

**SISTEM DETEKSI SERANGAN DEAUTHENTICATION
FRAME BERBASIS NODEMCU ESP8266 DAN
SOLUSI WI-FI ALTERNATIF BERBASIS
MIKROKONTROLER ESP32**

SKRIPSI



disusun oleh

**DZULFIQAR AHMAD SYAIFULLAH ARIANTO
21.83.0715**

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2025

**SISTEM DETEKSI SERANGAN DEAUTHENTICATION
FRAME BERBASIS NODEMCU ESP8266 DAN
SOLUSI WI-FI ALTERNATIF BERBASIS
MIKROKONTROLER ESP32**

SKRIPSI



disusun oleh

DZULFIQAR AHMAD SYAIFULLAH ARIANTO

21.83.0715

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2025

HALAMAN PERSETUJUAN

SKRIPSI
SISTEM DETEKSI SERANGAN DEAUTHENTICATION
FRAME BERBASIS NODEMCU ESP8266 DAN
SOLUSI WI-FI ALTERNATIF BERBASIS
MIKROKONTROLER ESP32

yang disusun dan diajukan oleh

DZULFIQAR AHMAD SYAIFULLAH ARIANTO

21.83.0715

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Mei 2025

Dosen Pembimbing,



Muhammad Kopravi, S.Kom., M.Eng

NIK. 190302454

HALAMAN PENGESAHAN

SKRIPSI

**SISTEM DETEKSI SERANGAN DEAUTHENTICATION FRAME
BERBASIS NODEMCU ESP8266 DAN SOLUSI WI-FI ALTERNATIF
BERBASIS MIKROKONTROLER ESP32**

yang disusun dan diajukan oleh

DZULFIQAR AHMAD SYAIFULLAH ARIANTO

21.83.0715

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Mei 2025

Susunan Dewan Penguji

Nama Penguji

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

Muhammad Kopravi, S.Kom., M.Eng
NIK. 190302454

Tanda Tangan



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Mei 2025

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : DZULFIQAR AHMAD SYAIFULLAH ARIANTO

NIM : 21.83.0715

Menyatakan bahwa Skripsi dengan judul berikut:

Sistem Deteksi Serangan Deauthentication Frame Berbasis NodeMCU ESP8266 Dan Solusi Wi-Fi Alternatif Berbasis Mikrokontroler ESP32

Dosen Pembimbing : Muhammad Kopravi, S.Kom., M.Eng.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Mei 2025

Yang Menyatakan,



Dzulfiqar Ahmad Syaifullah Arianto

KATA PENGANTAR

Alhamdulillah, puji syukur ke hadirat Allah SWT, karena atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan skripsi yang berjudul “Sistem Deteksi Serangan Deauthentication Frame Berbasis NodeMCU ESP8266 Dan Solusi Wi-Fi Alternatif Berbasis Mikrokontroler ESP32”. Skripsi ini disusun sebagai salah satu syarat kelulusan Program Sarjana Teknik Komputer dari Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta. Penulis menyadari bahwa tanpa bimbingan, dukungan, dan doa dari berbagai pihak, penyusunan skripsi ini tidak akan berjalan dengan lancar. Oleh karena itu, dengan segala kerendahan hati, penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa, atas segala nikmat dan kemudahan dalam menyelesaikan Skripsi ini.
2. Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Muhammad Koprari, S.Kom., M.Eng., selaku dosen pembimbing yang telah memberikan arahan serta masukan yang sangat berharga selama sesi bimbingan.
4. Kedua orang tua dan keluarga tercinta, Bapak Antok Trihadjanto dan Ibu Arie Purbowatie yang selalu memberikan doa, dukungan, dan semangat tanpa henti.
5. Teman-teman dan sahabat, yang telah memberikan bantuan, motivasi, serta kebersamaan dalam proses penyusunan skripsi ini.

Penulis menyadari bahwa penelitian ini masih banyak keterbatasan. Oleh karena itu peneliti berharap penelitian ini kedepan memiliki kemajuan kepada peneliti dengan tujuan yang sama, yaitu menciptakan keamanan jaringan Masyarakat.

