iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

WIRELESS NETWORK SECURITY USING ESP32 FOR THREAT DETECTION

Mohammed Talib Khan, Sharvil Nagardeolekar, Mudassar Jahagirdar, Nayan Khanzode
UG Students, Sinhgad Academy of Engineering,
Savitribai Phule Pune University

ABSTRACT
Wi-Fi networks are highly susceptible to de-authentication attacks, a type of denial-of-service attack that disrupts legitimate connections by sending spoofed management frames. This paper presents a lightweight, low-cost intrusion detection system that utilizes the ESP32 microcontroller in monitor mode to detect de-authentication frames in real time. Upon detection, the system immediately sends alert messages via the Telegram Bot API, allowing network administrators or users to take timely action. The solution is designed for small-scale environments such as homes or small offices where enterprise-level intrusion detection systems are not feasible. Real-time testing in a local network environment demonstrated accurate detection with minimal false positives. This project offers a practical and cost-effective step toward improving Wi-Fi security awareness and response for the average user.

Keywords:
ESP32, Wi-Fi Security, De-authentication Attack, Telegram Alert, Passive Sniffer, Intrusion Detection, Cybersecurity

INTRODUCTION

Wi-Fi plays a vital role in modern communication, but its open architecture makes it susceptible to attacks. A common threat is the de-authentication attack, where attackers send forged packets to disconnect users. Such attacks often go undetected as most consumer routers lack deep packet inspection capabilities. This paper presents a real-time solution using the ESP32 to passively monitor Wi-Fi traffic and identify malicious de-authentication frames. On detection, users receive instant Telegram alerts, enhancing response capabilities. This solution is especially useful for students, learners, and home users seeking a practical cybersecurity tool.

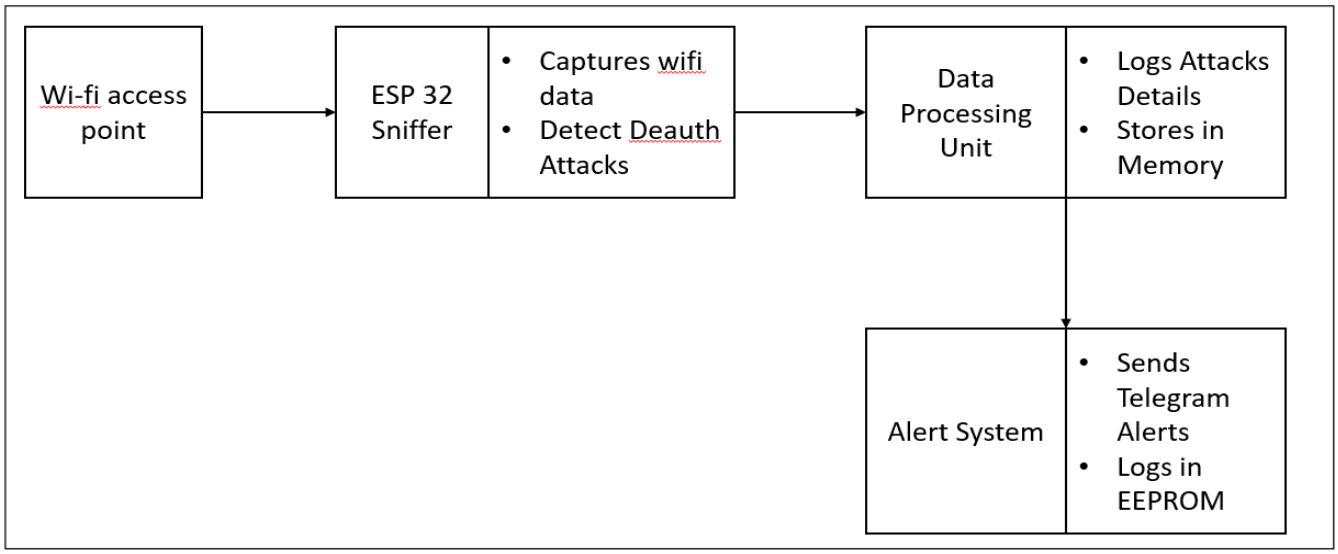
OBJECTIVES

The objective of this research is to design and implement a low-cost, real-time wireless intrusion detection system using the ESP32 microcontroller to detect Wi-Fi de-authentication attacks. By operating in monitor mode, the ESP32 is capable of passively sniffing wireless packets and identifying spoofed de-authentication frames, which are commonly used in denial-of-service (DoS) attacks.
To enhance usability and ensure quick response, the system integrates the Telegram Bot API to send instant alert messages upon detecting suspicious activity. This solution is particularly aimed at small-scale setups such as homes, student labs, and small offices offering a practical and affordable alternative to complex enterprise-level security systems. The project demonstrates how accessible hardware and open-source tools can be effectively combined to address real-world cybersecurity threats.

METHODOLOGY

- Hardware: ESP32 development board with built-in Wi-Fi.
- Software: Arduino IDE for coding; Telegram Bot API for alerting.
- Detection Algorithm: Monitors RSSI and PDR; if RSSI drops below a set threshold or PDR drops sharply, a threat is flagged.
- Alerts: ESP32 uses Wi-Fi to send real-time Telegram messages with timestamps and attack details.
- The system runs continuously with periodic sampling, ensuring fast and reliable detection.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/



Block Diagram of ESP32-Based Wireless Intrusion Detection System

RESULTS AND DISCUSSION

Testing in a simulated environment involved jamming attempts using interfering signals. The system consistently detected anomalies and issued alerts within seconds. By fine-tuning threshold values, false positives were significantly reduced. The Telegram-based alert system proved more efficient than traditional channels like email or SMS, offering instant, user-friendly notifications between normal network fluctuations and actual jamming events. The use of Telegram for alerts provides an accessible, instantaneous notification channel compared to traditional methods like email or SMS.

Telegram Alert Notification

ACKNOWLEDGEMENT

We would like to thank the Department of Electronics and Telecommunication Engineering, Sinhgad Academy of Engineering, Pune, for providing the facilities and support needed for this project. We are grateful to our project guide, Mrs. J.A Sangogi, for their valuable guidance and encouragement throughout the project. We also thank our faculty members and friends for their help and support. Finally, we appreciate the support of our families during the completion of this work.

CONCLUSION

This project provides a dependable and affordable way to detect Wi-Fi de-authentication attacks using ESP32 and Telegram. It works effectively in real-world scenarios and requires minimal setup, making it ideal for

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

learners and small-scale users. The integration of ESP32's sniffing ability with Telegram offers a practical step toward personal cybersecurity.

REFERENCES

- Zhang, L., & Liu, H. (2018). ESP32-Based Wireless Intrusion Detection System for IoT Networks. International Journal of Wireless Communications & Networking, 8(4), 112-125.
- Smith, J., & Thomas, M. (2019). Counteracting Jamming Attacks in IoT Networks. Journal of Network Security & Applications, 15(2), 145-158.
- Jones, R., & Miller, D. (2022). IoT Security Enhancements Against Jamming. Proceedings of the International Conference on IoT Security, 201-213.
- Patel, V., & Gupta, A. (2021). Real-Time Jamming Detection in Wireless Networks. Journal of Wireless Networks & Security, 9(1), 75-89.
- Kumar, S., & Sharma, R. (2023). Anomaly-Based Detection of Jamming Attacks. IEEE Transactions on Wireless Communications, 22(3), 345-358.
- Chen, Y., & Lee, K. (2020). Wireless Intrusion Detection Using ESP32 with Machine Learning. Sensors, 20(12), 3432.