AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

WIRELESS NETWORK SECURITY ASSESSMENT AND WIFI SECURITY ANALYSIS

[1]M Keeravani, [2]B Vineeth Kumar, [3]K Manoj, [4]B Naveen
[1]Assistant Professor, [234]Students
Department of Computer Science and Engineering,
Siddhartha Institute of Technology and Sciences, Narapally, Korremula Road,
Ghatkesar, Medchal-Malkajgiri, Hyderabad, Telangana - 500088. INDIA
keeravani@siddhartha.org.in, 23TQ1A6208@siddhartha.co.in,
24TQ5A6202@siddhartha.co.in, 23TQ1A6221@siddhartha.co.in

Abstract

Wireless networks have become an essential part of modern communication infrastructure, providing convenient connectivity for homes, organizations, educational institutions, healthcare facilities, and businesses. The widespread use of Wi-Fi also increases the importance of protecting wireless networks against unauthorized access, weak configurations, insecure authentication, and other security risks. A systematic wireless security assessment can help administrators identify configuration weaknesses and improve the overall security posture of their networks.

The proposed Wireless Network Security Assessment and WiFi Security Analysis system is designed to provide a centralized platform for evaluating the security configuration and risk characteristics of authorized wireless networks. The system can collect permitted information about wireless network configurations, authentication methods, encryption mechanisms, signal characteristics, and related security parameters. The collected information is analyzed using predefined security policies and assessment criteria.

The platform can identify potential security concerns such as weak security configurations, outdated encryption settings, insecure authentication practices, unauthorized or unknown wireless networks, and configuration inconsistencies. Findings can be classified according to severity and prioritized according to their potential security impact. The system focuses on defensive assessment and does not require harmful exploitation of wireless networks.

A centralized dashboard can display discovered wireless networks, security standards, encryption types, risk levels, assessment status, and historical trends. The system can also maintain assessment records and generate structured reports containing identified weaknesses, affected configurations, risk classifications, and recommended defensive measures.

The primary objective of the proposed system is to improve wireless network visibility, security assessment, and risk management. By combining wireless information collection, configuration analysis, risk assessment, visualization, and reporting into a unified platform, the system can help administrators identify security weaknesses and apply appropriate improvements.

I. Introduction

Wireless networks have transformed the way users and organizations access digital services and communicate with network resources. Wi-Fi provides flexibility and mobility by allowing devices to connect without physical network cables. Organizations commonly use wireless networks for employee access, guest connectivity, IoT devices, and business applications. Because wireless communication uses radio signals, appropriate security controls are necessary to prevent unauthorized access and protect transmitted information.

Wireless network security involves protecting wireless infrastructure, access points, connected devices, authentication mechanisms, and transmitted data. Modern Wi-Fi security standards provide mechanisms for authentication and encryption, but incorrect configuration can reduce their effectiveness. Weak passwords, outdated security protocols, inappropriate access-point settings, and unmanaged wireless devices can increase the risk of unauthorized access.

Traditional wireless security assessments may involve examining access-point configurations, encryption settings, authentication mechanisms, network identifiers, signal characteristics, and connected-device information. Network administrators may use different utilities and monitoring tools to collect this information. However, manually organizing results from multiple tools can make it difficult to obtain a complete picture of wireless security.

The proposed Wireless Network Security Assessment and WiFi Security Analysis system provides a centralized environment for collecting and analyzing authorized wireless network information. The platform can organize wireless networks according to security standards, encryption mechanisms, authentication methods, and risk levels. A dashboard can provide administrators with a visual representation of the current wireless security posture.

The main objective of the system is to help network administrators identify configuration weaknesses and prioritize security improvements. By combining assessment, analysis, risk classification, visualization, historical tracking, and reporting, the platform can simplify wireless security management. All assessments should be performed only on wireless networks for which the user has explicit authorization.

II. Literature Survey

Wireless network security has been extensively studied because Wi-Fi has become an important component of modern network infrastructure. Research has examined various security mechanisms for protecting wireless communication, including authentication, encryption, access control, and secure network configuration. These studies emphasize that wireless security requires both strong technical controls and appropriate administrative practices.

Wireless security standards have evolved over time in response to emerging security requirements. Earlier wireless security mechanisms provided basic protection but were affected by design and implementation weaknesses. Modern Wi-Fi security mechanisms provide stronger authentication and encryption capabilities. However,

using an advanced security standard alone does not guarantee complete protection if network configurations, credentials, or access-control policies are weak.