Yogyakarta, 15 Mei 2025

Penulis

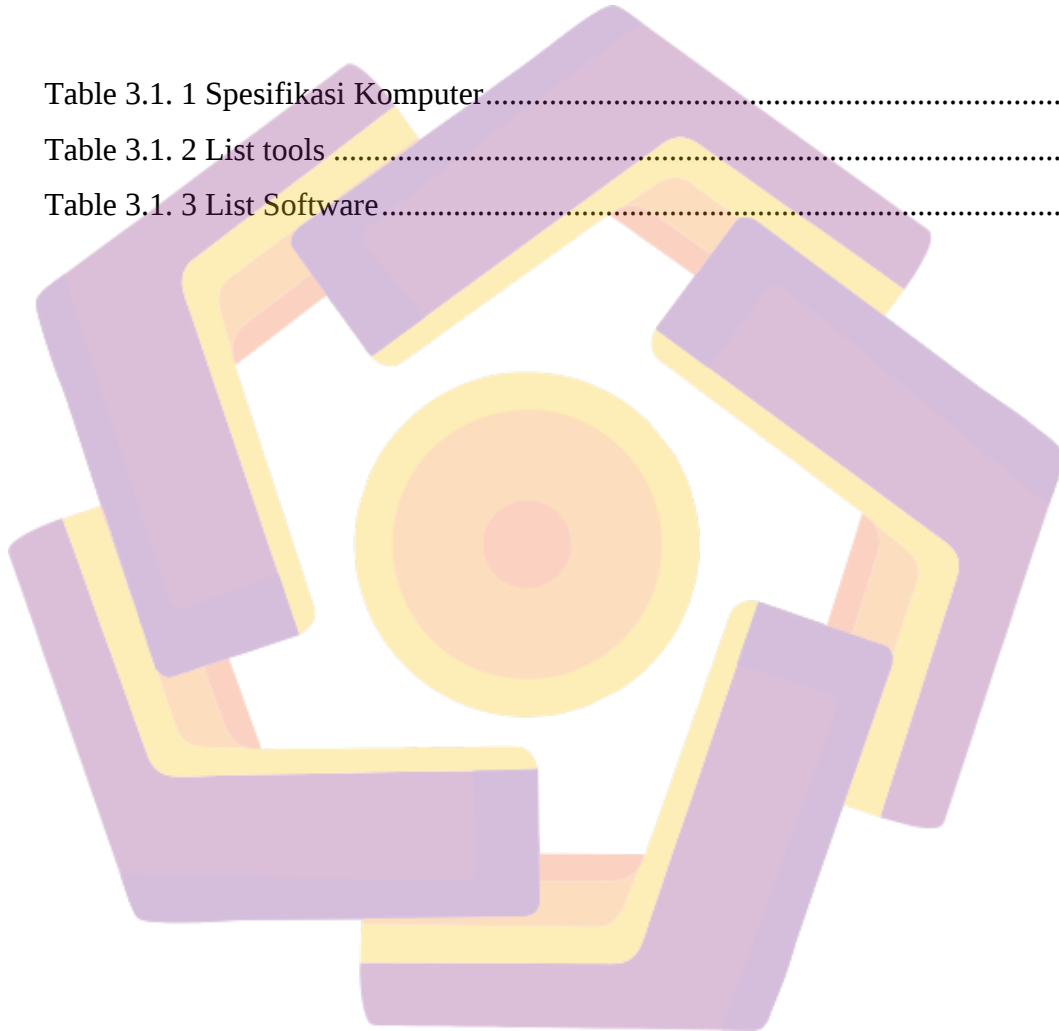
DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN.....	Error! Bookmark not defined.
HALAMAN PENGESAHAN	Error! Bookmark not defined.
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMPIRAN.....	xv
DAFTAR LAMBANG DAN SINGKATAN	xvi
DAFTAR ISTILAH	xvii
INTISARI	xviii
<i>ABSTRACT</i>	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA	5
2.1 Studi Literatur	5
2.2 Dasar Teori.....	12
BAB III METODE PENELITIAN	32

