Wifi Bastion

G. Sailaja
Computer Science & Engineering-Cybersecurity & IoT,
Malla Reddy University, Hyderabad, India
sailaja_g@mallareddyuniversity.ac.in

Sailakshman Rangisetti
Computer Science & Engineering
Cyber Security
Malla Reddy University, Hyderabad, India
2211CS040134@mallareddyuniversity.ac.in

S Mohammed Aadil
Computer Science & Engineering
Cyber Security
Malla Reddy University, Hyderabad, India
2211CS040139@mallareddyuniversity.ac.in

T. Bhavesh
Computer Science & Engineering
Cyber Security
Malla Reddy University, Hyderabad, India
2211CS040156@mallareddyuniversity.ac.in

Abstract — Wi-Fi Bastion is a web-based application designed to protect users from cyber threats posed by malicious Wi-Fi networks. It scans available networks in real time, detecting security risks such as weak encryption and "Evil Twin" attacks. The backend, developed in Python, utilizes advanced network scanning techniques to analyze SSIDs, BSSIDs, encryption types, and signal strengths. The front end, built with HTML, CSS, and JavaScript using Bootstrap, provides an intuitive and responsive interface. A MongoDB database stores historical scan data, allowing users to track threats over time. Wi-Fi Bastion offers real-time alerts and risk assessments, ensuring safer connections, particularly in public spaces like cafes and airports. This application enhances network security by enabling informed decision-making before connecting.

Keywords: Wi-Fi security, Cyber Threats, Malicious Networks, Evil Twin Attack, Encryption, Risk Assessment, SSID, BSSID, Network Analysis, Signal Strength, Real Time Scan.

I. INTRODUCTION

With the increasing reliance on wireless connectivity, ensuring the security of Wi-Fi networks has become a critical concern. Public Wi-Fi networks, commonly found in cafes, airports, and hotels, often lack robust security measures, making them prime targets for cybercriminals. Attackers exploit vulnerabilities in these networks to launch phishing attacks, steal sensitive information, and deploy malware. To address these threats, Wi-Fi Bastion is developed as an advanced web-based application designed to safeguard users from malicious Wi-Fi networks.

Wi-Fi Bastion operates by scanning available networks in real time, identifying security risks such as weak or absent encryption and Evil Twin attacks—where malicious actors create rogue access points mimicking legitimate hotspots. The application's backend, built with Python, utilizes advanced network scanning libraries to analyze critical network parameters, including SSIDs, BSSIDs, encryption types, and signal strengths. A MongoDB database is integrated to store historical network scan data, enabling users to track potential threats over time.

The intuitive front end, developed using HTML, CSS, JavaScript, and Bootstrap, ensures a seamless and responsive user experience across different devices. Wi-Fi Bastion provides real-time alerts and risk assessments, empowering users to make informed decisions before connecting to a network. By offering proactive security insights, Wi-Fi Bastion plays a crucial role in enhancing Wi-Fi safety, making it an essential tool for individuals and businesses alike.

II. LITERATURE SURVEY

The proliferation of public Wi-Fi networks has introduced significant security challenges, as these networks are often targeted by cybercriminals employing various attack vectors. One prevalent threat is the Man-in-the-Middle (MitM) attack, where an attacker intercepts communication between a user and the internet, potentially capturing sensitive information.

Another common threat is the Evil Twin attack, wherein malicious actors set up rogue Wi-Fi access points that mimic legitimate networks. Unsuspecting users may connect to these deceptive networks, inadvertently exposing their data to interception. To combat these threats, several solutions have been proposed and implemented. Intrusion Detection Systems (IDS), such as Kismet, monitor network traffic to identify and alert users of suspicious activities.

Additionally, certificate-based authentication (CBA) has been recommended as a robust security measure. By utilizing 802.1X certification, which authenticates both the wireless network and the user, CBA can significantly reduce the likelihood of unauthorized network access and mitigate potential attacks.

Despite these advancements, challenges persist. Many existing solutions require specialized hardware, are complex to deploy, or may not effectively detect sophisticated attacks. Therefore, there is a pressing need for user-friendly, accessible tools that can provide real-time protection against malicious Wi-Fi networks. Addressing this gap, applications like Wi-Fi Bastion have been developed to offer proactive security measures, enabling users to identify and avoid potential threats in public Wi-Fi environments.

