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 Koprawi, 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	Tanda Tangan
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	

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

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, 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:

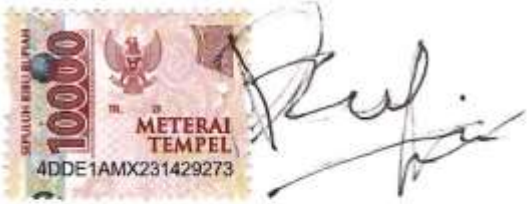
Sistem Deteksi Serangan Deauthentication Frame Berbasis NodeMCU ESP8266 Dan Solusi Wi-Fi Alternatif Berbasis Mikrokontroler ESP32

Dosen Pembimbing : Muhammad Koprawi, 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 Koprawi, 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 Trihadijanto 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

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

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	Data yang diproses secara langsung.
Akurasi	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) microcontroler.
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 (tipe 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 (De-authentication 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.*