3.1	Objek Penelitian	32
3.2	Alur Penelitian.....	33
BAB IV HASIL DAN PEMBAHASAN		49
4.1	Perancangan Sistem.....	49
4.2	Skenario Pengujian.....	89
4.3	Faktor yang Mempengaruhi	111
4.4	Hasil Efektivitas dan Akurasi Waktu Respon Pada NodeMCU ESP8226 Secara General atau Keseluruhan	113
BAB V PENUTUP		117
5.1	Kesimpulan.....	117
5.2	Saran.....	118
REFERENSI		120
LAMPIRAN.....		123

DAFTAR TABEL

Table 2. 1 Keaslian Penelitian	8
Table 2. 2 ESP32 Specification.....	15
Table 2. 3 Nodemcu & ESP8266 Specification.....	18
Table 3.1. 1 Spesifikasi Komputer.....	45
Table 3.1. 2 List tools	45
Table 3.1. 3 List Software.....	46



DAFTAR GAMBAR

Gambar 2.1. 1 Konsep IoT - Cloud System.....	12
Gambar 2.1. 2 Konsep IoT Multi-Function	13
Gambar 2.1. 3 Arduino IDE.....	14
Gambar 2.1. 4 ESP32 PINOUT	16
Gambar 2.1. 5 Wemos D1 ESP8266.....	17
Gambar 2.1. 6 NodeMCU V3	18
Gambar 2.1. 7 Visual Studio Code	20
Gambar 2.1. 8 GitHub.....	21
Gambar 2.1. 9 LCD I2C.....	22
Gambar 2.1. 10 PlatformIO	23
Gambar 2.1. 11 ESP-IDF	23
Gambar 2.1. 12 Wi-Fi Extender.....	24
Gambar 2.1. 13 Supabase.....	26
Gambar 2.1. 14 Vercel	27
Gambar 2.1. 15 Kali Linux	27
Gambar 2.1. 16 VirtualBox.....	28
Gambar 2.1. 17 Adapter Wi-Fi	29
Gambar 2.1. 18 Wireshark	29
Gambar 2.1. 19 Aircrack-ng Tools	30
 Gambar 3.1. 14 Objek Penelitian.....	 32
Gambar 3.1. 1 Alur Penelitian	33
Gambar 3.1. 2 Flowchart ESP32 NAT Router	35
Gambar 3.1. 3 Web Dashboard.....	36
Gambar 3.1. 4 Result Page.....	37
Gambar 3.1. 5 Apply.....	37
Gambar 3.1. 6 Flowchart NodeMCU - ESP32	38
Gambar 3.1. 7 Output Sniffer NodeMCU.....	39
Gambar 3.1. 8 Output I2C.....	40

Gambar 3.1. 9 Output Serial Monitor	40
Gambar 3.1. 10 Output Pada I2C	41
Gambar 3.1. 11 Table Data	42
Gambar 3.1. 12 realtime vercel	43
Gambar 3.1. 13 historic vercel	44
Gambar 3.1. 15 Skematik detector/packet sniffer, I2C, dan ESP32	46
Gambar 4. 13 Front-End	49
Gambar 4. 14 Back-End	50
Gambar 4. 15 About.html	50
Gambar 4. 16 Advanced.html	51
Gambar 4. 17 Fungsi txpower	52
Gambar 4. 18 wifi tx_power	52
Gambar 4. 19 Advanced.html Bandwidth Option	53
Gambar 4. 20 Backend Bandwidth	53
Gambar 4. 21 Advanced.html (2)	54
Gambar 4. 26 Advanced.html (3)	55
Gambar 4. 35 Back-end Apply	56
Gambar 4. 37 Tampilan Halaman clients.html	56
Gambar 4. 41 Halaman Konfigurasi	57
Gambar 4. 47 Tampilan Halaman Lock UI	58
Gambar 4. 52 Portmap config	59
Gambar 4. 53 back-end portmap	60
Gambar 4. 54 Back-end portmap	61
Gambar 4. 55 portmap_end.html "protocol"	61
Gambar 4. 56 external port	62
Gambar 4. 57 ambil ip	62
Gambar 4. 58 mengambil ipport	63
Gambar 4. 59 table portmap router_globals.h	64
Gambar 4. 60 Tampilan OTA (Over The Air)	64
Gambar 4. 61 Back-end ota	65

