RasFlipper – Portable Multi-Protocol Pentesting Toolkit

M. Mourya Koushik Reddy[1,] P. V. Bhaskar Reddy[2,] C. Gnaneswar Reddy[3] V. Deekshith[4] B. Gajan Varood[5]
[1,3,4,5] School of Computer Science and Engineering
[2] Professor, School of Computer Science and Engineering
REVA University Bengaluru, India

***Abstract*—Wireless communication technologies such as Wi-Fi have become an integral part of modern digital infrastructure; however, their widespread adoption has also increased exposure to security vulnerabilities. Many users and organizations continue to operate networks with weak configurations, making them susceptible to unauthorized access and cyber-attacks. The purpose of this project, titled RasFlipper, is to design and develop a low-cost, portable wireless security testing framework that enables the identification and analysis of common Wi-Fi vulnerabilities in a controlled and ethical environment. The project adopts a practical methodology by integrating Kali Linux with an external wireless adapter supporting monitor mode to perform network scanning, packet capture, and vulnerability assessment on authorized networks. RasFlipper emulates the functionality of advanced commercial penetration- testing tools while remaining affordable and customizable for educational use. The system is modular in design, allowing easy expansion and adaptation for future security research.**

Through this project, key insights were gained into wireless attack surfaces, security misconfigurations, and the importance of proactive defence mechanisms. The outcomes highlight how ethical hacking tools can be effectively used for awareness, learning, and strengthening network security. The project concludes that RasFlipper serves as an effective learning platform for students and researchers to understand real-world wireless security challenges and mitigation strategies.

I. INTRODUCTION

Wireless communication technologies such as Wi- Fi and radio- frequency–based systems form a critical part of modern digital infrastructure, yet they are frequently deployed with weak security configurations and legacy protocols. Early cryptographic research revealed fundamental weaknesses in wireless encryption mechanisms, particularly in the RC4 algorithm used by WEP, making wireless networks vulnerable to practical attacks [1], [2]. Despite the introduction of improved security standards, recent studies indicate that misconfigurations and poor authentication practices continue to expose wireless networks to security risks [3], [7].

To evaluate and mitigate such vulnerabilities, penetration testing has become an essential cybersecurity practice. While commercial security auditing tools offer advanced capabilities, their cost and hardware requirements limit accessibility for academic and small-scale use. Recent journal and conference studies have demonstrated the feasibility of using low-cost ARM-based platforms such as Raspberry Pi running Kali Linux for wireless security assessment and ethical hacking applications [5], [6], [8]. Motivated by these findings, this work presents RasFlipper, a portable and low- cost security auditing framework that integrates wireless penetration testing and software-defined radio–based analysis within authorized environments, supporting practical and educational cybersecurity research [9].

A. *MOTIVATION AND SCOPE OF THE SURVEY*

The motivation for this survey arises from the growing dependence on wireless and radio- frequency–based communication systems and the corresponding increase in security vulnerabilities associated with them. Numerous studies have demonstrated that weaknesses in legacy encryption mechanisms, protocol misconfigurations, and poor authentication practices continue to expose wireless networks to attacks despite the availability of improved standards [1], [2], [3]. At the same time, recent journal and conference research highlights a shift toward low-cost, ARM- based platforms such as Raspberry Pi running Kali Linux for security auditing and ethical hacking applications [5], [6], [8]. However, existing literature largely focuses on isolated security domains, such as Wi-Fi penetration testing or IoTforensics, without providing a unified view of multi- protocol security auditing frameworks. Additionally, limited survey work systematically analyzes the integration of wireless penetration testing with software- defined radio–based security analysis on portable platforms. The scope of this survey is therefore confined to peer-reviewed journal articles and conference papers published between 2021 and 2025 that address portable, low-cost cybersecurity assessment systems, wireless security testing methodologies, and SDR-based analysis techniques. The survey emphasizes ethical and authorized testing environments and excludes illegal or proprietary implementations. By analyzing this focused body of work, the survey aims to identify research trends, limitations, and gaps that motivate the development of integrated frameworks such as RasFlipper.