Several studies have explored the vulnerabilities of public Wi-Fi networks and the effectiveness of existing security protocols. Research highlights the risks posed by open and weakly encrypted networks, emphasizing the ease with which attackers can intercept data using tools like packet sniffers and rogue access points. Studies on WPA3 improvements suggest better encryption methods, yet adoption remains slow, leaving many users exposed to older, less secure protocols. Additionally, recent advancements in intrusion detection systems (IDS) and AI-driven threat analysis have shown promise in identifying malicious Wi-Fi networks in real time, reinforcing the need for automated security solutions like Wi-Fi Bastion to bridge the gap between awareness and protection.

III. SYSTEM ANALYSIS

Problem Statement: With the increasing reliance on public Wi-Fi networks, users are frequently exposed to security risks such as Man-in-the-Middle (MitM) attacks, Evil Twin attacks, rogue access points, and weak encryption vulnerabilities. Many users unknowingly connect to malicious networks that can intercept sensitive data, leading to identity theft, credential leaks, financial fraud, and unauthorized surveillance. Traditional security solutions, such as antivirus software and VPNs, do not always provide real-time detection of these threats, leaving users vulnerable to cyberattacks. Additionally, most existing Wi-Fi security tools are either too complex for general users or lack real-time network analysis capabilities. There is a significant gap in the market for a user-friendly, real-time threat detection system that can analyze public Wi-Fi networks, classify risks, and alert users before they connect to an unsafe network.

Wi-Fi Bastion addresses this gap by providing an automated, real-time Wi-Fi security assessment tool that scans available networks, evaluates their security attributes, and warns users of potential risks. By leveraging advanced network scanning techniques, risk classification models, and a historical database of suspicious networks, Wi-Fi Bastion empowers users to make informed decisions and safeguard their data from cyber threats in public environments.

The growing reliance on public Wi-Fi networks has introduced significant security concerns, as cybercriminals increasingly exploit vulnerabilities in open networks to launch attacks such as Evil Twin attacks, Man-in-the-Middle (MitM) attacks, and rogue access points. Traditional security solutions often fail to detect such threats in real-time, leaving users vulnerable to data breaches and unauthorized access. Wi-Fi Bastion is designed to bridge this security gap by providing real-time scanning and threat detection for wireless networks, helping users make informed decisions before connecting to a potentially dangerous network.

Wi-Fi Bastion leverages Python-based backend processing with advanced network scanning libraries to assess SSIDs, BSSIDs, encryption types, and signal strengths. By integrating a MongoDB database, the application enables historical tracking of suspicious networks, allowing users to monitor potential threats over time. Its front-end, developed using HTML, CSS, JavaScript, and Bootstrap, ensures a user-friendly interface accessible from any modern web browser. By combining real-time threat detection with intelligent risk assessment, Wi-Fi Bastion enhances wireless security for individuals and organizations, particularly in high-risk environments like cafes, airports, and hotels.

Wi-Fi Bastion is designed to provide real-time threat detection and risk assessment for public wireless networks, ensuring users can make informed decisions before connecting. The system continuously scans nearby Wi-Fi networks, analyzing SSID, BSSID, encryption protocols, and signal strength to detect vulnerabilities such as weak encryption, open networks, and rogue access points. One of its standout features is Evil Twin attack detection, where it identifies malicious networks that impersonate legitimate ones, helping users avoid potential Man-in-the-Middle (MitM) attacks. The platform also incorporates a risk classification system, categorizing detected networks into low, moderate, or high-risk levels and offering recommendations accordingly. Furthermore, Wi-Fi Bastion maintains a historical database using MongoDB, allowing users to track security trends and analyze threats over time. A user-friendly dashboard consolidates all collected data into an intuitive interface, displaying network attributes, security alerts, and past scan records in an easily accessible format. The system’s cross-platform compatibility ensures seamless access from desktops, tablets, and mobile devices, making it a convenient and effective cybersecurity tool.

Existing System:

Currently, most users rely on basic security measures such as antivirus software, VPNs, and manual verification of network names to protect themselves while using public Wi-Fi. However, these methods are often inadequate in detecting sophisticated attacks like Evil Twin attacks, Man-in-the-Middle (MitM) attacks, and rogue access points. Traditional security solutions such as firewalls and endpoint protection mainly focus on device-level security rather than assessing the safety of wireless networks before users connect.

Additionally, many existing Wi-Fi security solutions provided by operating systems and mobile applications lack real-time scanning and proactive risk assessment. Users often have no means to verify a network's security status before connecting, making them vulnerable to cyber threats. While enterprise-level security tools offer advanced protection, they are typically too complex and costly for everyday users, leaving a gap in accessible Wi-Fi security solutions.

