IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EVIL TWIN WI-FI NETWORK DETECTION SYSTEM

1st Mr. Dr. S. SASIKALA
AP - Cyber security Engineering
Paavai Engineering College
(Anna University Affiliated)
Namakkal, India

2nd S. MANOJ KUMAR
Cyber security Engineering
Paavai Engineering College
(Anna University Affiliated)
Namakkal, India

3rd K. MADHAN
Cyber security Engineering
Paavai Engineering College
(Anna University Affiliated)
Namakkal, India

4th S. SENTHAMARAI KANNAN
Cyber security Engineering
Paavai Engineering College (Anna University Affiliated)
Namakkal, India

Abstract: The rapid expansion of public Wi-Fi access in places such as airports, cafés, and educational institutions has increased exposure to wireless security threats. One of the most dangerous among them is the Evil Twin attack, a type of rogue access point attack where an attacker creates a fraudulent Wi-Fi network that mimics a legitimate one. Unsuspecting users connect to this malicious network, allowing attackers to intercept sensitive information such as login credentials, banking details, and personal data through techniques like man-in-the-middle attacks and packet sniffing.The proposed Evil Twin Wi-Fi Network Detection System is designed to identify and prevent connections to such malicious access points by continuously monitoring wireless network parameters and analyzing inconsistencies. The system compares attributes such as SSID (Service Set Identifier), BSSID (MAC address), signal strength, encryption type, channel number, and network certificates to detect suspicious variations between genuine and rogue networks. Machine learning algorithms can be integrated to enhance detection accuracy by identifying behavioral anomalies in real time.The system operates through three major modules: network scanning, anomaly detection, and alert generation. It performs real-time monitoring of nearby Wi-Fi networks, validates them against trusted profiles, and notifies users or administrators when a potential Evil Twin is detected. The solution can be implemented using lightweight tools and Python-based frameworks, making it suitable for deployment in educational campuses, corporate environments, and public Wi-Fi hotspots. By providing early detection and automated alerts, the proposed system significantly reduces the risk of data breaches and identity theft. It enhances wireless security awareness and contributes to building a safer networking environment for users in increasingly connected digital ecosystems.

Keywords – Sign language, Arduino, ASL, Sound Glove, Dumb, Gesture recognition, Deaf, Flex.

I. INTRODUCTION:

Wireless networks have become an essential part of modern digital infrastructure, enabling seamless internet connectivity in homes, offices, educational institutions, and public spaces. With the widespread adoption of Wi-Fi technology, users increasingly rely on wireless networks for communication, online transactions, cloud access, and remote work. However, this convenience has also introduced significant security vulnerabilities. Among various wireless threats, the Evil Twin attack has emerged as one of the most deceptive and dangerous forms of cyberattack.

An Evil Twin attack occurs when a malicious actor sets up a rogue access point that imitates a legitimate Wi-Fi network by copying its Service Set Identifier (SSID) and other characteristics. Because most devices automatically connect to known or stronger signals, users may unknowingly connect to the fraudulent network. Once connected, attackers can intercept data, monitor traffic, inject malicious content, or perform man-in-the-middle attacks. Sensitive information such as usernames, passwords, banking details, and confidential organizational data can be compromised without the user’s knowledge.

Traditional security measures such as encryption protocols and password protection are not always sufficient to defend against Evil Twin attacks, especially in public Wi-Fi environments where users cannot easily verify network authenticity. Furthermore, many users lack awareness about identifying suspicious networks, making them more vulnerable to exploitation. Therefore, there is a critical need for an intelligent and automated detection mechanism that can identify rogue access points before damage occurs.

The proposed Evil Twin Wi-Fi Network Detection System aims to address this challenge by continuously monitoring wireless network parameters and detecting anomalies that indicate the presence of a fake access point. By analyzing attributes such as MAC addresses (BSSID), signal strength fluctuations, encryption standards, channel information, and network behavior patterns, the system can differentiate between legitimate and malicious networks. Real-time alerts and automated responses further enhance protection.

This system not only strengthens wireless security but also promotes safer internet usage in public and private environments, helping organizations and individuals protect their sensitive data from increasingly sophisticated wireless threats.

II. EXISTING SYSTEM:

In the current scenario, protection against Evil Twin Wi-Fi attacks primarily depends on traditional wireless security mechanisms and general network monitoring tools. Most organizations rely on encryption protocols such as WPA2 and WPA3 to secure wireless communications. While these protocols provide strong data encryption, they do not inherently prevent attackers from creating rogue access points with the same SSID as legitimate networks. As a result, users may still connect to a malicious network that appears authentic.