Wireless network assessment research commonly focuses on identifying available access points, examining their security configurations, and evaluating associated network characteristics. Security professionals can use authorized assessment tools to collect information about wireless networks and identify configuration differences. Such assessments can help administrators discover networks that are improperly configured or operating outside organizational policies.

Authentication and encryption are important areas of wireless security analysis. Strong authentication mechanisms help ensure that only authorized users and devices can connect to protected networks, while encryption helps protect wireless communications from unauthorized observation. Security assessments therefore commonly evaluate the selected security protocol, authentication configuration, credential policies, and other related settings.

Wireless intrusion detection and monitoring systems provide another important area of research. These systems can monitor wireless environments for suspicious activity, unauthorized access points, unusual behavior, and policy violations. Centralized monitoring can improve an administrator's ability to identify changes in the wireless environment and investigate potentially unauthorized devices or configurations.

Existing wireless security tools demonstrate the value of network discovery, configuration analysis, monitoring, and reporting. However, organizations may need to use multiple tools to obtain complete wireless security information, while the resulting data may require manual interpretation. The proposed system builds upon these concepts by integrating authorized wireless discovery, security-configuration analysis, risk assessment, visualization, historical tracking, and reporting into a centralized defensive platform.

III. System Analysis

System analysis for the proposed wireless security platform focuses on identifying the requirements for safe and effective Wi-Fi assessment. The system should provide authenticated access to authorized network administrators and security analysts. It should allow users to define the wireless environment and assessment scope before beginning an evaluation. The collection module should gather permitted information about wireless networks, access points, security standards, and authentication configurations. The system should normalize collected information so that different wireless environments can be compared consistently. A security-analysis engine should evaluate configurations against predefined organizational security policies. Potential weaknesses should be classified according to severity and security relevance. A risk-assessment module should prioritize findings based on potential impact and exposure. The database should maintain wireless-network information, assessment results, findings, and historical records. A dashboard should display wireless security statistics, network classifications, and risk distributions. The system should provide recommendations to help administrators improve insecure configurations.

Existing System

Traditional wireless security assessment often depends on separate wireless scanning utilities, access-point administration interfaces, monitoring systems, and manual configuration reviews. Administrators may collect information about available wireless networks and then manually examine their security settings. Different tools can produce different formats and levels of detail, making correlation difficult. Wireless security information may also be distributed between access-point management systems and separate monitoring tools. Risk classification is frequently performed manually according to organizational policies. Historical comparisons can be difficult when assessment results are stored as separate documents or spreadsheets. Administrators may also have limited centralized visualization of wireless security conditions. Identifying unauthorized or unexpected wireless infrastructure can require additional monitoring activities. Report preparation can consume considerable time when information is collected from multiple sources. Repeated assessments may require the same manual analysis tasks. These limitations can reduce the efficiency and consistency of wireless security management.

Disadvantages of Existing System

- Requires multiple tools for wireless security assessment.
- Wireless information may be distributed across different systems.
- Manual configuration analysis can be time-consuming.
- Different tools may produce inconsistent output formats.
- Limited centralized risk assessment.
- Difficult to compare security configurations over time.
- Unauthorized or unexpected wireless infrastructure may be difficult to track.
- Security-policy compliance may require manual verification.
- Repeated assessments can increase administrative workload.

Proposed System

The proposed Wireless Network Security Assessment and WiFi Security Analysis platform provides a centralized environment for evaluating authorized wireless networks. The system allows authenticated administrators to define the wireless assessment scope and configure appropriate assessment parameters. The collection module gathers permitted information about wireless networks, access points, security standards, authentication mechanisms, and other relevant configuration indicators. The processing module validates and normalizes the collected information. A security-analysis engine compares wireless configurations against predefined security policies and assessment criteria. Potential security weaknesses are categorized according to their type and severity. The risk-assessment component evaluates the potential impact and prioritizes findings requiring administrative attention. The database stores wireless-network information, assessment results, security findings, and historical records. A dashboard presents network statistics, security classifications, encryption information, and risk distributions. Administrators can review individual findings and access recommended defensive improvements. Historical results can be compared to determine whether wireless security posture has improved. The reporting module generates structured assessment reports for network administrators and security teams. Overall, the proposed platform provides a systematic workflow for wireless discovery, security analysis, risk assessment, monitoring, and reporting.

