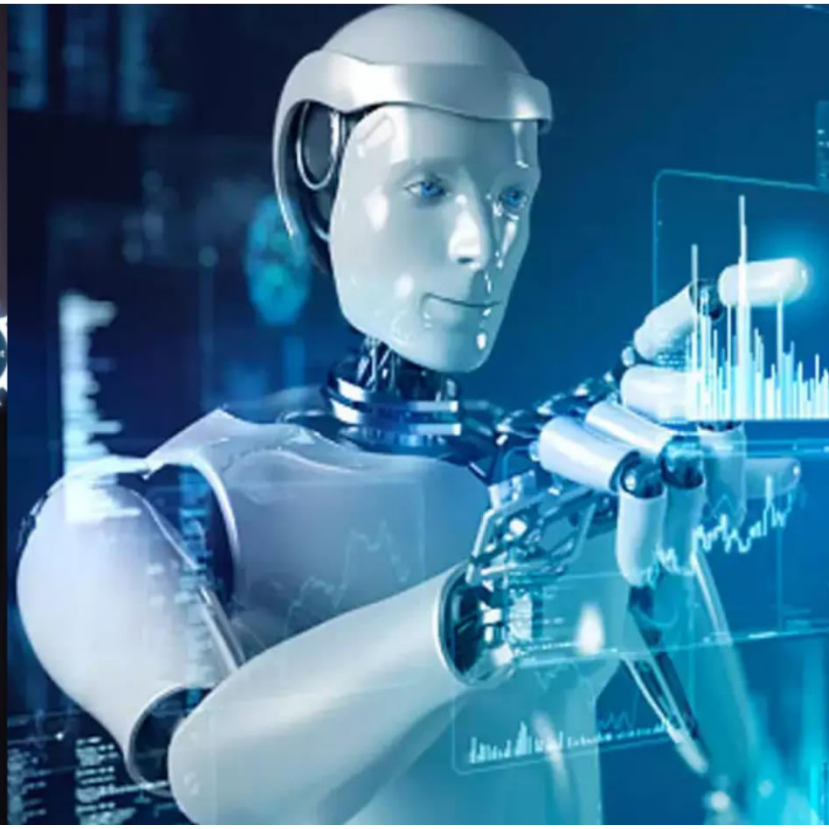
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

Secure Air Wireless - Spying Shield Rouge Accesspoint Detector

Ria Govitrikar[1], Panchami Hegde[2], Aishwarya Dabak[3]

Engineering Student, Department of Computer Engineering, KC College of Engineering and Management Studies, Maharashtra, India[1]

Engineering Student, Department of Computer Engineering, KC College of Engineering and Management Studies, Maharashtra, India[2]

Engineering Student, Department of Computer Engineering, KC College of Engineering and Management Studies, Maharashtra, India[3]

ABSTRACT: Wireless communications provide the foundation of the modern digital existence but unwittingly result in numerous security risks, such as those based on rogue access points that impersonate authentic Wi-Fi networks and steal information from unsuspecting targets. The present study presents a novel, low-cost, real-time monitorable honeypot and rogue AP detector: Secure Air. The system uses Wi-Fi modules to sniff SSIDs, MACs, and connection attempts, and Raspberry Pi or a comparable processor board is used to process, log, and analyze data. Data are securely sent over Bluetooth to a connected PC, and Python scripts are run to identify duplicate SSIDs, spoofed MACs, and unauthorized open networks. The honeypot AP captures every malicious attempt to make a connection, acting as an integrated dual-layer safeguard. A Flask-based dashboard allows real-time visualization, behavior monitoring, and forensic log downloads. Secure Air puts security, reliability, and usability first while staying budget-friendly, making it perfectly suitable for institutions, workplaces, public spaces, and home use. In addition, experimental testing shows that the system performs at an accuracy rate of around 90%, which proves its feasibility in real-world deployment.

KEYWORDS: Secure Air ; Wi-Fi Security; Rogue Access Points; Honeypot; Raspberry Pi; Wireless Threat Detection; Bluetooth Data Transfer; Flask Dashboard; Portable Cybersecurity Solution.