Furthermore, manual methods such as checking for HTTPS encryption, avoiding open networks, or verifying Wi-Fi names with service providers are not always reliable and depend on user awareness. Many users unknowingly connect to networks that appear legitimate but are, in fact, malicious clones designed to capture sensitive information. The absence of centralized threat intelligence and historical tracking makes it difficult to identify recurring security risks.

Given these challenges, there is a clear need for an automated Wi-Fi security assessment tool that can analyze public networks, detect potential threats, and provide users with real-time warnings before they connect. Wi-Fi Bastion addresses this issue by offering a streamlined and intelligent approach to safeguarding wireless network connections, making it a valuable tool for individuals and businesses alike.

Proposed System:

Wi-Fi Bastion offers numerous advantages by adopting a proactive approach to Wi-Fi security rather than relying on reactive defenses. By analyzing networks before a connection is established, the system prevents unauthorized access and mitigates potential cyber threats. Automated alerts and real-time notifications ensure that users are immediately informed of suspicious networks, reducing the risk of data breaches. The integration of advanced analytics and historical data tracking allows users to gain deeper insights into evolving cyber threats and make informed security decisions. Designed for scalability and high performance, Wi-Fi Bastion efficiently handles multiple network scans while maintaining speed and accuracy. The platform also prioritizes privacy and data security, ensuring that all collected information is encrypted and stored securely, with access restricted to authorized users. By offering comprehensive wireless security insights, Wi-Fi Bastion empowers individuals, businesses, and frequent travelers to protect their personal data and online activity while using public Wi-Fi.

IV. METHODOLOGY

A. Architecture Modules:

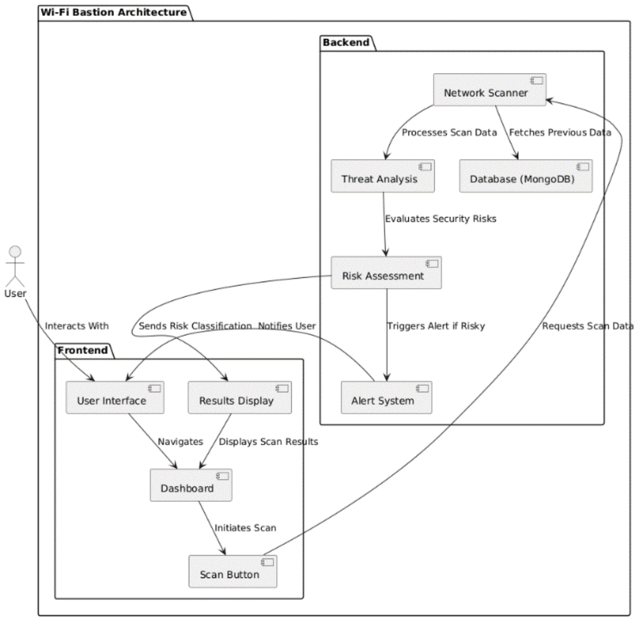

Figure 1: Architecture diagram

The Wi-Fi Bastion system architecture is designed to provide real-time threat detection and risk assessment for wireless networks. The application consists of a frontend (User Interface and Dashboard) that interacts with backend services through API requests. These backend services handle critical functionalities like network scanning, threat analysis, risk assessment, and notifications while integrating with a MongoDB database for storing scan history and detected threats.

Frontend Module:

The frontend layer provides an intuitive interface for users to interact with the system. The Dashboard allows users to initiate Wi-Fi scans, view risk assessments, and access historical scan reports. The User Interface is designed for seamless navigation across features, ensuring a smooth experience across devices. The system displays scan results in a structured format, categorizing networks into low, moderate, or high-risk levels while offering security recommendations.

Backend Module:

The backend layer is responsible for processing scan data, evaluating risks, and storing network insights. The Network Scanning Service collects information about nearby Wi-Fi networks, including SSID, BSSID, encryption type, and signal strength. The Threat Analysis Module examines network attributes to identify security risks such as Evil Twin attacks, rogue access points, and weak encryption. The Risk Assessment Engine assigns risk levels based on predefined security criteria, while the Notification Service alerts users about high-risk networks.

Database Module:

The database layer, built on MongoDB, stores scan results, user data, and historical threat logs. It maintains records of previously scanned networks, enabling users to track security patterns over time. The backend services interact with the database to retrieve past scan data and refine threat detection accuracy.

Additional Considerations

Future enhancements could include cloud-based deployment for scalability, caching mechanisms to optimize performance, and AI-driven threat prediction models. Implementing load balancing strategies would improve the system's ability to handle high user traffic, while integration with enterprise security platforms could extend its use for corporate environments. The modular design ensures maintainability, security, and ease of future upgrades.

