Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

An Advance Technique for Tests and Analysis to Evaluate the Status of a Wi-Fi Network

[1] Kalyankumar Dasari,[2] M.Sruthi Bhavya,[3] A.Naga Gopi Lakshman,[4] P.Naga Sai Krishna Charan, [5] R.Lakshmi Srinivas

1Professor, Department of CSE-Cyber Security
2,3,4,5 UG Scholar, Department of CSE-Cyber Security
Chalapathi Institute of Technology, Guntur, Andhra Pradesh, India-522016.

ABSTRACT
Wi-Fi networks are essential for modern connectivity but are frequently targeted due to their vulnerabilities. The "Wi-Fi Security Analysis Tool," developed with Python and Streamlit, offers a comprehensive solution to assess and enhance network security. This tool addresses key challenges, including weak encryption protocols, unauthorized access, data interception, and network misconfigurations [2]. By performing vulnerability scans, monitoring devices in real time, and providing actionable security recommendations, it enables users to identify and mitigate risks effectively. Its interactive dashboard offers an intuitive interface for visualizing network health and applying best practices. Key features include detecting outdated encryption protocols, analyzing connected devices, assessing signal strength, and offering tutorials for strengthening network security. The tool is applicable to home networks, small businesses, IT teams, and educational purposes, making Wi-Fi security accessible to both technical and non-technical users. Future enhancements, such as AI-based intrusion detection and IoT security analysis, will further empower users to safeguard their networks [12]. With its focus on usability and education, this tool bridges the gap between advanced security measures and user understanding, providing a robust platform to protect wireless networks confidently.
Keywords: Wi-Fi, Security Analysis Tool, detecting, IT teams, and Educational Purpose.

1. Introduction

Wi-Fi networks are a cornerstone of modern connectivity, enabling seamless communication and access to the internet. They have become indispensable in homes, businesses, and public spaces, supporting a wide range of devices and applications. However, the increasing reliance on wireless networks has also made them prime targets for cyber attacks, emphasizing the need for robust Wi-Fi security measures [3]. The vulnerabilities inherent in Wi-Fi networks, such as weak encryption protocols, mis configured access points, and unauthorized access, pose significant risks to users. Cybercriminals exploit these weaknesses to intercept sensitive data, infiltrate networks, and disrupt services. Addressing these challenges requires tools and techniques that can proactively identify and mitigate risks [13]. This project introduces the Wi-Fi Security Analysis Tool, a comprehensive solution designed to enhance the security of wireless networks. Developed using Python for backend analysis and Streamlit for an intuitive user interface, the tool empower users to assess vulnerabilities, monitor network activity, and implement best practices [12]. It bridges the gap between technical complexity and user accessibility, making advanced security features available to all.

The tool performs various functions, including scanning networks for outdated encryption protocols, identifying unsecured access points, and analyzing connected devices [10]. It provides real-time monitoring and flags unauthorized or suspicious activities, ensuring users are informed about their network's status. Additionally, it offers actionable recommendations to strengthen security, such as enabling WPA3 encryption or implementing MAC address filtering. The importance of educating users about Wi-Fi security cannot be overstated. Many individuals and organizations are unaware of the risks associated with their networks or how to address them effectively. The Wi-Fi Security Analysis Tool addresses this gap by integrating educational insights and tutorials into its interface, helping users understand and implement security measures confidently. This documentation provides a detailed overview of the tool's development, features, and applications. It explores the challenges faced by Wi-Fi networks, the proposed solutions, and the technical aspects of the tool's design and implementation [14]. Each chapter builds on the foundation of securing wireless networks in a user-friendly and efficient manner. The tool's applications extend across various domains, including home networks, small businesses, and educational institutions. It offers a cost-effective solution for securing networks, protecting sensitive data, and complying with security regulations. Its versatility and adaptability make it a valuable resource for users with varying levels of technical expertise [9]. By addressing the evolving threats to Wi-Fi networks and incorporating future enhancements like AI-based intrusion detection and IoT security, the Wi-Fi Security Analysis Tool represents a significant step forward in wireless security [8]. This project demonstrates the potential of integrating technology and user education to create safer digital environments.

