AirSecure

Raham Butt, Josh George, Riya Happy, Chris Szynwald

Prof. Thomas G. Re

ABSTRACT

AirSecure is a wireless network intrusion detection system that detects various Wi-Fi based attacks. Using a Raspberry Pi 5 and machine learning algorithm (Random Forest, IEEE AWID3), it secures wireless networks through:

- 📡 **Live traffic monitoring**
- 🧠 **AI-driven detection**
- 🔐 **Secure PostgreSQL backend**
- 🌐 **Easy-to-use Next.js web app**

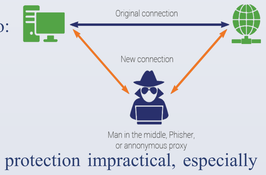
AirSecure provides fast, reliable, and affordable network protection for small and medium-sized organizations.

PROBLEM

Wireless networks face serious threats from rogue Wi-Fi access points (RAPs) — unauthorized devices disguised as legitimate networks to intercept or manipulate sensitive information. Traditional defenses frequently fail to detect these hidden threats, leaving organizations vulnerable to data leaks and credential theft.

Existing solutions fall short due to:

- 💰 **High costs**
- ☁️ **Cloud dependency**
- ⚙️ **Complex integrations**



These drawbacks make effective protection impractical, especially for smaller organizations.

AirSecure

AirSecure is a cost-effective, locally hosted solution for detecting rogue Wi-Fi access points. Utilizing a Raspberry Pi 5-based scanner operating in monitor mode and a Random Forest Classifier trained on the AWID3 dataset, it autonomously monitors and analyzes wireless traffic. With all processing and storage performed locally, AirSecure ensures data privacy, affordability, and ease of use, offering real-time detection and alerts without the need for cloud services or complex, expensive infrastructure.

AirSecure

PROJECT GOALS

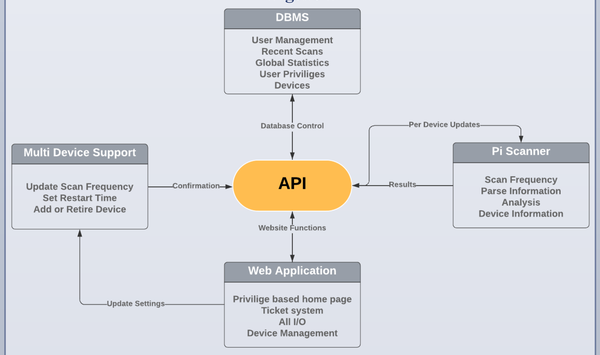
Hardware Based Protection	• Develop a hardware solution to reduce breaches from rogue devices.
Advanced Anomaly Detection	• Use machine learning algorithms for real-time identification of unauthorized access points.
Intuitive Web Interface	• Provide user-friendly web tools, personalized experiences, and detailed analytics.
Robust Data Management	• Maintain a secure database to track flagged networks, devices, and locations.
Instant Notifications	• Deliver immediate alerts within seconds of threat detection.

SYSTEM DESIGN

The diagram showcases AirSecure's streamlined system architecture, integrating key components seamlessly via a powerful central API:

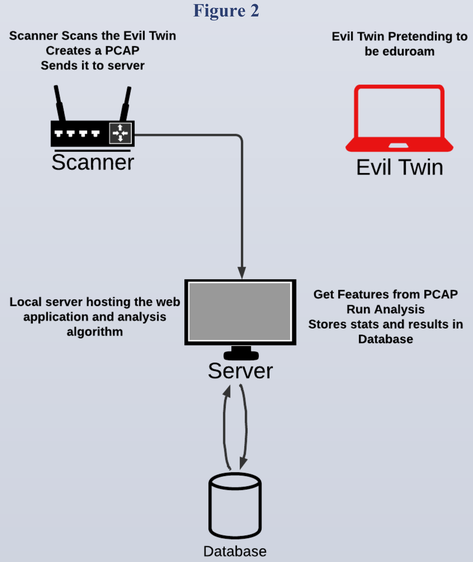
1. 🚦 **Central API:** Coordinates secure, efficient interactions among all components.
2. 🗂️ **Database (DBMS):** Organizes critical data—user profiles, scan results, statistics, user privileges, and device records.
3. 📡 **Pi Scanner:** Continuously scans wireless networks, captures live data, identifies threats, and reports detailed device insights.
4. 🌐 **Web Application:** Delivers an intuitive, privilege-based dashboard experience with robust device management and streamlined issue tracking.
5. 📱 **Multi-Device Management:** Easily controls multiple scanners—updating settings, scheduling scans, and managing device lifecycles from one place.

Figure 1



IMPLEMENTATION

Figure 2

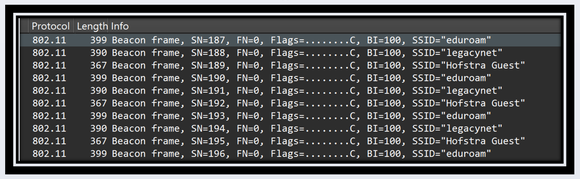


RESULTS

AirSecure was tested across multiple environments to evaluate detection speed, accuracy, and system performance. Simulated rogue access points (using duplicated SSIDs like "eduroam") were used to test the system with both live and replayed packet data.