Advantages of Proposed System

- Provides centralized wireless security assessment.
- Improves visibility into authorized Wi-Fi environments.
- Organizes wireless security information in a structured format.
- Supports security-configuration analysis.
- Provides risk-based prioritization of findings.
- Helps identify insecure or outdated configurations.
- Provides centralized dashboards and visual summaries.
- Reduces repetitive manual analysis.
- Helps administrators prioritize defensive improvements.

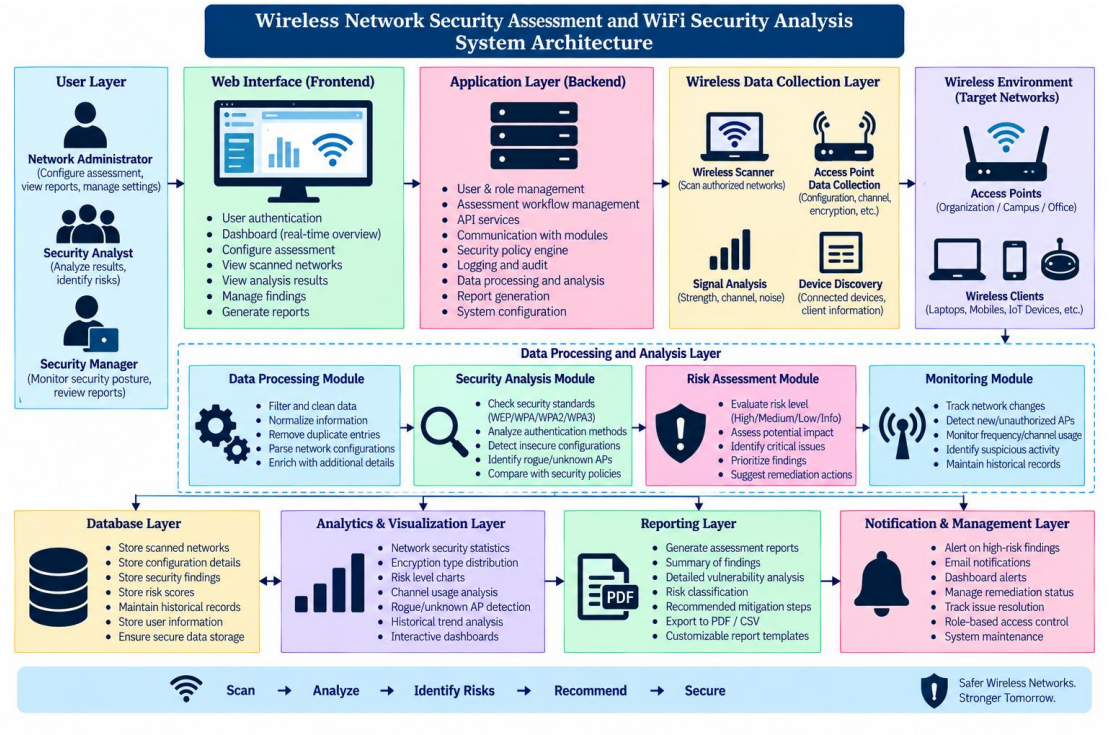
IV. Methodology

The methodology begins by authenticating the authorized network administrator or security analyst. The user defines the approved wireless environment and selects the appropriate assessment configuration. The system collects permitted information about wireless networks and associated access points. Relevant security parameters such as authentication mechanisms, encryption standards, and configuration indicators are extracted. The collected information is validated and normalized before analysis. The security-analysis engine compares the observed configuration against predefined security policies and assessment criteria. Potential security weaknesses are identified and categorized according to their characteristics. The risk engine evaluates severity, potential impact, and exposure to determine assessment priority. The results are stored securely in the centralized database for future reference. The dashboard presents wireless-network statistics, security classifications, risk levels, and historical trends. Administrators can review findings and apply recommended defensive configuration improvements. Finally, the reporting module generates a structured wireless security assessment report for authorized stakeholders.