I. INTRODUCTION

The high rate of wireless network penetration has led to a dramatic change in daily life and business technology. But as Wi-Fi continues to pervade our surroundings, the users are being exposed to emerging cybersecurity threats as well. Perhaps the most insidious and perilous of these threats is the rogue access point (AP). A rogue AP is an unauthorized wireless access point that mimics a valid Wi-Fi network to trick users into joining, compromising their credentials, communications, or personal information. Because such attacks are so easy to carry out—usually with low-cost, easily obtained hardware—rogue APs have been a long-standing cybersecurity threat.

Legacy Wi-Fi security features like WPA2/WPA3 encryption are intended to block unauthorized access but are still ineffective against rogue AP attacks, which exploit human familiarity and trust with known SSIDs. Therefore, unsuspecting users can be tricked into joining malicious networks, which provide attackers with access to sensitive data. This weakness calls for affordable, real-time monitoring tools with the ability to proactively identify and respond to rogue APs.

To fill this void, we present a Bluetooth-linked Wi-Fi honeypot and rogue AP detector called Secure Air. In contrast to traditional plug-and-play equipment relying on IP-based connectivity on a network, Secure Air securely connects to a user's PC through Bluetooth. This enables greater portability, easy configuration, and versatile deployment opportunities—especially in settings where Wi-Fi or Ethernet-based monitoring is not feasible.

Secure Air integrates both hardware and software components in a cohesive architecture. Wi-Fi scanning modules continuously monitor nearby networks, collecting metadata such as SSIDs, MAC addresses, and signal strength. This

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

information is transmitted over a secure Bluetooth channel to a PC, where a Python-based detection algorithm identifies anomalies such as duplicate SSIDs, spoofed MAC addresses, and unauthorized open networks. A honeypot Wi-Fi AP may also be used to lure and monitor malicious connection attempts, enabling thorough behavioral analysis of suspected attackers.

On the software side, a Flask-based dashboard offers an easy-to-use interface for real-time visualization and administration. Users are able to observe live network activity, examine flagged rogue APs, and download security logs for post-event analysis. In comparison with enterprise-class wireless intrusion detection systems, Secure Air prioritizes affordability, accessibility, and usability, making it appropriate not just for organizations but also for schools, small enterprises, and individuals.

Overall, Secure Air provides the following main contributions:
1. Development of a Bluetooth-empowered rogue AP detection system for safe and portable network monitoring.
2. Integration of honeypot functionality to actively capture and record malicious activity.
3. Execution of a real-time Flask-based dashboard offering user-friendly visualization for non-technical users.
In total, Secure Air is a low-cost, portable, and efficient solution that equips users to protect themselves against wireless attacks. Its focus on Bluetooth connectivity minimizes reliance on legacy network infrastructure, promoting better adaptability across various deployment situations.

II. LITERATURE SURVEY

1) RAP: Guarding Commodity Wi-Fi Networks Against Rogue Access Points — Liran Ma, Xiuzhen Cheng, Min Song, and Amin Y. Teymorian (2007)
RAP, a practical protection for commodity Wi-Fi deployments with no modification to the 802.11 standard and no special hardware. The authors first develop a taxonomy of rogue APs before designing RAP as a plugin-style protection layer, classifying unauthorized APs by fusing traffic inspection and policy checks. Their cost-effectiveness and deployability emphasize how sophisticated, off-the-shelf, open-source tools can be orchestrated to enhance network resilience against adversaries, including those who break the standard. RAP is well suited for practical integration on the AP side, but since it relies on visibility on the network side, it would work less well when client behavior comes into play (consider autoconnect, for example) or an off-path adversary is dominant. Work such as Secure Air takes inspiration from this, targeting a similar low-cost commodity deployment environment but shifts sensing to portable hardware with host-side analytics.

2) Wireless Rogue Access Point Detection Using Shadow Honeynet — Neha Agrawal, Shashikala Tapaswi (2015)
The "Shadow Honeynet" architecture proposed by Agrawal and Tapaswi combines anomaly detection and honeypot deception. Their system passively monitors for signs of RAP behavior to verify threats and minimize risk to production assets. It uses controlled honeynet interaction when it detects suspicious activity. The two main contributions are (i) an operational model for interacting safely with potential attackers and (ii) a hybrid detection pipeline that reduces false positives compared to methods that rely solely on anomaly detection. Among the reported benefits are better identification of spoofed SSIDs and attacker probing behavior. However, containment and trigger tuning might be needed to stop attackers from pivoting.

3) Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network — Vishwa Modi, Chandresh Parekh (2017)
Modi and Parekh focus particularly on Evil Twin (ET) scenarios and propose a lightweight detector, which compares the external IP features and identifiers of authentic and fraudulent APs. The authors' approach identifies ETs that can mimic SSIDs but fail to accurately replicate back-end identity traits by leveraging differences that are visible at the client or local monitor. This approach avoids heavy RF fingerprinting or protocol changes, which is desirable for resource-constrained settings. In addition, the authors discuss limitations in cases when even sophisticated attackers impersonate upstream properties and in very dynamic public hotspots that lack "ground truth" regarding legitimate infrastructure. These observations encourage the maintenance of blacklists and whitelists, beacon-level metadata observation, and correlation with backhaul cues in the context of Secure Air to boost confidence in ET detection.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

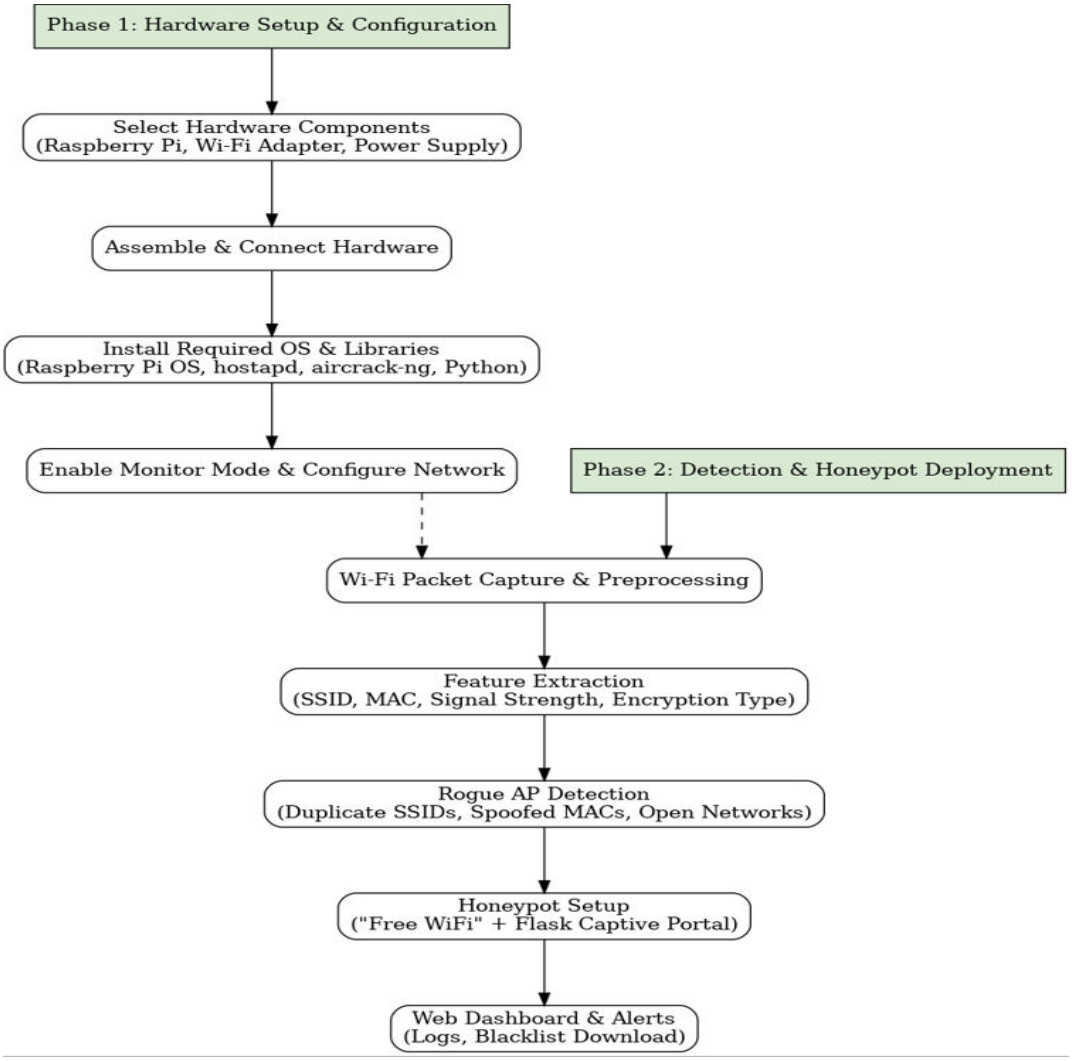
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