Detection Accuracy:
Achieved 96.4% accuracy using a Random Forest Classifier trained on labeled packet features. The system-maintained precision even with multiple SSIDs sharing the same name.

Figure 3



Protocol	Length	Info
802.11	399	Beacon frame, SN=187, FN=0, Flags=.......C, BI=100, SSID="eduroam"
802.11	390	Beacon frame, SN=188, FN=0, Flags=.......C, BI=100, SSID="legacynet"
802.11	367	Beacon frame, SN=189, FN=0, Flags=.......C, BI=100, SSID="Hofstra Guest"
802.11	399	Beacon frame, SN=190, FN=0, Flags=.......C, BI=100, SSID="eduroam"
802.11	390	Beacon frame, SN=191, FN=0, Flags=.......C, BI=100, SSID="legacynet"
802.11	367	Beacon frame, SN=192, FN=0, Flags=.......C, BI=100, SSID="Hofstra Guest"
802.11	399	Beacon frame, SN=193, FN=0, Flags=.......C, BI=100, SSID="eduroam"
802.11	390	Beacon frame, SN=194, FN=0, Flags=.......C, BI=100, SSID="legacynet"
802.11	367	Beacon frame, SN=195, FN=0, Flags=.......C, BI=100, SSID="Hofstra Guest"
802.11	399	Beacon frame, SN=196, FN=0, Flags=.......C, BI=100, SSID="eduroam"

Figure 4

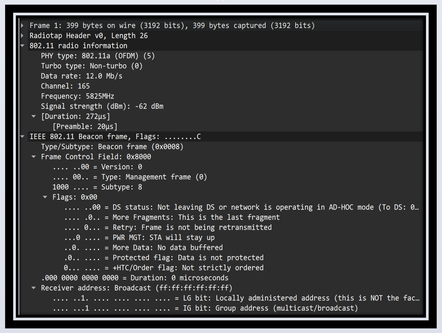
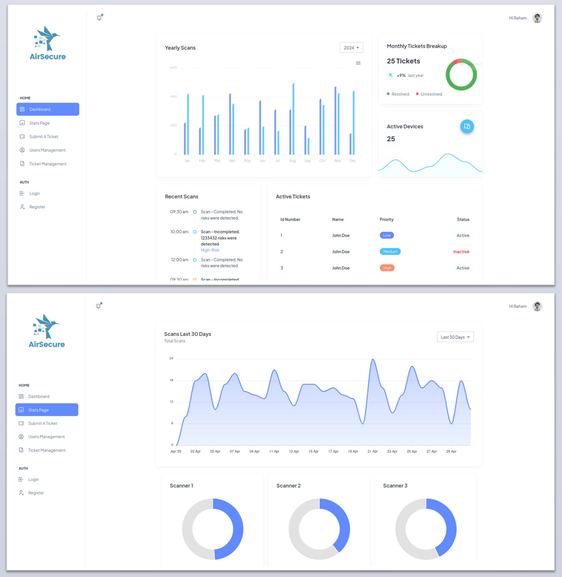


Figure 5 & 6



CONCLUSIONS

AirSecure successfully proved to be a low-cost, scalable, and highly accurate solution for rogue access point detection—built entirely on commodity hardware and open-source tools.

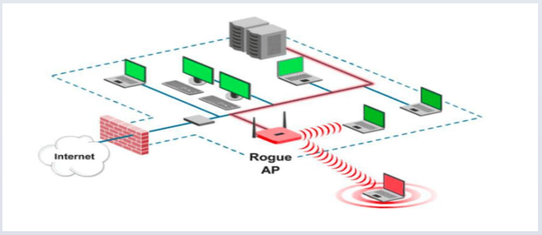
By combining:

- 💤 Passive network scanning
- ⚙️ Real-time packet parsing
- 🧠 Machine learning classification

AirSecure detected spoofed wireless networks with minimal latency and no enterprise infrastructure.
The system's integration with PostgreSQL and a custom Next.js dashboard gave administrators real-time visibility, intuitive controls, and instant alerts—making wireless threat management simple and effective.

🚀 Future Work

- 🌐 Deploying AirSecure in enterprise environments with roaming clients
- 🧬 Enhancing detection with deep learning for sequence-based packet analysis
- 🔒 Automating RADIUS-based responses to isolate rogue devices instantly



REFERENCES

- **AWID3 Dataset:** https://icsdweb.aegean.gr/awid/download-dataset
- **Scapy Documentation:** https://scapy.readthedocs.io
  Next.js Documentation: https://nextjs.org/docs
  PostgreSQL Documentation: https://www.postgresql.org/docs
- **Random Forest – scikit-learn:** https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html
- **Radiotap Reference:** https://www.radiotap.org

ACKNOWLEDGEMENT

- We sincerely thank **Prof. Thomas G. Re** for his continuous guidance, mentorship, and technical feedback throughout the development of AirSecure.
- We are grateful to **Dr. Doboli** for organizing the senior design program and supporting us at every step of the process.
- Special thanks to **Dr. Fu** for his insights and guidance on the security aspects that helped shape key components of this project.
- We truly appreciate **Alex** for assisting with hardware procurement and providing backup equipment when shipments were delayed.
- Lastly, we thank Hofstra University for offering the resources and environment that enabled this project to succeed.