V. CONCLUSION

The increasing reliance on public Wi-Fi networks has introduced significant cybersecurity risks, making users vulnerable to attacks such as Evil Twin attacks, Man-in-the-Middle (MitM) attacks, and rogue access points. Traditional security solutions often fail to provide real-time detection and protection against these sophisticated threats. Wi-Fi Bastion addresses this critical security gap by offering an advanced real-time network scanning and threat detection system that helps users make informed decisions before connecting to a wireless network.

Wi-Fi Bastion's intelligent risk assessment framework ensures that users receive detailed insights into the security status of detected networks. By leveraging Python-based backend processing and advanced network scanning libraries, the system accurately analyzes SSID, BSSID, encryption protocols, and signal strength to identify potential threats. The MongoDB database allows for historical tracking of suspicious networks, enabling users to monitor evolving security risks over time. This feature is particularly beneficial for individuals and organizations that frequently operate in high-risk environments such as cafes, airports, and hotels.

In conclusion, Wi-Fi Bastion represents a significant advancement in wireless security by offering real-time network monitoring, intelligent risk assessment, and proactive threat prevention. With its modular architecture, user-friendly design, and comprehensive security features, it serves as an essential tool for individuals, businesses, and security professionals looking to safeguard their wireless connections from cyber threats. By continuously evolving to counter emerging attack techniques, Wi-Fi Bastion ensures a safer and more secure digital experience in an increasingly interconnected world.

VI. FUTURE SCOPE

One of the most promising advancements is the integration of artificial intelligence (AI) and machine learning (ML) to enhance threat detection capabilities. By analyzing patterns in network activity, attack vectors, and user behavior, AI can help predict and prevent emerging threats before they occur. ML algorithms can also reduce false positives by learning from historical data, improving the accuracy of risk assessments. Over time, this adaptive learning model will make Wi-Fi Bastion more intelligent in detecting sophisticated man-in-the-middle (MitM) attacks, rogue access points, and Evil Twin networks.

Cloud-based deployment is another key area for future development. Hosting Wi-Fi Bastion on a cloud platform would enable users to access network security insights from any location, ensuring continuous monitoring of Wi-Fi networks across multiple devices. This approach would also improve scalability, allowing organizations to monitor large-scale enterprise networks without compromising performance. Additionally, cloud integration can support centralized threat intelligence sharing, where multiple users contribute to a crowdsourced database of malicious Wi-Fi networks, enhancing security for the entire user base.

In summary, the future of Wi-Fi Bastion lies in AI-powered security enhancements, cloud-based scalability, mobile integration, and advanced automation. Wi-Fi Bastion can become an indispensable tool for individuals and organizations seeking unparalleled wireless network protection.

REFERENCES

1. **How To Secure Your Home Wi-Fi Network**
   Federal Trade Commission, Consumer Advice, 2022.

2. **Securing Wireless Networks**
   Cybersecurity & Infrastructure Security Agency (CISA), 2020.

3. **Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained**
   eSecurity Planet, 2023.

4. **Wi-Fi Security: Do We Still Have to Look Back?**
   International Association for Cryptologic Research (IACR), 2022.

5. **Wireless Technology Security and Privacy: A Comprehensive Study**
   ResearchGate, 2024.

6. **Securing Wireless Devices in Public Settings**
   U.S. Department of Defense, 2021.

7. **Everything You Should Know About Wi-Fi Security**
   Smallstep, 2023.

8. **Wireless Network Security: Risks, Evolutions, and Best Practices**
   LBMC, 2022.

9. **ComPass: Proximity Aware Common Passphrase Agreement Protocol for Wi-Fi Devices Using Physical Layer Security**
   arXiv, 2021.

10. **A Wireless Intrusion Detection System for 802.11 WPA3 Networks**
    arXiv, 2021.

    Tamper-Evident Pairing
    arXiv, 2023.

11. **From Dragondoom to Dragonstar: Side-channel Attacks and Formally**

12. **The Evolution of Wi-Fi Security: Why WPA Matters in 2024**
    Lifewire, 2024.

13. **Matter Will Be Better in 2025 - Say the People Who Make It**
    The Verge, 2025.

14. **Wi-Fi Security: Best Practices for Protecting Your Network**
    TechRadar, 2023.

15. **Understanding WPA3: The Next Generation of Wi-Fi Security**
    Network World, 2022.

16. **Wi-Fi Security Threats and How to Mitigate Them**
    CSO Online, 2023.

17. **Advancements in Wi-Fi Security Protocols: A Comparative Analysis**
    Journal of Cybersecurity Research, 2024.