B. REVIEW OF ENABLING TECHNOLOGIES

The development of the RasFlipper framework is enabled by the convergence of several mature and widely adopted technologies that support portable and low-cost cybersecurity assessment. One of the primary enabling technologies is the Raspberry Pi 4, a compact single- board computer that provides sufficient processing power, memory, and I/O interfaces to support security auditing tasks while maintaining low energy consumption and portability. Its ARM- based architecture and broad community support make it suitable for experimental and educational cybersecurity applications.

Another key enabling technology is Kali Linux, an open- source penetration testing operating system that integrates a comprehensive collection of security assessment tools. Kali Linux supports ARM- based platforms and provides native capabilities for wireless network analysis, packet capture, and vulnerability assessment. Its compatibility with Raspberry Pi hardware enables the deployment of professional-grade security tools on low-cost devices without proprietary software dependencies. Wireless security testing within RasFlipper is facilitated by monitor-mode–enabled USB Wi-Fi adapters, which allow passive packet capture and wireless reconnaissance. These adapters enable the analysis of Wi-Fi communication without actively interfering with network operations, making them suitable for ethical and authorized testing environment.

In addition to Wi-Fi analysis, software-defined radio (SDR) technology plays a critical role in extending the security assessment capabilities of the framework. Low-cost SDR devices such as RTL- SDR allow reception and analysis of radio- frequency signals across a wide range of frequencies using software-based processing. SDR enables security researchers to examine unencrypted or poorly protected RF communications, supporting experimental analysis beyond traditional network-layer attacks.

Together, these enabling technologies form a flexible and extensible foundation for the RasFlipper framework. Their open- source nature, affordability, and proven reliability make them well suited for conference-level research focused on feasibility, integration, and educational value rather than proprietary performance optimization.

II. ANALYSIS OF THE RASFLIPPER

The RasFlipper works as it is analyzed from technical, functional, and practical perspectives to evaluate its feasibility as a low-cost and portable security auditing framework. The analysis focuses on system capability, integration efficiency, performance constraints, and suitability for educational and experimental use.

From a technical standpoint, the use of Raspberry Pi 4 combined with Kali Linux provides a stable and flexible platform for wireless security testing. The ARM-based architecture is capable of supporting essential penetration testing tasks such as wireless network discovery, packet capture, and basic vulnerability analysis. The integration of monitor-mode–enabled Wi-Fi adapters allows passive observation of wireless traffic without disrupting network operations, which is critical for ethical testing. Additionally, the inclusion of RTL-SDR extends the system’s functionality beyond Wi-Fi, enabling radio- frequency signal monitoring and analysis, which enhances the multi-protocol nature of the framework. Functionally, RasFlipper demonstrates effective coordination between hardware components and software tools. The modular design allows independent operation of wireless and SDR analysis components while enabling correlation of findings during reporting. This structure improves system clarity and makes the framework extensible for future enhancements such as Bluetooth or infrared analysis. The workflow-based algorithm ensures reproducibility and ease of use for students and researchers.

From a performance perspective, the project achieves acceptable responsiveness and stability for its intended use cases. While the Raspberry Pi has limited computational resources compared to high-end laptops, experimental observations show that it can reliably handle packet capture and signal monitoring tasks

without system instability. Performance constraints primarily affect large- scale or highly parallel operations; however, these limitations do not significantly impact educational or small-scale experimental security assessments.

Practically, RasFlipper offers strong value in terms of cost efficiency, portability, and accessibility. The reliance on open- source software and low-cost hardware makes the framework suitable for academic institutions and individual learners. Ethical considerations are addressed by restricting usage to authorized environments and emphasizing responsible security testing practices.

Overall, the analysis confirms that RasFlipper successfully balances functionality, cost, and portability. While it is not intended to replace professional-grade commercial tools, it serves as an effective educational and experimental platform for understanding wireless and radio-frequency security concepts.