4) Real-Time Rogue Wireless Access Point Detection with the Raspberry Pi — Chris Jenks (Linux Journal, 2015)

Jenks demonstrates the use of the Kali Linux ecosystem along with external Wi-Fi adapters to yield a functional WIDS build on the Raspberry Pi that allows for real-time scanning for unauthorized APs. The article, heavily engineering-focused, speaks about imaging, driver support, monitor mode, power-stability warnings on SBCs, and the toolchain needed to identify and notify of rogues. While not a research paper published in a peer-reviewed venue, it provides great value in terms of guidance for deployment, performance trade-offs on low-power hardware, and various practical pitfalls such as USB power drops corrupting SD cards. Confirming that small, portable platforms can provide substantial visibility for rogue-APs if configured correctly and with the appropriate logging pipeline, this validates Secure Air's hardware selections and field-deployment procedures.

III. PROPOSED METHODOLOGY



IV. IMPLEMENTATION / EXPERIMENTAL SETUP

The implementation of Secure Air combines hardware and software to create a low-cost, efficient system for rogue access point detection and honeypot deployment. It focuses on portability, real-time monitoring, and easy deployment in diverse environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

1. Hardware Setup

1. Raspberry Pi (Central Controller Unit):

The Raspberry Pi serves as the core processing unit of the system. It continuously scans nearby Wi-Fi networks, collects beacon frames and probe requests, and performs analysis to identify suspicious or rogue access points. The Raspberry Pi also manages Bluetooth communication, acts as the local server for data transfer, and hosts the honeypot functionalities.

2. Bluetooth Module (Built-in or External Dongle):

A Bluetooth interface enables seamless communication between the Raspberry Pi and the connected PC. This secure link facilitates real-time data transfer without relying on IP-based networks such as Wi-Fi or Ethernet, thereby enhancing portability and minimizing attack exposure.

3. Power Supply:

The Raspberry Pi is powered through a portable power bank or a 5V/3A USB-C adapter, allowing flexible deployment even in remote or outdoor environments.

2. Software Setup

1. Operating System:

The system operates on **Raspberry Pi OS (Lite)** to ensure efficient resource utilization and minimal latency.

2. Programming Languages and Libraries:

- **Python 3:** Core programming language for detection logic, data parsing, and honeypot management.
- **Scapy:** Used for packet capture, parsing beacon frames, and analyzing Wi-Fi traffic.
- **PyBluez:** Handles secure Bluetooth communication between the Raspberry Pi and PC.
- **Flask Framework:** Powers the lightweight web dashboard for data visualization.

3. Web Dashboard:

The dashboard, hosted locally on the Raspberry Pi, provides an intuitive interface for monitoring real-time network activity. It displays live logs, differentiates between legitimate and rogue APs, and offers visualization of honeypot interactions. The dashboard is accessible on a connected PC via Bluetooth tethering.

4. Detection Mechanism:

Secure Air employs multiple anomaly-based parameters, including **SSID duplication**, **irregular signal strength**, **spoofed MAC addresses**, and **unusual beacon intervals**, to identify rogue APs. All detections are logged and transmitted for further analysis.

5. Honeypot Deployment:

The system deploys a **fake access point** that mimics open public Wi-Fi networks, enticing malicious devices to connect. The honeypot logs all attempted connections, capturing attacker MAC addresses and behaviors for forensic analysis.

3. Experimental Environment

1. Deployment Sites:

The system was tested in diverse environments—**offices, cafés, classrooms, and public areas**—to ensure adaptability under different network conditions.