Another commonly used approach in existing systems is manual verification by network administrators. Administrators monitor network traffic logs, check MAC addresses, and periodically scan for unauthorized access points using tools like wireless analyzers or intrusion detection systems (IDS). However, this method is time-consuming and requires technical expertise. It is not suitable for real-time detection in large or dynamic environments such as airports, colleges, or corporate campuses.

Some enterprises implement Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS). These systems can detect rogue access points by comparing connected devices against a predefined list of authorized access points. Although effective in controlled enterprise networks, they are often expensive and require specialized hardware, making them impractical for small organizations or public Wi-Fi setups.

Additionally, most end-user devices lack built-in mechanisms to automatically verify the authenticity of Wi-Fi networks beyond password matching. Users must rely on visual identification of network names and signal strength, which attackers can easily replicate.

Overall, the existing system suffers from limitations such as high deployment cost, lack of real-time automated detection for individual users, limited scalability, and dependency on manual monitoring. These challenges highlight the need for a more intelligent, lightweight, and automated solution specifically designed to detect Evil Twin Wi-Fi networks effectively.

III. PROPOSED SYSTEM:

The proposed Evil Twin Wi-Fi Network Detection System is designed as an automated, intelligent, and lightweight solution to identify and prevent rogue access point attacks in real time. Unlike traditional systems that rely mainly on manual monitoring or expensive enterprise hardware, this system focuses on continuous wireless network analysis combined with anomaly detection techniques to ensure faster and more accurate identification of malicious networks.

The system operates in three major phases: network scanning, verification, and alert generation. During the scanning phase, the system continuously monitors nearby Wi-Fi networks and collects parameters such as SSID, BSSID (MAC address), signal strength (RSSI), channel number, encryption type, and authentication protocol. In the verification phase, the collected data is compared with a trusted database of legitimate access points. Any mismatch in MAC address, sudden signal strength fluctuation, duplicate SSIDs with different BSSIDs, or changes in encryption standards is flagged as suspicious behavior.

To enhance detection accuracy, the proposed system can integrate machine learning algorithms that analyze historical network behavior and identify abnormal patterns. For example, if two networks share the same SSID but operate on different channels or exhibit unusual signal behavior, the system recognizes it as a potential Evil Twin attack.

Once a threat is detected, the alert module immediately notifies users or administrators through on-screen warnings, logs, or email notifications. The system can also optionally block automatic connections to suspicious networks.

This proposed solution is cost-effective, scalable, and suitable for deployment in educational institutions, corporate offices, and public Wi-Fi zones. By combining real-time monitoring with intelligent analysis, the system significantly strengthens wireless network security and reduces the risk of data interception and identity theft.

IV. HARDWARE DESCRIPTION:

1. Central Processing Unit (CPU)

The Central Processing Unit (CPU) acts as the core component of the Evil Twin Wi-Fi Network Detection System. It is responsible for executing detection algorithms, processing captured wireless packets, comparing network parameters, maintaining logs, and generating alerts. Since the system performs continuous real-time monitoring, the processor must be capable of handling multiple parallel tasks such as packet decoding, anomaly detection, and database verification without performance lag.

A minimum dual-core processor can support small-scale deployments, but for enterprise-level monitoring, a multi-core processor such as Intel i5/i7 or AMD Ryzen 5/7 is recommended. Higher clock speeds ensure faster packet analysis and quicker identification of rogue access points. If machine learning algorithms are integrated for advanced anomaly detection, additional processing power is required to train and execute models efficiently.

The system also benefits from sufficient RAM (8 GB or more) to temporarily store packet captures and run background services smoothly. Solid-State Drives (SSD) are preferred over traditional HDDs because they allow faster read/write operations for log files and threat databases. For portable or low-cost implementations, compact devices like the Raspberry Pi 4 can be deployed as distributed sensors in multiple locations.

Overall, the CPU ensures real-time responsiveness, accurate threat detection, and smooth system operation, making it a fundamental hardware component of the proposed solution.

2. Wireless Network Interface Card (NIC)

The Wireless Network Interface Card (NIC) is the most critical hardware component in the Evil Twin Detection System. Its primary function is to capture wireless signals, scan nearby access points, and collect detailed information about network parameters such as SSID, BSSID, signal strength (RSSI), encryption type, and channel number.

Unlike standard Wi-Fi adapters used for normal internet connectivity, the detection system requires a NIC that supports monitor mode. Monitor mode allows the adapter to capture raw IEEE 802.11 frames without connecting to any specific network. This capability enables deep packet inspection and identification of duplicate SSIDs or suspicious MAC addresses. Additionally, support for packet injection is beneficial for advanced testing and verification of rogue access points.