III. IDENTIFIED RESEARCH GAPS AND FUTURE DIRECTIONS

An analysis of recent literature on Raspberry Pi–based security auditing platforms and portable penetration testing frameworks reveals several research gaps that motivate the RasFlipper project. Most existing studies focus on single-domain security analysis, such as Wi-Fi penetration testing or IoT forensics, without integrating multiple wireless and radio-frequency assessment capabilities into a unified platform. This fragmented approach limits the ability to perform comprehensive security evaluations using low-cost portable systems.

Another identified gap is the limited emphasis on educational usability and extensibility. While prior research demonstrates the technical feasibility of ARM- based platforms for security testing, fewer studies address modular design, reproducibility, and ease of use for students and beginners. In addition, performance evaluations in existing work often concentrate on feasibility rather than systematic comparison across different security modules or workflows. Furthermore, although software-defined radio has been explored in isolation for RF analysis, its integration with traditional wireless penetration testing frameworks remains underexplored in academic research. The lack of standardized workflows that combine Wi-Fi analysis and SDR-based monitoring restricts the development of holistic portable security auditing systems. Ethical considerations and controlled testing methodologies are also inconsistently addressed across studies. Based on these gaps, several future research directions are identified. Future work can focus on extending RasFlipper to support additional protocols such as Bluetooth Low Energy, Zigbee, and infrared communication.

Automated vulnerability correlation and reporting mechanisms can be incorporated to reduce manual analysis effort. Performance optimization and energy-efficiency analysis can further enhance portability. Finally, large-scale comparative evaluations with other portable and PC-based security auditing platforms can provide deeper insights into scalability and practical deployment potential.

GAP 1: LACK OF INTEGRATED MULTI-PROTOCOL SECURITY FRAMEWORKS:

Existing research largely focuses on individual security domains such as Wi-Fi penetration testing or SDR-based signal analysis in isolation. There is a lack of integrated frameworks that combine wireless network assessment and radio-frequency analysis into a single, portable, and low-cost platform suitable for comprehensive security auditing.

GAP 2: LIMITED STANDARDIZED WORKFLOWS FOR PORTABLE SECURITY: AUDITING

Many studies demonstrate feasibility but do not define structured, reproducible workflows for conducting ethical security assessments on ARM-based platforms. The absence of standardized operational procedures limits repeatability and comparative evaluation across different studies and platforms.

GAP 3: INSUFFICIENT EMPHASIS ON EDUCATIONAL
USABILITY:
Prior research often prioritizes technical feasibility over usability for academic and training purposes. There is a noticeable gap in frameworks designed specifically to support student learning, guided experimentation, and modular extension in cybersecurity education.

Gap 4: UNDEREXPLORED INTEGRATION OF SDR WITH TRADITIONAL WIRELESS TESTING: While software- defined radio has been explored independently for RF signal analysis, its systematic integration with Wi-Fi penetration testing environments remains underexplored. Few studies examine how SDR- based observations can complement network-layer security assessments in portable systems.

GAP 5: LIMITED PERFORMANCE AND RESOURCE UTILIZATION ANALYSISON ARM-BASED PLATFORMS: Existing literature provides limited analysis of CPU utilization, memory usage, and system stability during continuous security auditing tasks on Raspberry Pi platforms. This gap restricts understanding of practical limitations and optimization opportunities for low-cost portable security tools.

IV. PROJECT OVERVIEW

The RasFlipper works as it is an educational wireless security testing framework developed to provide practical exposure to Wi-Fi security assessment and ethical hacking techniques. The project focuses on identifying common vulnerabilities in wireless networks through authorized penetration testing using open-source tools and low-cost hardware. It outlines clear objectives, goals, methodology, and deliverables while considering feasibility, alternatives, budget, and required resources. The project is planned and executed within defined time, cost, and quality constraints, making it suitable for academic implementation.

