancang dapat bekerja dengan baik.

Berdasarkan hasil pengujian yang telah dilakukan dengan jumlah pengujian yang berhasil berjumlah 10 dan kegagalan 0. Berikut merupakan perhitungan persentase keberhasilan alat yang telah dirancang:

$$\frac{10}{10}\ X\ 100\% = 100\%$$

Berdasarkan hasil perhitungan persentase keberhasilan alat yang tealh dirancang, didapatkan hasil 100%.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian dan pengujian yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Berdasarkan hasil pengujian yang dilakukan, persentase keberhasilan yaitu 100% sehingga dapat ditarik kesimpulan bahwa alat yang dirancang dapat berjalan sesuai dengan yang diharapkan.
b. Selama pengujian dilakukan terdapat kondisi jaringan yang digunakan mikrokontroler kurang stabil sehingga mengakibatkan pesan notifikasi gagal terkirim.

5.2. Saran

Jika dilakukan penelitian lebih lanjut terkait dengan penelitian ini untuk kedepannya, berikut merupakan saran yang dapat dipertimbangkan untuk menjadi acuan pengembangan sistem berikutnya:

a. Disarankan menggunakan jaringan yang stabil untuk koneksi mikrokontroler agar terhindar dari kegagalan mikrokontroler mengirimkan notifikasi melalui telegram.
b. Disarankan melakukan metode pengujian dengan skema serangan *deauthentication* yang bervariasi untuk mengetahui apakah alat tetap bekerja sesuai dengan yang diharapkan.
c. Untuk meminimalisir serangan *deauthentication* dapat melakukan penggantian perangkat *access point* dengan perangkat terbaru yang dapat mencegah serangan *deauthentication*.
d. Untuk mencegah kerusakan dini pada alat yang dirancang, disarankan untuk

mempertimbangkan arus listrik dan tegangan listrik yang digunakan pada alat.

DAFTAR PUSTAKA

[1] M. Agarwal, S. Biswas, and S. Nandi, "*An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in* 802.11 Wi-Fi *Networks*," *Int. J. Wirel. Inf. Networks*, vol. 25, no. 2, pp. 130–145, 2018, doi: 10.1007/s10776-018-0396-1.

[2] A. Amoordon, V. Deniau, A. Fleury, and C. Gransart, "*A Single Supervised Learning Model to Detect Fake Access Points, Frequency Sweeping Jamming and Deauthentication Attacks in* IEEE 802.11 *Networks*," *Mach. Learn. with Appl.*, vol. 10, no. June, p. 100389, 2022, doi: 10.1016/j.mlwa.2022.100389.

[3] P. R. Janardhan, Karthikeyan, "*Comparing Naive Bayes Classifier with Random Forest Classifier for Accurate Deauthentication Attack Detection .*," vol. 10, pp. 1552–1562, 2023.

[4] R. Rinaldi and M. Sadikin, "Analisa dan Pengujian Serangan *Evil Twin* pada Jaringan berbasis *Wireless* dengan Keamanan WPA2-PSK," *Ph. D. diss.*, no. September, 2019, [Online]. Available: https://www.researchgate.net/profile/Roy-Renaldi/publication/335929306_Analisa_dan_Pengujian_Serangan_Evil_Twin_pada_Jaringan_berbasis_Wireless_dengan_Keamanan_WPA2-PSK/links/5d84c06a92851ceb791dee47/Analisa-dan-Pengujian-Serangan-Evil-Twin-pada-Jaringan-

[5] R. Poudél, "*Practically Detecting WiFi Deauthentication Attack*, 802.11 *Deauth Packets using Python and Scapy*," no. August, 2020.

[6] H. A. Noman, S. M. Abdullah, and H. I. Mohammed, "*An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless* 802 . 11 *Networks*," *IJCSI Int. J. Comput. Sci. Issues*, vol. 12, no. 4, pp. 107–112, 2015.

[7] Y. Kristiyanto and E. E, "*Analysis of Deauthentication Attack on* IEEE 802.11 *Connectivity Based on IoT Technology using External Penetration Test*," *CommIT (Communication Inf. Technol. J.*, vol. 14, no. 1, p. 45, 2020, doi: 10.21512/commit.v14i1.6337.