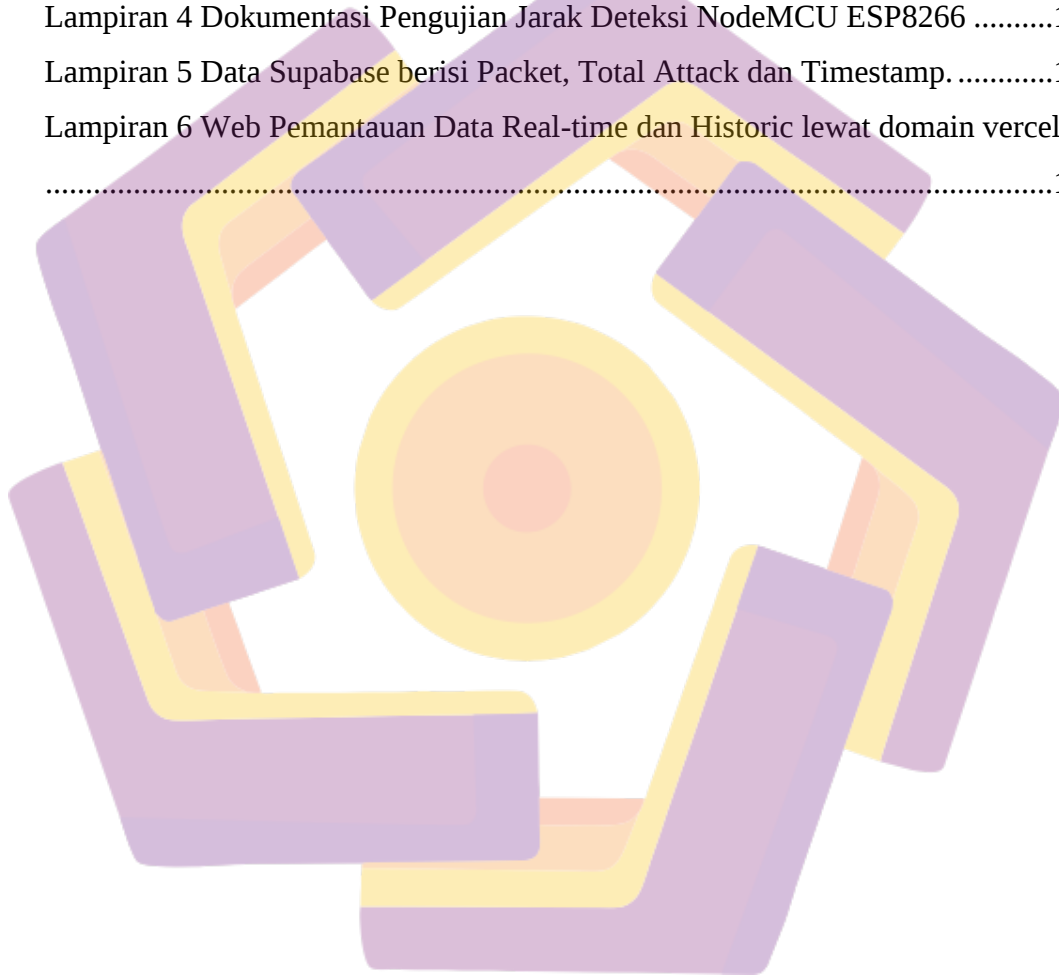
Gambar 4. 62 Embed Files.....	66
Gambar 4. 63 ota.html %s.....	66
Gambar 4. 64 Wifi Scan button	67
Gambar 4. 65 Back-end scanhandler.c.....	68
Gambar 4. 66 Back-end scan.c.....	68
Gambar 4. 67 Proses scan	69
Gambar 4. 68 Hasil Scan	69
Gambar 4. 69 resulthandler.c	70
Gambar 4. 70 Broadcast ESP32_NAT_Router.....	71
Gambar 4. 71 Hasil Scan	72
Gambar 4. 72 Connected, secured	73
Gambar 4. 73 Library NodeMCU	73
Gambar 4. 74 Fungsi Channel dan Variable Runtime	75
Gambar 4. 75 Variabel Time.....	75
Gambar 4. 76 Reset.....	76
Gambar 4. 77 Fungsi SNIFFER.....	76
Gambar 4. 78 update display.....	77
Gambar 4. 79 Fungsi attack_started dan stopped	77
Gambar 4. 80 Fungsi kirim data.....	78
Gambar 4. 81 sniffer_start	78
Gambar 4. 82 if reset timer	79
Gambar 4. 83 if update time.....	79
Gambar 4. 84 Logika Serangan	80
Gambar 4. 85 Display I2C	80
Gambar 4. 86 Send to ESP32S3	81
Gambar 4. 87 Mengganti Channel	81
Gambar 4. 88 Konfigurasi ESP32-S3	81
Gambar 4. 89 Library ESP32 - S3	82
Gambar 4. 90 preferences esp32s3	82
Gambar 4. 91 Menyimpan Jumlah Paket dan total attack.....	82
Gambar 4. 92 Penyimpanan SSID dan Password	83