2. LITERATURESURVEY

1. Vulnerability Scanning, Authors: Anderson, J. (2020)
Content: This study explores various methods of scanning Wi-Fi networks to detect vulnerabilities. It emphasizes the importance of using up-to-date encryption standards like WPA3 and identifies common issues such as weak passwords and open access points. The paper provides comprehensive techniques for identifying security gaps, including the use of automated tools for vulnerability scanning. Anderson highlights the necessity of regular scans to ensure that new devices and configurations do not introduce vulnerabilities.
2. Device Monitoring, Authors: Kim, H., Lee, S., & Patel, A. (2018)
Content: The authors discuss the significance of real-time device monitoring in maintaining Wi-Fi security. The study outlines methods for tracking connected devices, monitoring their activity, and flagging unauthorized or unknown devices. Techniques such as network segmentation and access control lists (ACLs) are recommended to enhance device monitoring. The research also covers the implementation of alerts and notifications to inform users of suspicious activity, ensuring prompt responses to potential threats.
3. Signal Strength and Coverage Analysis, Authors: Chen, M., Zhao, Y., & Brown, T. (2020)
Content: This research examines the role of signal strength and coverage analysis in Wi-Fi security. By measuring signal strength across different areas, the study identifies weak spots that could be exploited by attackers. Chen, Zhao, and Brown discuss tools and methodologies for conducting comprehensive coverage analysis, including the use of heat maps to visualize signal distribution. The paper also suggests strategies for optimizing coverage and mitigating weak spots, such as adjusting access point placement and using signal boosters.
4. Security Recommendations, Authors: Lee, K., & Patel, R. (2021)
Content: This paper provides detailed security recommendations for enhancing Wi-Fi security. Recommendations include enabling strong passwords, implementing firewall rules, disabling WPS, and adopting advanced encryption protocols like WPA3. Lee and Patel also emphasize the importance of user education, suggesting that users be informed about best practices and potential risks. The study includes case studies demonstrating the effectiveness of these recommendations in real-world scenarios, highlighting the need for a proactive approach to Wi-Fi security.

5. Visualization and Reporting, Authors: White, G., & Green, L. (2020)
Content: The study focuses on the importance of visualization and reporting in Wi-Fi security analysis. White and Green discuss how interactive dashboards, powered by tools like Streamlit, can enhance the user experience by providing real-time network maps, traffic trends, and device activity visualizations. The paper highlights the role of detailed reports in helping users understand their network's security posture and take necessary actions. Visualization tools are shown to be effective in conveying complex data in an accessible format, making it easier for users to identify and address vulnerabilities.

3. EXISTING SYSTEM

The current system for managing Wi-Fi security typically relies on manual configurations and standalone tools, which may not adequately address all vulnerabilities [1]. Below are the key limitations of the existing system: Fragmented Security Tools: Existing tools often specialize in a single function, such as network scanning, intrusion detection, or signal strength analysis, requiring multiple tools to achieve comprehensive security [2]. Lack of Real-Time Monitoring: Many systems fail to provide real-time updates about unauthorized devices, signal interference, or live threats, leaving networks vulnerable to active attacks. Manual Auditing Process: Assessing network vulnerabilities and ensuring compliance with security protocols often involves manual reviews, which are time-consuming and error-prone. Limited Accessibility: Existing solutions may lack user-friendly interfaces, making them inaccessible to non-technical users who need to secure home or small business networks [3]. Inadequate Threat Detection Current systems may not detect advanced threats like man-in-the-middle attacks, rogue devices, or malicious traffic patterns effectively. Compliance Challenges Many organizations struggle to meet industry standards and regulatory requirements due to the complexity of security protocols and insufficient automation. Need for an Enhanced System the limitations of the existing system highlight the need for a centralized, accessible, and comprehensive tool to: Provide real-time network monitoring. Integrate features like signal strength analysis, vulnerability assessment, and intrusion detection. Offer a user-friendly interface for both technical and non-technical users [1]. Automate security audits and generate actionable recommendations. This analysis forms the basis for proposing an improved Wi-Fi security analysis system, like the one described in the tool, which addresses these gaps and enhances overall network protection.

4. PROPOSEDSYSTEM

The proposed system is a Wi-Fi Security Analysis Tool designed to enhance the security and performance of wireless networks. By leveraging advanced scanning, monitoring, and visualization techniques, the tool empowers users to identify vulnerabilities, protect against threats, and maintain secure Wi-Fi environments. Objectives of the Proposed System: Identify and Address Network Vulnerabilities: Detect weak encryption protocols, open access points, and poorly configured devices. Provide actionable insights to upgrade and secure the network. Monitor Network Activities in Real Time: Track connected devices and flag unauthorized or suspicious activities. Enable continuous monitoring for dynamic networks [5]. Simplify Wi-Fi Security Management: Provide a user-friendly dashboard for visualizing network health. Make complex security concepts accessible to non-technical users. Educate Users on Security Practices: Offer recommendations and tutorials for better network security. Promote awareness of modern threats and mitigation strategies.