[8] S. R. Gopal *et al.*, "*Deauthentication of IP Drones and Cameras that Operate on* 802 . 11 *Wifi Standards using* ESP8266," vol. 10, no. 2, pp. 23–30, 2019.

[9] Yusantono, "Analisis dan Perbandingan Jaringan WiFi dengan frekuensi 2 . 4 GHz dan 5 GHz dengan Metode QoS," vol. 05, no. 05, pp. 34–52, 2020.

[10] A. M. Lukman and Y. Bachtiar, "Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet pada IT Telkom Purwokerto," vol. 6, no. 2, pp. 49–56, 2018.

[11] M. A. Abdillah, A. Yudhana, and A. Fadil, "*Sniffing* Pada Jaringan WiFi Berbasis Protokol 802.1x Menggunakan Aplikasi *Wireshark*," *J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, p. 1, 2020, doi: 10.30645/j-sakti.v4i1.181.

[12] Michael, I. Ruslianto, and R. Hidayati, "Analisis Perbandingan Sistem Keamanan Jaringan Wi-Fi *Protected Access* 2-Pre *Shared Key* (Wpa2-Psk) Dan *Captive* Portal Pada Jaringan Publik *Wireless*," *J. Komput. dan Apl.*, vol. 09, no. 01, pp. 108–118, 2021.

[13] J. O. Agyemang, J. J. Kponyo, G. S. Klogo, and J. O. Boateng, "*Lightweight Rogue Access Point Detection Algorithm for* WiFi-enabled *Internet of Things*(IoT) *devices*," *Internet of Things (Netherlands)*, vol. 11, p. 100200, 2020, doi: 10.1016/j.iot.2020.100200.

[14] R. Hermawan and A. Abdurrohman, "Pemanfaatan Teknologi *Internet of Things* pada Alarm Sepeda Motor Menggunakan NodeMCU LoLiN V3 dan Media Telegram," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 5, no. 2, p. 58, 2020, doi: 10.32897/infotronik.2020.5.2.453.

[15] M. R. Hidayat, C. Christiono, and B. S. Sapudin, "Perancangan Sistem Keamanan Rumah Berbasis IoT dengan NodeMCU ESP8266 menggunakan Sensor PIR HC-SR501 dan Sensor *Smoke Detector*," *Kilat*, vol. 7, no. 2, pp. 139–148, 2018, doi: 10.33322/kilat.v7i2.357.

[16] S. Samsugi, Ardiansyah, and D. Kastutara, "*Internet of Things* (IoT): Sistem Kendali Jarak Jauh Berbasis Arduino Dan Modul Wifi ESP8266," *Pros. Semin. Nas. ReTII*, pp. 295–303, 2018.

[17] N. H. L. Dewi, M. F. Rohmah, and S. Zahara, "*Prototype Smart Home* dengan NodeMCU ESP8266 Berbasis IoT," *J. Ilm. Tek.*, vol. 1, no. 2, pp. 101–107, 2022, doi: 10.56127/juit.v1i2.169.

[18] M. D. Arniyanto, J. D. Irawan, and F. S. Wahyuni, "Rancang Bangun Alat Pengisian Minuman Dan Monitoring Air Galon Berbasis IoT (*Internet of Things*)," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 5, no. 2, pp. 565–572, 2021, doi: 10.36040/jati.v5i2.3807.

[19] E. E. Prasetiyo, "Aplikasi *Internet of Things* (IoT) untuk Pemantauan dan Pengendalian Beban Listrik Di Ruangan," *J. Tek. STTKD*, vol. 4, no. 2, pp. 28–35, 2017.

[20] M. Jamil, H. Saefudin, and S. Marasabessy, "Sistem Peringatan Dini Kebakaran Hutan Menggunakan Modul NodeMCU dan Bot Telegram dengan Konsep *Internet of Things* (IoT)," vol. 3, pp. 1–5,2019, doi:10.30865/komik.v3i1.155