2. Test Setup:

Testing involved multiple client devices, including laptops, smartphones, and IoT devices, to simulate realistic traffic and rogue AP scenarios.

3. Evaluation Metrics:

- **Detection Accuracy:** Ability to correctly identify rogue vs. legitimate APs (achieved ~90%).
- **Latency:** Time delay between detection and dashboard update.
- **Resource Utilization:** CPU and memory consumption of the Raspberry Pi.
- **False Positives/Negatives:** Rate of incorrect classification.

4. Additional Considerations:

- **Portability:** Can operate on battery power, enabling flexible on-site deployment.
- **Cost-Effectiveness:** Designed using low-cost hardware components
- **Scalability:** Supports networking multiple Raspberry Pis for extended coverage.
- **User Accessibility:** Provides real-time insights via a browser-based dashboard with minimal setup.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

V. RESULT

Comparison Parameter	RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points	Wireless Rogue Access Point Detection Using Shadow and Pot	Detection of Rogue Access Points to Prevent Evil Twin Attacks in Wireless Network	Real-time Rogue Wireless Access Point Detection with the Raspberry Pi (Linux Journal)	Online Detection of 802.11 Traffic Using Sequential Hypothesis Testing with TCP ACK-Pairs	Secure Air (Proposed)
Year	2007	2015	2017	2015	2009	2025
Technique Used	Traffic inspection + policy enforcement	Hybrid anomaly detection + honeypot interaction	MAC/IP anomaly checks for Evil Twin	SBC-based packet sniffing with open-source tools	Statistical TCP ACK-pair timing	honeypot + Bluetooth data transfer + Flask dashboard
Hardware Requirement	Commodity Wi-Fi APs	Standard Wi-Fi cards	Any Wi-Fi client/monitor	Raspberry Pi + Wi-Fi adapter	Wired monitoring point	Raspberry Pi + Bluetooth link
Cost	Low (commodity hardware)	Moderate	Low	Very low	Low	Very low (affordable ESP + Pi)
Real-time Capability	Partial (network-side)	Yes	Yes	Yes	Yes	Yes (live dashboard over Bluetooth)
Detection Focus	Rogue APs (general)	Rogue APs + attacker profiling	Evil Twin APs	Unauthorized APs (general)	Wi-Fi traffic presence, not rogue-specific	Rogue APs, Evil Twins, spoofed MACs, open APs
Honeypot Support	No	Yes	No	Limited (manual setup)	No	Yes (captive portal honeypot, attacker logging)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

User Interface	Limited (network policy alerts)	Admin analysis, not user-friendly	Basic anomaly alerts	CLI/logs, technical	None (statistical output only)	Flask web dashboard, real-time visualization
Communication Method	Network-based	Network-based	Network-based	Ethernet/ Wi-Fi	Wired link	**Bluetooth to PC**
Deployment Complexity	Moderate (requires integration)	Moderate to high (honeypot setup)	Low	Moderate (Linux config, drivers)	Low (statistical, requires traces)	Very low (ESP + Pi + Bluetooth pairing)
Scalability	Limited to network perimeter	Scales with additional sensors	Scales in local hotspots	Scales to small sites	Scales where traffic traces are available	Scales across classrooms, cafés, offices, events
Strengths	Commodity-friendly, practical	Reduces false positives, attacker profiling	Lightweigh t, targeted ET defense	Portable, low-cost, practical	Passive, efficient, mathematically grounded	Combines honeypot + detection, Bluetooth portability, affordable, real-time UI
Limitations	Limited client-side detection	Needs careful containment	Requires baseline knowledge	Hardware instability, not user-friendly	Not specific to rogue APs	Prototype stage, requires broader field validation

Software:

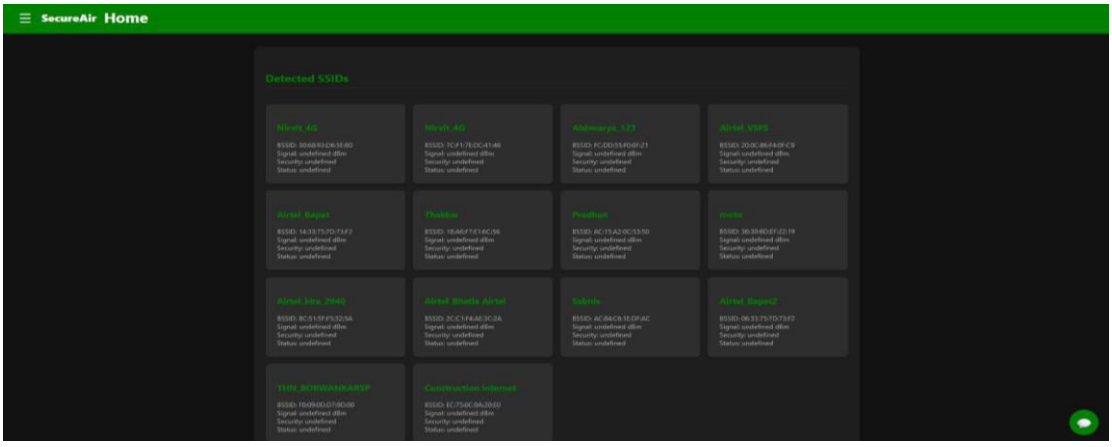


Fig.Home

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

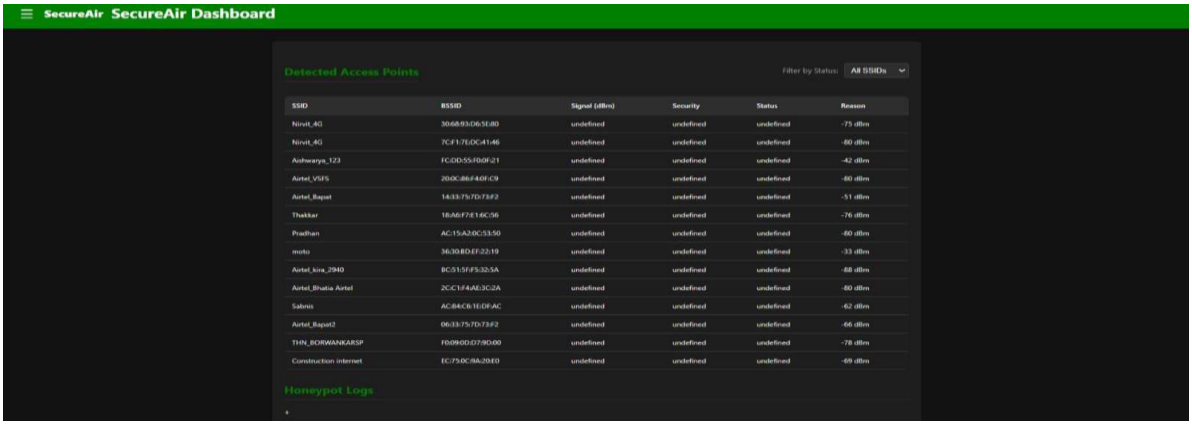


Fig . Dashboard

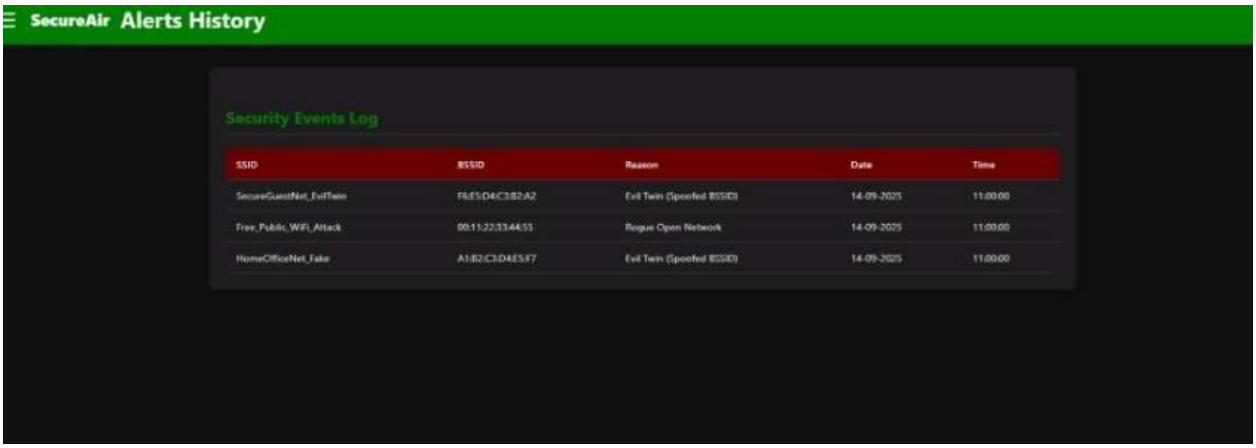


Fig . Alert History

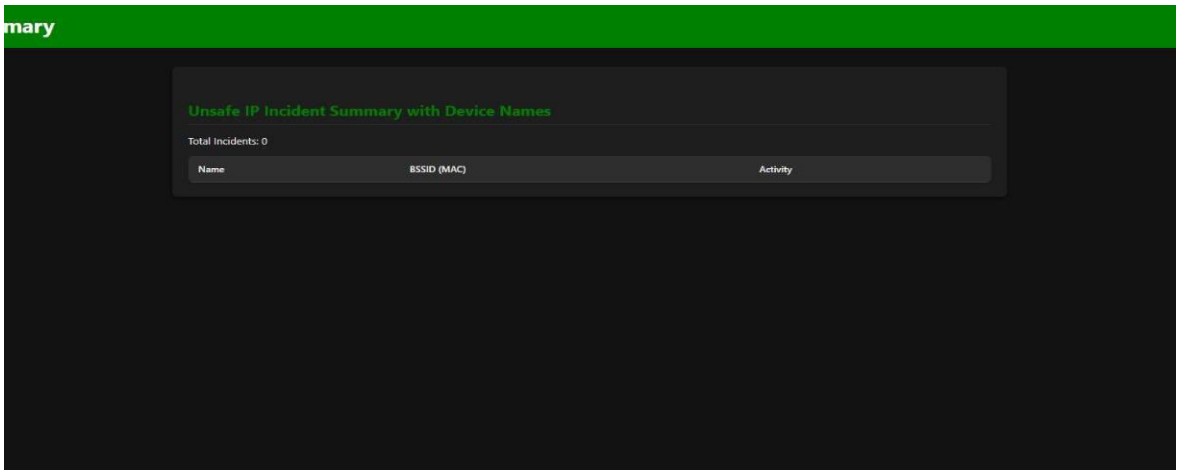


Fig .Summary

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

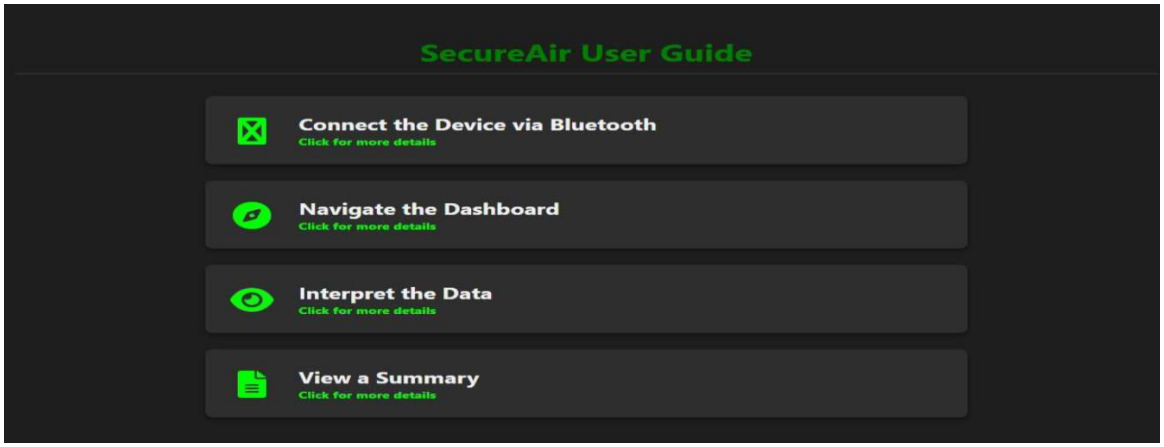


Fig . User Guide

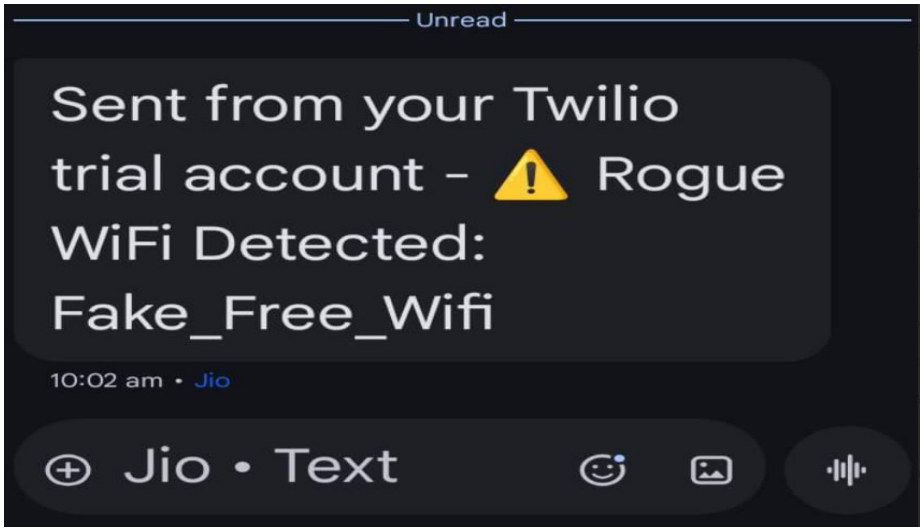


Fig Alerts sent for malicious network

Hardware:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503063|

VI. CONCLUSION

The proposed Secure Air system provides an effective, low-cost framework for rogue APs' detection and mitigation of potential security threats in wireless networks. It combines the perfect blend of portability, scalability, and efficacy by using a Raspberry Pi for detection and honeypot deployment and a dashboard with Bluetooth for visualization. The experimental testbed demonstrates real-time detection of Evil Twin attacks, duplicate