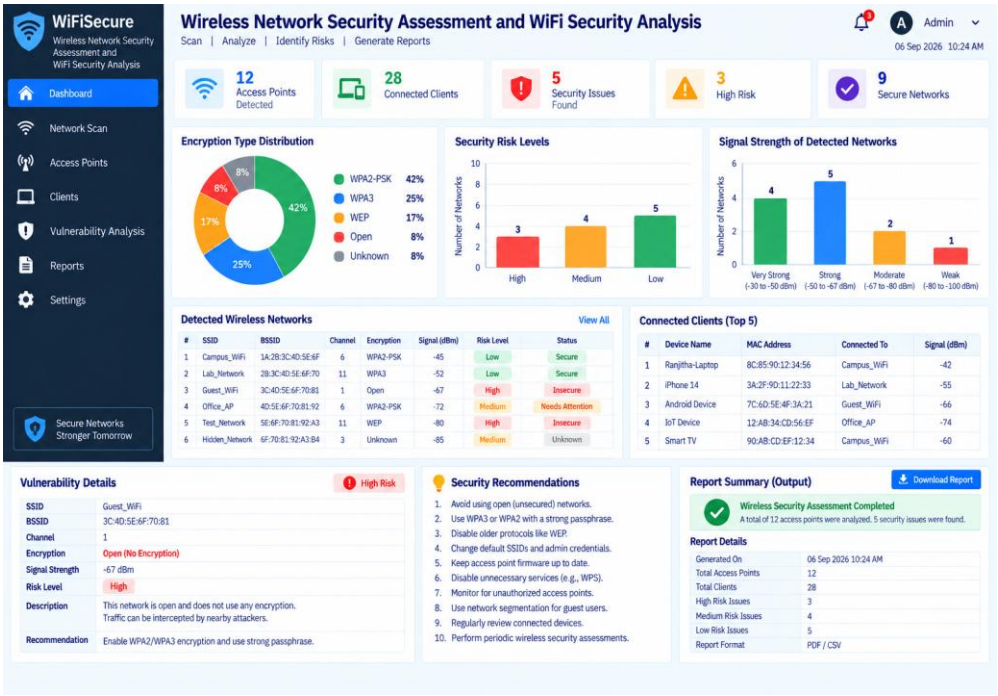
System Architecture

The system architecture consists of several interconnected layers designed to provide a centralized wireless security assessment platform. The User Layer contains authorized network administrators, security analysts, and security managers who interact with the system according to their assigned roles. The Web Interface Layer provides authentication, wireless-environment management, assessment configuration, dashboards, finding management, and report access. The Application Layer manages users, roles, assessment workflows, configuration, validation, logging, and communication between system components. The Wireless Data Collection Layer gathers permitted information about wireless networks, access points, security standards, authentication mechanisms, and configuration indicators. The Data Processing Layer validates, filters, normalizes, and organizes collected wireless information. The Security Analysis Layer evaluates wireless configurations against predefined security policies and identifies potential weaknesses. The Risk Assessment Layer evaluates severity, potential impact, and exposure and assigns appropriate risk priorities. The Database Layer stores wireless-network information, assessment results, findings, risk scores, configuration records, and historical data. The Analytics and Visualization Layer presents wireless security statistics, encryption distributions, security classifications, risk trends, and assessment results. The Reporting Layer

generates structured wireless security assessment reports containing findings, risk classifications, and recommended defensive actions. The Monitoring Layer can support authorized tracking of changes in the wireless environment and configuration status. Access control, logging, secure data handling, and appropriate retention policies protect the assessment platform. The overall architecture provides a controlled flow from authorized assessment through wireless information collection, processing, security analysis, risk assessment, visualization, monitoring, and reporting.



V. Result and Output



VI. Conclusion

The Wireless Network Security Assessment and WiFi Security Analysis system provides a structured approach for evaluating the security posture of authorized wireless networks. By collecting and analyzing information about access points, connected devices, authentication mechanisms, encryption standards, signal characteristics, and security configurations, the system helps administrators identify potential weaknesses.

The proposed platform reduces the limitations of manual wireless security assessment by providing centralized analysis, risk classification, visualization, historical tracking, and reporting. The dashboard makes it easier to identify insecure configurations, prioritize high-risk findings, and monitor changes in the wireless environment over time.

Overall, the system can serve as a useful solution for wireless security auditing, network administration, cybersecurity education, and authorized security assessment. Future enhancements can include continuous wireless monitoring, improved anomaly detection, automated security-policy compliance checking, integration with enterprise network-management platforms, and advanced risk analytics. When used only on authorized networks, the system can contribute to stronger Wi-Fi configurations, improved network visibility, and better overall wireless security.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.
[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.
[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm
[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.
[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, “Real-Time Object Detection in Drone Surveillance Using YOLOv5,” in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.
[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, “Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks,” in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.
[7] R. D. Kumar, V. N. S.Manaswini, “Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology,” in

Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.