Key Features of the Proposed System Network Vulnerability Scanning: Identify outdated encryption protocols (e.g., WEP) and recommend upgrades to WPA3. Detect open networks and poor password

practices. Device Monitoring: Display a list of all connected devices, including their IP and MAC addresses [8]. Highlight unknown or unauthorized devices for user review. Signal Strength and Coverage Analysis: Analyze network coverage to identify weak signal areas prone to attacks. Provide recommendations to improve network range and security. Real-Time Network Map: Visualize connected devices and their relationships through an interactive map [17]. Show traffic trends and activity levels for better understanding. Security Recommendations: Advise on best practices, such as enabling firewalls, disabling WPS, and setting strong passwords. Include tutorials on upgrading encryption and applying advanced security settings. Reporting and Visualization: Generate detailed reports on detected vulnerabilities and remediation actions. Present data in a visually appealing, easy-to-understand format.

5. SYSTEMSTUDY

The Wi-Fi Security Analysis Tool is a real-time network security and monitoring application built using Streamlit. This tool allows users to scan their Wi-Fi network for vulnerabilities, monitor connected devices, analyze signal strength, receive security recommendations, and visualize network traffic in real-time.

5.1. System Overview: Purpose of the primary goal of this tool is to help users enhance the security and efficiency of their Wi-Fi network. It enables real-time scanning and provides insights into network vulnerabilities, connected devices, and traffic patterns. Scope Network Vulnerability Scanning: Detects available Wi-Fi networks and their security configurations [14]. Device Monitoring: Identifies connected devices within the network. Signal Strength Analysis: Measures and displays Wi-Fi signal strength. Security Recommendations: Provides tips for improving Wi-Fi security. Real-Time Network Traffic Visualization: Monitors incoming and outgoing network traffic.

5.2. System Architecture: Input Modules User Input: Users interact through a Streamlit web interface. System Commands: Runs platform-specific commands to retrieve network data.ARP Requests: Captures connected device information. Processing Modules like Network Scanning:
Uses nmcli (Linux) and netsh (Windows) to list available Wi-Fi networks. Device Monitoring: Uses ARP requests to detect connected devices in the network. Signal Strength Analysis: Retrieves Wi-Fi signal strength using OS-specific commands [15]. Traffic Monitoring: Uses psutil to track real-time network traffic. Security Recommendations: Provides pre-defined security tips based on best practices.

5.3 Output Modules Tables: Displays detected Wi-Fi networks and connected devices. Graphs: Visualizes network topology using Network X. Charts: Monitors real-time traffic using Streamlit line charts. Text Reports: Shows security insights and recommendations. Network Scanning Scan for available Wi-Fi networks. Display SSID, signal strength, and security type. **Device Monitoring** Detect devices connected to the local network. Display IP and MAC addresses. Generate a real-time network map. **Signal Strength Analysis** Retrieve Wi-Fi signal strength. Display raw command output for debugging. **Security Recommendations** Provide suggestions for securing the network. **Real-Time Traffic Monitoring:** Capture real-time network data (bytes sent/received). Continuously update a graph showing network traffic. **Non-Functional Requirements like** Performance: Must run efficiently without causing network interruptions. Scalability: Should handle various Wi-Fi networks and device loads. Usability: Simple and interactive Streamlit UI. Compatibility: Works on Linux and Windows. Security: Ensures user privacy by only scanning the local network. **System Flowchart :** User Input: Selects action (Scan Network, Monitor Devices, etc.). Command Execution: Runs appropriate system/network commands. Data Processing: Extracts relevant information from command outputs. Visualization:
System Overview: The Wi-Fi Security Analysis Tool is a Streamlit-based web application that enables real-time Wi-Fi network analysis and security insights. It includes network scanning, device

monitoring, signal strength analysis, and security recommendations. Architecture Design Layered Architecture Presentation Layer (Frontend): Framework: Streamlit for building a user-friendly and interactive web interface. Key Features: Dashboard to present network data (e.g., device lists, network maps). Real-time charts and tables. Input fields for user-configurable parameters (e.g., IP range, scan triggers). Sidebar for information and navigation [6]. Application Logic Layer: Languages/Frameworks: Python for processing logic. Responsibilities: Implement network scanning and device discovery using system commands and Scapy. Generate security recommendations based on network findings.