SSIDs, and unauthorized APs, while malicious connection attempts are captured by the honeypot module to further strengthen the defense. This research moves forward the development of practical intrusion detection systems suitable for environments where light and moderately priced solutions are imperative. Future improvements may be made to the detection engine through the inclusion of machine learning models, increased accuracy against complex spoofing methods, and incorporation of cloud-based monitoring for wider deployments.

REFERANCES

1. Ma, L., Teymorian, A.Y., Cheng, X., & Song, M. (2007). *RAP: Protecting commodity Wi-Fi networks from rogue access points*. IEEE.
2. Agrawal, N., & Tapaswi, S. (2015). *Wireless rogue access point detection using Shadow Honeynet*. International Journal of Computer Applications.
3. Modi, V., & Parekh, C. (2017). *Detection of rogue access points to prevent Evil Twin attacks in wireless networks*. International Journal of Computer Applications.
4. Jenks, C. (2015). *Real-time rogue wireless access point detection with the Raspberry Pi*. Linux Journal.
5. Wei, W., Suh, K., Wang, B., Gu, Y., Kurose, J., Towsley, D., & Jaiswal, S. (2009). *Passive online detection of 802.11 traffic using sequential hypothesis testing with TCP ACK-pairs*. IEEE.
6. Franco, J., Aris, A., Canberk, B., & Uluagac, A.S. (2021). *A survey of honeypots and honeynets for IoT, IIoT, and CPS*.
7. Fan, W., Du, Z., Smith-Creasey, M., & Fernández, D. (2024). *HoneyDOC: An efficient honeypot architecture enabling all-round design*.
8. Wählisch, M., Schmidt, T.C., Keil, C., Schönfelder, J., & Akkaya, K. (2013). *Design, implementation, and operation of a mobile honeypot*.
9. Fan, W., Du, Z., Fernández, D., & Villagra, V.A. (2017). *Enabling an anatomic view to investigate honeypot systems: A survey*.
10. Nawrocki, M., Wählisch, M., Schmidt, T.C., Keil, C., & Schönfelder, J. (2016). *A Survey on Honeypot Software and Data Analysis*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details