Gambar 4. 93 WiFi ditemukan.....	83
Gambar 4. 94 startAP()	84
Gambar 4. 95 Konfigurasi NTP	84
Gambar 4. 96 AP STA Mode ESP32-S3	85
Gambar 4. 97 Fungsi handleroot()	86
Gambar 4. 98 Halaman Utama.....	86
Gambar 4. 99 WiFi Setup	87
Gambar 4. 100 Menyimpan konfigurasi	87
Gambar 4. 101 Data Terkirim ke Supabase	88
Gambar 4. 102 Struktur Web	88
Gambar 4. 123 Target	89
Gambar 4. 124 scapy reason 1	90
Gambar 4. 125 wireshark capture deauth reason 1	90
Gambar 4. 126 Data Supabase (1)	90
Gambar 4. 127 Reason Code: Unspecified reason.....	90
Gambar 4. 128 Wireshark capture deauth reason 5	91
Gambar 4. 129 Data Supabase (2)	91
Gambar 4. 130 Reason Code: Disassociated because AP is unable to handle all currently associated STAs.....	91
Gambar 4. 131 Wireshark capture deauth reason 15	92
Gambar 4. 132 Data Supabase (3)	92
Gambar 4. 133 Reason Code: 4-way handshake timeout.	92
Gambar 4. 134 Wireshark capture deauth reason 20	93
Gambar 4. 135 Data Supabase (4)	93
Gambar 4. 136 Reason Code 20: Invalid AKMP (Authentication and Key Management Protocol).....	93
Gambar 4. 137 Wireshark capture deauth reason 22	94
Gambar 4. 138 Data Supabase (5)	94
Gambar 4. 139 Deteksi Reason Code 22: Invalid RSN information element capabilities.	94
Gambar 4. 140 Data Supabase Jarak 50 cm.....	97