Dual-band capability (2.4 GHz and 5 GHz) is important because attackers may create Evil Twin networks on different frequency bands to avoid detection. A high-sensitivity external USB Wi-Fi adapter improves scanning range and ensures accurate signal strength comparison. This helps in detecting anomalies such as sudden signal spikes or unusual fluctuations that indicate a rogue access point operating nearby.

Enterprise environments may deploy multiple wireless adapters as distributed sensors across buildings to ensure complete coverage. The NIC continuously feeds collected data to the processing unit for analysis. Therefore, selecting a reliable, monitor-mode-supported Wi-Fi adapter directly impacts the system’s detection accuracy and overall performance.

3. Antenna and Signal Monitoring Hardware

The antenna system plays a significant role in improving the accuracy and coverage of Evil Twin detection. Wireless signals vary based on distance, interference, and physical obstacles. Therefore, high-quality antennas ensure better reception of beacon frames and more precise measurement of signal strength.

High-gain omnidirectional antennas are suitable for small environments such as classrooms, labs, or offices, as they capture signals from all directions. In larger enterprise setups, directional antennas can be used to focus on specific areas, helping administrators identify the approximate location of a rogue access point. By analyzing signal strength variations from multiple sensor points, triangulation techniques can be applied to locate suspicious devices.

Advanced deployments may include multiple sensor nodes placed at strategic positions across a campus. These nodes collect wireless data and send it to a centralized server for analysis. This distributed approach enhances detection coverage and reduces blind spots.

Signal monitoring hardware also helps in distinguishing between legitimate access points and Evil Twin networks. For example, if two networks share the same SSID but have significantly different signal patterns or transmission power levels, the system flags them as suspicious.

Overall, antenna quality and placement significantly influence detection reliability, making signal monitoring hardware an essential component of the system.

4. Power Supply and Reliability Components

Continuous operation is essential for effective Evil Twin detection, especially in enterprise and public environments. Therefore, a stable power supply system is required to prevent downtime. An Uninterruptible Power Supply (UPS) ensures that the monitoring system remains active during power failures, allowing continuous wireless scanning and threat detection.

In enterprise deployments, the system may be installed in server racks along with cooling systems to prevent overheating during 24/7 operation. Proper ventilation and temperature control increase hardware lifespan and ensure consistent performance.

For distributed sensor-based setups, compact power adapters or Power over Ethernet (PoE) solutions can be used. PoE simplifies installation by delivering both data and power through a single Ethernet cable, reducing wiring complexity.

Backup storage mechanisms are also important for maintaining log integrity. External storage devices or network-attached storage (NAS) systems can store large volumes of packet capture data for forensic analysis. Reliable hardware prevents data loss and ensures accurate historical record maintenance.

In summary, stable power and supporting hardware infrastructure guarantee uninterrupted monitoring, maintain system reliability, and enhance the overall effectiveness of the Evil Twin Wi-Fi Network Detection System.

V. SOFTWARE REQUIREMENTS:

1. Operating System Environment

The Operating System (OS) forms the foundation for the Evil Twin Wi-Fi Network Detection System. Since the system relies heavily on wireless packet capturing and monitor mode functionality, Linux-based operating systems are highly preferred. Distributions such as Kali Linux and Ubuntu provide built-in driver compatibility and advanced networking utilities required for cybersecurity applications.

Linux environments support low-level access to wireless network interface cards, allowing the system to enable monitor mode and capture raw IEEE 802.11 frames. This capability is essential for analyzing beacon frames, authentication packets, and management frames that help identify rogue access points. Additionally, Linux offers strong process control, memory management, and multi-threading capabilities, enabling the detection system to perform continuous background scanning without affecting system performance.

The OS also manages hardware resource allocation such as CPU usage, RAM distribution, and storage access. Stable kernel architecture ensures that packet capture tools operate efficiently without crashes. Security updates and patch management further enhance the reliability of the detection system.

Although Windows and macOS environments can support certain scanning tools, they often have limitations in monitor mode support due to driver restrictions. Therefore, Linux remains the most suitable platform for deploying this system in both research and enterprise environments. A stable operating system ensures uninterrupted monitoring, reliable packet analysis, and overall system performance.

2. Programming Language and Development Framework

The Evil Twin Wi-Fi Detection System is primarily developed using Python due to its simplicity, flexibility, and strong support for cybersecurity applications. Python provides extensive libraries for networking, packet analysis, database management, and machine learning, making it an ideal choice for rapid and modular development.