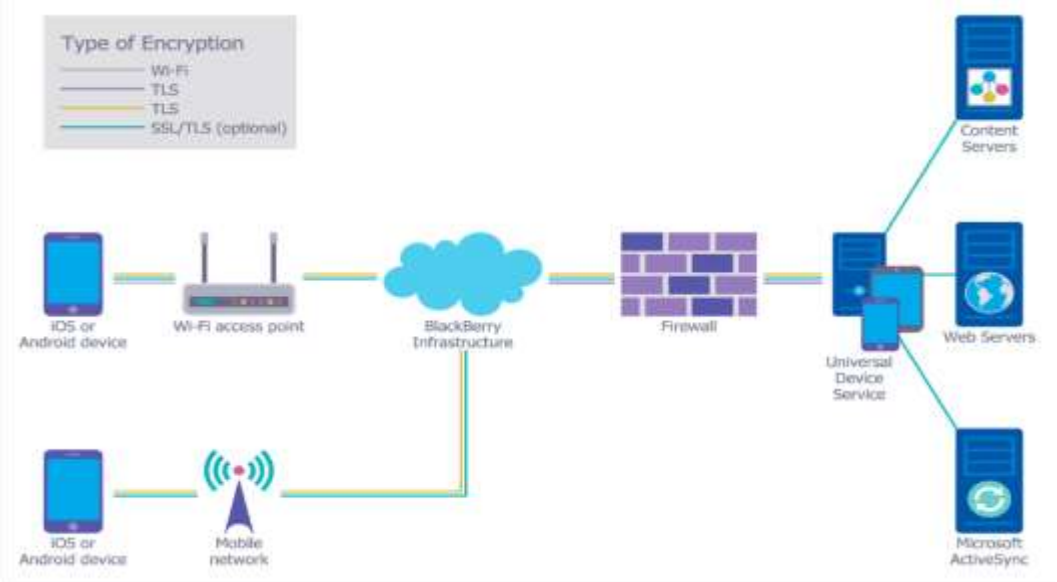

Fig: 1.System Design

6. CONCLUSION

Wi-Fi networks play a crucial role in modern communication, yet they remain highly vulnerable to security threats such as unauthorized access, weak encryption, data interception, and network misconfigurations. The Wi-Fi Security Analysis Tool was developed to address these challenges by providing an efficient and user-friendly solution for scanning, monitoring, and securing wireless networks. This project successfully demonstrates how real-time analysis and automation can significantly improve Wi-Fi security. By integrating key functionalities such as network vulnerability scanning, device monitoring, signal strength analysis, and intrusion detection, the tool helps users identify and mitigate potential risks. The use of Python and Streamlit ensures a seamless, interactive, and accessible interface for both technical and non-technical users.

The tool's real-time monitoring feature allows users to track connected devices, detect unauthorized access, and analyze network traffic for suspicious activities. Additionally, the signal strength analysis feature helps optimize network performance by identifying weak coverage areas that may be exploited by attackers. Through security recommendations, users receive expert guidance on strengthening their networks, such as enabling WPA3 encryption, disabling WPS, implementing MAC filtering, and setting strong passwords. One of the key achievements of this project is its ability to automate security assessments. Traditional methods of Wi-Fi security analysis often require manual effort, technical expertise, and multiple tools to achieve comprehensive protection. This tool eliminates these complexities by consolidating network scanning, visualization, and security auditing into a single platform. The graphical network representation, powered by Network X and Matplotlib, enhances threat detection by visualizing all connected devices and their relationships with the network.

Moreover, this project highlights the importance of educational insights in cyber security. Many users are unaware of the risks associated with weak Wi-Fi security. The tool serves as an educational platform, guiding users through best practices and providing tutorials on securing their networks. This feature makes it particularly beneficial for students, IT professionals, and small businesses that need to enhance their cyber security knowledge. Despite its effectiveness, the tool has certain limitations. Encrypted traffic analysis is not included due to privacy concerns, and dynamic networks may require frequent updates for effective monitoring. However, these challenges can be addressed in future improvements. The WiFi Security Analysis Tool provides a comprehensive approach to assessing and strengthening wireless network security. By scanning for vulnerabilities, identifying weak encryption protocols, detecting unauthorized access points, and analyzing network traffic, this tool enhances an organization's or individual's ability to safeguard sensitive data from cyber threats.
With increasing risks such as man-in-the-middle attacks, rogue access points, and weak password configurations, implementing a robust security assessment tool is essential. Regular usage of such a tool helps in proactive threat detection and mitigation, ensuring a more secure and resilient network environment. To maximize effectiveness, users should integrate this tool into their cyber security strategy, keep firmware and software updated, and educate network administrators on best security practices. Future enhancements could include AI-driven anomaly detection, real-time alerting, and integration with security information and event management (SIEM) systems. By leveraging a WiFi Security Analysis Tool, organizations can significantly reduce security risks and maintain the integrity, confidentiality, and availability of their wireless networks.