Gambar 4. 141 Wireshark capture: uji jarak IDS NodeMCU 50 cm.....	97
Gambar 4. 142 Pengujian Dengan Jarak 50 cm Dari Akses Poin.....	98
Gambar 4. 143 Pengujian Dengan Jarak 50 cm Dari Akses Poin.....	99
Gambar 4. 144 Wireshark capture: uji jarak IDS NodeMCU 180 cm.....	99
Gambar 4. 145 Data Supabase Jarak 180 cm.....	99
Gambar 4. 146 Pengujian Dengan Jarak 500 cm Dari Akses Poin.....	100
Gambar 4. 147 Wireshark capture: uji jarak IDS NodeMCU 500cm.....	100
Gambar 4. 148 Data Supabase Jarak 500cm.....	101
Gambar 4. 149 WPA3 SAE Concepts	103
Gambar 4. 150 Target Akses Poin	103
Gambar 4. 151 set target	104
Gambar 4. 152 open with wireshark	104
Gambar 4. 153 Wireshark EAPOL	104
Gambar 4. 154 uji EAPOL.....	105
Gambar 4. 155 Aireplay-ng ke ESP32 NAT Router.....	106
Gambar 4. 156 Espressif Broadcast Deauth	106
Gambar 4. 157 informasi reason code	106
Gambar 4. 158 Client Join ke jaringan	107
Gambar 4. 159 Informasi Beacon Frame	108
Gambar 4. 160 RSN Information: Cipher.....	108
Gambar 4. 161 RSN Capabilities.....	108
Gambar 4. 162 Pengujian ping CMD	110
Gambar 4. 163 Pengujian Speedtest	110
Gambar 4. 164 Pengujian menggunakan Discord Voice Channel.....	111
Gambar 4. 165 Diagram Grafik Confusion Matrix Data 1 sampai 5.....	115
Gambar 4. 166 Diagram Akurasi dari Data 1 hingga Data 5.....	115
Gambar 4. 167 Diagram Grafik Waktu Respon.....	116

DAFTAR LAMPIRAN

Lampiran 1 Source Code sistem Deteksi Frame Deauthentication NodeMCU ESP8266.....	123
Lampiran 2 Source sdkconfig dan menuconfig ESP-IDF.....	124
Lampiran 3 Dokumentasi Pengujian Serangan ke ESP32 NAT Router	125
Lampiran 4 Dokumentasi Pengujian Jarak Deteksi NodeMCU ESP8266	125
Lampiran 5 Data Supabase berisi Packet, Total Attack dan Timestamp.	126
Lampiran 6 Web Pemantauan Data Real-time dan Historic lewat domain vercel	127