Python's readable syntax allows developers to design structured modules such as network scanning, anomaly detection, alert systems, and database management separately. This modular architecture improves scalability and simplifies system maintenance. If updates or enhancements are required, new modules can be integrated without affecting existing functionalities.

Several frameworks and libraries support development. Packet analysis libraries enable real-time capture and inspection of wireless frames. Data processing libraries help organize and filter collected network parameters. Machine learning libraries assist in detecting abnormal behavior patterns based on historical network data.

Python also supports multi-threading and asynchronous programming, allowing the system to scan networks and analyze data simultaneously. This improves detection speed and ensures real-time alert generation. Additionally, Python integrates easily with web frameworks, enabling dashboard creation for administrators.

Because Python is open-source and cross-platform, it reduces development cost and ensures compatibility with multiple hardware platforms. Overall, Python enhances flexibility, scalability, and rapid development of the Evil Twin Wi-Fi Network Detection System.

3. Network Scanning and Packet Capture Module

The Network Scanning and Packet Capture Module is responsible for collecting wireless network data from the surrounding environment. This module activates monitor mode in the wireless adapter and continuously scans available Wi-Fi networks. It captures beacon frames broadcasted by access points and extracts important parameters such as SSID, BSSID (MAC address), signal strength (RSSI), channel number, encryption type, and authentication protocol.

The scanning process operates in real time, updating the list of available networks dynamically. The module ensures that duplicate SSIDs are identified immediately. Since attackers often replicate legitimate network names to create Evil Twin access points, detecting multiple networks with the same SSID is a primary defense mechanism.

Captured packets are temporarily stored in memory buffers for analysis. The module filters unnecessary data to reduce processing load. Efficient packet filtering improves system performance and minimizes storage consumption.

In enterprise environments, the scanning module can operate continuously and synchronize with centralized monitoring servers. For portable setups, it can function independently on a single device.

The accuracy of detection depends heavily on this module's ability to capture reliable data. Therefore, proper configuration of scanning intervals, channel hopping techniques, and signal strength thresholds is essential. Overall, this module forms the backbone of the detection system by providing accurate and real-time wireless data for further analysis.

4. Anomaly Detection and Analysis Engine

The Anomaly Detection Engine is the intelligence core of the Evil Twin Wi-Fi Detection System. It analyzes collected wireless parameters and identifies suspicious patterns that indicate the presence of a rogue access point.

This module compares scanned network data with a predefined database of authorized access points. It verifies whether the BSSID matches the legitimate MAC address assigned to a specific SSID. If two access points share the same SSID but have different MAC addresses, the system flags the network as suspicious.

In addition to basic comparison, the engine analyzes signal strength fluctuations. For example, if a network with a known SSID suddenly appears with significantly stronger or weaker signal levels in unusual locations, it may indicate a potential Evil Twin. Encryption mismatches and sudden changes in authentication protocols are also considered warning signs.

To enhance detection accuracy, machine learning algorithms can be integrated. These algorithms learn normal network behavior over time and detect deviations automatically. Behavioral analysis reduces false positives and improves reliability.

The engine processes data continuously and operates with predefined thresholds. If suspicious conditions exceed these thresholds, the alert module is triggered. By combining rule-based detection with intelligent analysis, the anomaly detection engine ensures efficient identification of malicious wireless networks.

5. Alert, Reporting, and Logging Module

The Alert and Reporting Module ensures immediate response when a potential Evil Twin network is detected. Once the anomaly detection engine confirms suspicious behavior, this module generates notifications for users or network administrators.

Alerts can be displayed as on-screen warnings, pop-up messages, email notifications, or SMS alerts in enterprise systems. The notification includes details such as SSID name, rogue MAC address, signal strength comparison, and time of detection. Providing detailed information helps administrators take quick corrective action.

The module also maintains comprehensive logs of detected events. Logs include packet details, network parameters, timestamps, and detection results. These logs are stored in a secure database for future forensic analysis.

Reporting features may include graphical dashboards showing network trends, duplicate SSID occurrences, and historical attack patterns. This visualization improves decision-making and enhances security awareness.

In large organizations, the reporting module can generate periodic security reports summarizing detected threats and system performance metrics. Automated reporting reduces manual effort and ensures consistent monitoring.

Overall, this module strengthens system responsiveness and accountability by providing timely alerts, maintaining detailed records, and supporting post-incident investigation.