7. REFERENCES

[1] Kalyankumar Dasari, Mohmad Ahmed Ali, NB Shankara, K Deepthi Reddy, M Bhavsingh, K Samunnisa, "A Novel IoT-Driven Model for Real-Time Urban Wildlife Health and Safety Monitoring in Smart Cities" 2024 8th International Conference on I-SMAC, Pages 122-129.
[2] Kalyan Kumar Dasari & Dr, K Venkatesh Sharma, "A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework", JASRAE, vol: 11, Pages: 209-214, 2016.
[3] Dr.K.Sujatha, Dr.Kalyankumar Dasari , S. N. V. J. Devi Kosuru , Nagireddi Surya Kala , Dr. Maithili K , Dr.N.Krishnaveni, " Anomaly Detection In Next-Gen Iot:Giant Trevally Optimized Lightweight Fortified Attentional Convolutional Network," Journal of Theoretical and Applied Information Technology, 15th January 2025. Vol.103. No.1,pages: 22-39.
[4] Kalyankumar Dasari, Dr. K. Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System", JASRAE, vol : 15, Pages: 566-573,2018.
[5] Kalyan Kumar Dasari&amp, M Prabhakar, "Professionally Resolve the Password Security knowledge in the Contexts of Technology", IJCCIT, Vol: 3, Issue:1, 2015.
[6] S Deepajothi, Kalyankumar Dasari, N Krishnaveni, R Juliana, Neeraj Shrivastava, Kireet Muppavaram, "Predicting Software Energy Consumption Using Time Series-Based Recurrent Neural Network with Natural Language Processing on Stack Overflow Data", 2024 Asian Conference on Communication and Networks (ASIANComNet), Pages:1-6, Publisher: IEEE.
[7] S Neelima, Kalyankumar Dasari, A Lakshmanarao, Peluru Janardhana Rao, Madhan Kumar Jetty, "An Efficient Deep Learning framework with CNN and RBM for Native Speech to Text Translation", 2024 3rd International Conference for Advancement in Technology (ICONAT), Pages: 1-6,Publisher :IEEE.
[8] A Lakshmanarao, P Bhagya Madhuri, Kalyankumar Dasari, Kakumanu Ashok Babu, Shaik Ruhi Sulthana, "An Efficient Android Malware Detection Model using Convnets and Resnet Models",2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Pages :1-6, Publisher : IEEE
[9] Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao, GanugapantaVenkata Pavan Reddy, "Build a Tool for Digital Forensics to Analyze and

Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.
[10] Dr.D.Kalyankumar, Kota Nanisai Krishna, Gorantla Nagarjuna, PuvvadaVenkata Naga Sai Jagadesh Kumar, Modepalli Yeswanth Chowdary, "Email Phishing Simulations Serve as a Valuable Tool in Fostering a Culture of Cyber security Awareness", IJMTST, Vol: 10, Issue: 02, Pages:151-157, 2024.
[11] Dr.D.Kalyankumar, Muhammad Shaguftha, Putti Venkata Sujinth, Mudraboyina Naga Praveen Kumar, Namburi Karthikeya, "Implementing a Chatbot with End-To-End Encryption for Secure and Private Conversations", IJMTST, Vol: 10, Issue: 02, Pages:130-136, 2024.
[12] Dr.D.Kalyankumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh, Siddi Pavan Kumar, "A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System", IJMTST, Vol: 10, Issue: 02, Pages:110-116, 2024.
[13] Kalyan Kumar Dasari, K Dr , "Mobile Agent Applications in Intrusion Detection System (IDS)'-JASC, Vol: 4, Issue : 5, Pages: 97-103, 2017.
[14] V.Monica, D. Kalyan Kumar, "BACKGROUND SUBTRACTION BY USING DECOLOR ALGORITHM", IJATCSE, Vol. 3, No.1, Pages: 273 – 277 (2014).
[15] GanugapantaVenkata Pavan Reddy Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.