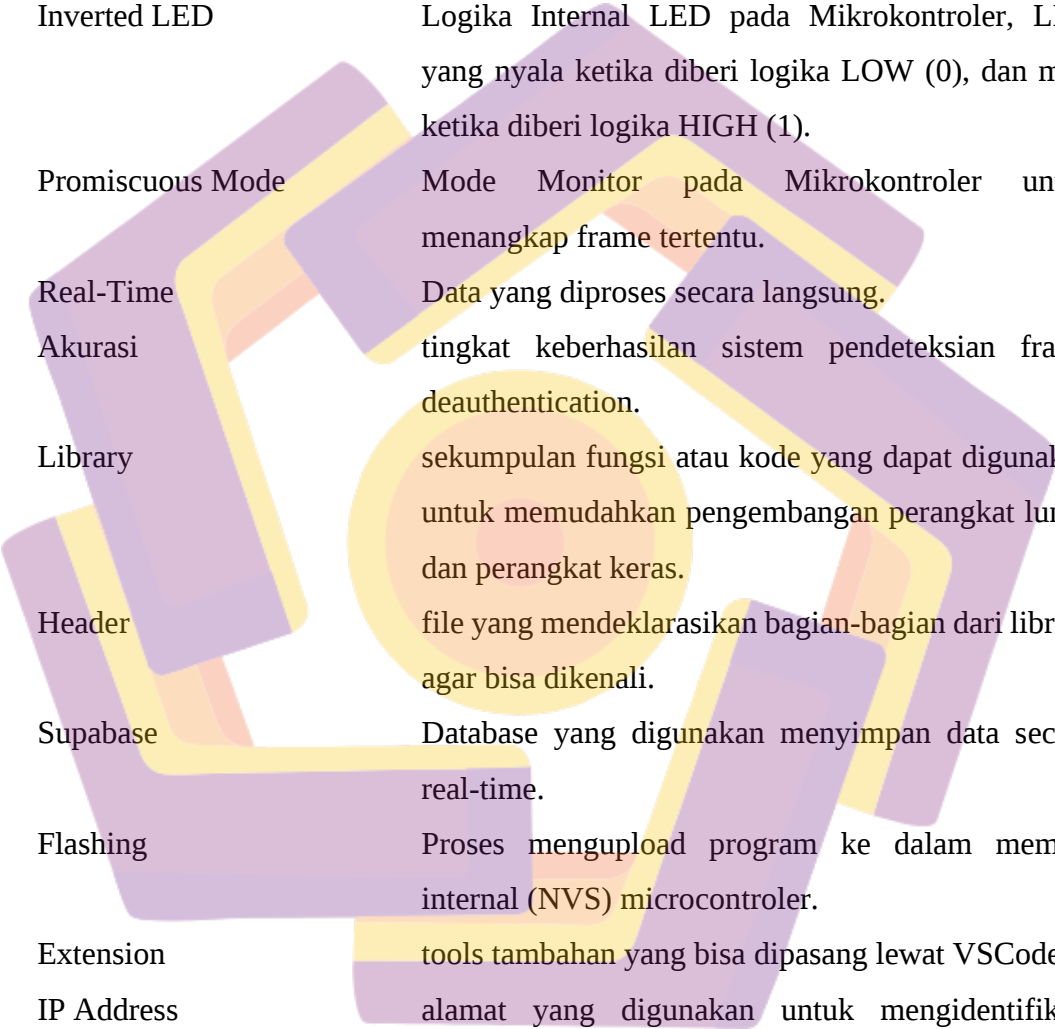


DAFTAR LAMBANG DAN SINGKATAN



IDS	Intrusion Detection System
UART	Universal Asynchronous Receiver/Transmitter
NAT	Network Address Translation
UI	User Interface
RAM	Random Access Memory
SSD	Solid State Drive
PC	Personal Computer
Wi-Fi	Wireless Fidelity
GHz	Gigahertz
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
IoT	Internet of Things
PMF	Protected Management Frame
SAE	Simultaneous Authentication of Equals
AES	Advanced Encryption Standard
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
BSSID	Basic Service Set Identifier
MAC	Media Access Control
RSSI	Received Signal Strength Indicator
EAPOL	Extensible Authentication Protocol over LAN
WPA	Wi-Fi Protected Access
IEEE	Institute of Electrical and Electronics Engineers
RSN	Robust Security Network
NTP	Network Time Protocol
ESP-IDF	Espressif IoT Development Framework
NVS	Non-Volatile Storage

DAFTAR ISTILAH



Frame Deauthentication	Salah satu tipe frame di protokol Wi-Fi (IEEE 802.11), dan sering disalahgunakan untuk serangan jaringan.
Inverted LED	Logika Internal LED pada Mikrokontroler, LED yang nyala ketika diberi logika LOW (0), dan mati ketika diberi logika HIGH (1).
Promiscuous Mode	Mode Monitor pada Mikrokontroler untuk menangkap frame tertentu.
Real-Time Akurasi	Data yang diproses secara langsung, tingkat keberhasilan sistem pendeteksian frame deauthentication.
Library	sekumpulan fungsi atau kode yang dapat digunakan untuk memudahkan pengembangan perangkat lunak dan perangkat keras.
Header	file yang mendeklarasikan bagian-bagian dari library agar bisa dikenali.
Supabase	Database yang digunakan menyimpan data secara real-time.
Flashing	Proses mengupload program ke dalam memori internal (NVS) microcontroller.
Extension	tools tambahan yang bisa dipasang lewat VSCode.
IP Address	alamat yang digunakan untuk mengidentifikasi perangkat di dalam jaringan komputer atau internet.
Autentikasi	proses untuk memastikan identitas suatu perangkat yang ingin mengakses jaringan atau layanan.

INTISARI

Teknologi jaringan nirkabel dan perangkat Internet of Things (IoT) berkembang pesat dan menjadi bagian penting dalam berbagai industri dan aktivitas manusia. Namun, selain penggunaannya yang luas, hal ini juga menimbulkan tantangan keamanan yang signifikan, terutama terhadap serangan deautentikasi dan ancaman lain seperti brute force dan spoofing. Masalah ini juga berasal dari protokol IEEE 802.11 yang mana frame ini (Deauthentication Frame) tidak dienkripsi atau diautentikasi dalam standar 802.11 asli, sehingga mudah dipalsukan. Karena tidak ada enkripsi atau autentikasi, penyerang bisa mengirim frame deauthentication palsu yang seolah-olah berasal dari AP atau STA yang sah. Akibatnya, koneksi bisa diputus secara paksa, menyebabkan gangguan layanan.