VI. CONCLUSION:

The Evil Twin Wi-Fi Network Detection System provides an effective and intelligent solution to one of the most serious wireless security threats in modern networking environments. As public and private Wi-Fi usage continues to grow rapidly, attackers increasingly exploit user trust by creating fraudulent access points that imitate legitimate networks. Traditional security mechanisms such as WPA2/WPA3 encryption alone are not sufficient to prevent users from connecting to rogue networks. Therefore, proactive detection mechanisms are essential to ensure data confidentiality and network integrity.

The proposed system addresses this challenge through continuous wireless monitoring, real-time packet analysis, and intelligent anomaly detection. By examining parameters such as SSID, BSSID, signal strength, channel information, and encryption type, the system can accurately identify suspicious networks that mimic authorized access points. The integration of machine learning techniques further enhances detection accuracy by recognizing abnormal behavioral patterns and reducing false alarms.

Additionally, the modular software architecture ensures scalability and flexibility. The system can be deployed as a lightweight standalone tool for small environments or expanded into a distributed enterprise-level monitoring solution with centralized control. Automated alerts and detailed logging improve response time and support forensic investigation.

Overall, the Evil Twin Wi-Fi Network Detection System strengthens wireless network security, protects sensitive user information, and promotes safe internet usage. By combining cost-effective hardware requirements with intelligent software analysis, the system provides a practical and reliable defense against evolving wireless threats in today’s digital ecosystem.

VII. RESULT AND DISCUSSION:

7.1 RESULT:

The Evil Twin Wi-Fi Network Detection System was tested in a controlled wireless environment consisting of legitimate access points and simulated rogue (Evil Twin) networks. The system continuously scanned nearby Wi-Fi signals and analyzed parameters such as SSID, BSSID (MAC address), signal strength (RSSI), encryption type, and channel number.

During testing, when a rogue access point was configured with the same SSID as a legitimate network but with a different MAC address, the system successfully identified the duplication. It detected inconsistencies between authorized database records and the scanned network parameters. In cases where the attacker used stronger signal strength to lure users, the system flagged abnormal signal spikes and generated alerts in real time.

The detection accuracy improved further when anomaly-based analysis was enabled. The system demonstrated high reliability in identifying duplicate SSIDs and encryption mismatches. False positives were minimal when threshold values were properly configured. Alert notifications were generated instantly, and detailed logs were recorded for further investigation.

Performance evaluation showed that the system consumed moderate CPU and memory resources, making it suitable for deployment on both standard computers and compact devices. Overall, the experimental results confirmed that the system can effectively detect Evil Twin attacks in real-time scenarios.

7.2 DISCUSSION:

The results indicate that continuous wireless monitoring combined with intelligent parameter comparison is an effective strategy for identifying rogue access points. Unlike traditional security methods that rely only on encryption, this system actively analyzes network behavior and configuration details.

One key observation is that signal strength analysis plays a critical role in detection, especially when attackers attempt to attract victims using stronger transmission power. However, environmental factors such as interference and physical obstacles may affect signal measurements, which must be considered when configuring detection thresholds.

The integration of machine learning enhances system performance by learning normal network behavior over time. This reduces false alarms and improves accuracy in dynamic environments. However, training models requires sufficient historical data for reliable results.

In enterprise deployments, distributed sensors improve coverage and help locate rogue devices more precisely. Although initial setup may require configuration effort, the long-term security benefits outweigh the complexity.

Overall, the system proves to be a practical, scalable, and cost-effective solution for protecting users against Evil Twin Wi-Fi attacks while maintaining efficient performance and high detection reliability.

VIII. ACKNOWLEDGEMENT:

Certainly, acknowledging the support and contribution of Paavai Engineering College, particularly the teaching and non-teaching staff of the Department of Cyber security, is essential. Additionally, expressing gratitude to our parents, friends, and all those who have provided direct or indirect support for this research is imperative.

IX. REFERENCE:

[1] IEEE, IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 802.11 Standard.

[2] Wi-Fi Alliance, Wi-Fi Protected Access 3 (WPA3) Specification, Security Enhancements for Wireless Networks.

[3] National Institute of Standards and Technology, Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153.

[4] William Stallings, Wireless Communications and Networks, Pearson Education.

[5] Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall.

[6] OWASP, Wireless Security Testing Guide.

[7] SANS Institute, Wireless Network Security and Rogue Access Point Detection Reports.

[8] Kali Linux Documentation, Offensive Security, Wireless Penetration Testing Tools.

[9] Scapy Official Documentation, Packet Capture and Analysis Framework.

[10] International Journal of Computer Applications, Research Articles on Rogue Access Point Detection and Wireless Intrusion Detection Systems.