Pada penelitian ini menunjukkan bahwa sistem keamanan yang sering diterapkan di jaringan publik, seperti Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK), menunjukkan kelemahan dalam mencegah serangan ini. Di sisi lain, ini juga berdampak pada produk yang dikembangkan dengan basis IoT terutama yang membutuhkan akses internet secara langsung. Pada penelitian ini, memberikan sebuah solusi keamanan dengan menggunakan mikrokontroler ESP32 yang difungsikan sebagai NAT Router yang dilengkapi dengan Protected Management Frame (PMF), menjamin keamanan jaringan nirkabel. Lebih lagi mikrokontroler ini juga mendukung protokol keamanan WPA3. Ditambah sistem Intrusion berbasis NodeMCU ESP8266 sebagai pendeteksi untuk Frame Deauthentication (type 0x00, subtype 0x0C).

Hasil Penelitian ini menunjukkan bahwa ESP32 NAT Router yang difungsikan penulis sebagai Wi-Fi Alternatif, mampu memberikan layanan internet dari Access Point. ESP32 NAT Router juga mampu bertahan dari serangan Deauthentication Frame yang sudah dilengkapi PMF (Proteksi Managemen Frame). Melalui analisis mendalam, penelitian ini bertujuan untuk mengembangkan solusi keamanan inovatif yang lebih efektif mengatasi kerentanan pada jaringan nirkabel dan perangkat IoT serta memberikan referensi untuk memperkuat ketahanan siber perangkat IoT khususnya pada jaringan nirkabel. Walau Bandwidth yang dihasilkan masih jauh dari cukup, untuk kegiatan yang membutuhkan akses internet skala besar seperti zoom meeting, menurut penulis akses internet yang dihasilkan sudah cukup untuk memberikan keamanan dan kelancaran.

Kata kunci: Internet of Things, Wi-Fi Protected Access 2 Pre-Shared Key, Serangan Deautentikasi.

ABSTRACT

Wireless network technology and Internet of Things (IoT) devices are evolving rapidly and are becoming an important part of various industries and human activities. However, in addition to its widespread use, it also poses significant security challenges, especially against deauthentication attacks and other threats such as brute force and spoofing. This problem can occur anywhere and at any time depending on the resilience of the Wi-Fi network in each location. This issue also stems from the IEEE 802.11 protocol where this frame (Deauthentication Frame) is not encrypted or authenticated in the original 802.11 standard, making it easy to counterfeit. Since there is no encryption or authentication, an attacker could send a fake deauthentication frame that appears to be from a legitimate AP or STA. As a result, the connection can be forcibly disconnected, causing service interruptions.

This study shows that security systems that are often implemented in public networks, such as Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK), show weaknesses in preventing these attacks. On the other hand, it also has an impact on products developed on an IoT basis especially those that require direct internet access. In this study, it provides a security solution using the ESP32 microcontroller which functions as a NAT Router equipped with a Protected Management Frame (PMF), ensuring the security of the wireless network. Moreover, this microcontroller also supports the WPA3 security protocol. Plus NodeMCU-based Intrusion systems ESP8266 as detectors for Deauthentication Frame (type 0x00, subtype 0x0C).

The results of this study show that the ESP32 NAT Router, which the author functions as an Alternative Wi-Fi, is able to provide internet service from Access Points. The ESP32 NAT Router is also able to withstand Deauthentication Frame attacks that are equipped with PMF (Frame Management Protection). Through in-depth analysis, this research aims to develop innovative security solutions that are more effective in addressing vulnerabilities in wireless networks and IoT devices and provide a reference to strengthen the cyber resilience of IoT devices, especially in wireless networks. Although the bandwidth generated is still far from enough, for activities that require large-scale internet access such as zoom meetings, according to the author, the resulting internet access is enough to provide security and smoothness.

Keyword: Internet of Things, Wi-Fi Protected Access 2 Pre-Shared Key, Deauthentication Attack.