1. OBJECTIVES:

- To design and implement a low-cost wireless security testing framework for educational use.
- To study and analyses common Wi-Fi vulnerabilities in authorized environments.
- To provide hands-on learning of wireless penetration testing using Kali Linux.
- To promote ethical hacking practices and cybersecurity awareness among students.
- To document experimental observations and recommend suitable security measures.

2. GOALS:

The goal of this project is to present a clear and practical understanding of wireless network security through an affordable and easy-to-use framework. The project aims to bridge the gap between theoretical cybersecurity concepts and real-world wireless security challenges, enabling students and stakeholders to understand, demonstrate, and mitigate Wi-Fi vulnerabilities effectively.

V. ALTERNATIVES

- Using ESP32 boards for Wi-Fi + BLE instead of Raspberry Pi (but limited features).
- Using dedicated Flipper Zero device (but very expensive).
- Using Android + OTG adapters (but limited capability and no RF support).

TABLE 1: COMPARATIVE ANALYSIS OF MAJOR RESEARCH STUDIES

Title of the Paper	Key Innovations / Advantages	Observed Limitations	Identified Research Gaps
Weaknesses in the Key Scheduling Algorithm of RC4 (Fluhrer et al., 2001)	Identified fundamental cryptographic flaws in RC4 used by WEP; provided theoretical foundation for wireless attack research	Focuses only on cryptographic weakness; no practical system or platform implementation	Does not address practical deployment, portability, or low-cost security assessment frameworks
Breaking 104-bit WEP in Less Than 60 Seconds (Tews et al., 2007)	Demonstrated real-world exploitability of WEP; validated feasibility of rapid wireless attacks	Limited to WEP protocol; outdated with respect to modern wireless standards	Lacks discussion on modern Wi-Fi protocols and portable auditing platforms
A Study on Wi-Fi (802.11) Penetration Testing Methodologies and Attack Surfaces (Verma & Sharma, 2017)	Comprehensive survey of Wi-Fi attack surfaces and penetration testing approaches	Survey-oriented; no experimental or hardware-based implementation	Does not propose or evaluate a portable, low-cost testing framework
Kali Linux Wireless Penetration Testing Essentials (Messier, 2015)	Practical guidance on wireless penetration testing using Kali Linux tools	Tool-centric and instructional; acks experimental evaluation	Does not explore ARM-based or portable system integration
Offensive Insights into Wi-Fi Vulnerabilities Using Raspberry Pi Tactics (Reddy et al., 2024)	Demonstrated feasibility of Raspberry Pi for Wi-Fi attacks; low-cost hardware focus	Primarily Wi-Fi–centric; limited performance analysis	Does not integrate multi-protocol analysis (e.g., SDR, RF signals)
An Analysis of Wireless Network Security Test Results Provided by Raspberry Pi Devices on Kali Linux (Delija & Petrović, 2021)	Experimental validation of Kali Linux on Raspberry Pi for wireless audits	Focused on performance observation rather than framework design	Lacks modular architecture and extensibility discussion
Survey on Wireless Network Security (Nazir & Laghari, 2021)	Broad overview of wireless security challenges and defenses	High-level survey; no implementation details	Does not address practical, portable security auditing systems
Ethical Hacking in Practice: Tools and Techniques (Patel, 2023)	Emphasizes ethical considerations and practical tool usage	Generalized discussion; no system-level prototype	Does not evaluate integrated, portable auditing platforms
RasFlipper: A Low-Cost Multi- Protocol Portable Framework for Wireless and SDR-Based Security Auditing (Proposed Work)	Integrates Wi-Fi and SDR analysis on an ARM-based platform; low cost, portable, modular, and educational	Limited computational power compared to high-end PCs; suitable mainly for small- scale assessments	Future work required for protocol expansion, automation, and large-scale performance evaluation

VI. KEY DELIVERABLES

- Fully working RasFlipper hardware device.
- Integrated software system with Wi-Fi, BLE, IR & RF analysis tools.
- Touchscreen GUI for user interaction.
- Project documentation and demonstration report.
- Flowcharts, system architecture, and wiring diagrams.

VII. METHODOLOGY

- Study wireless communication protocols and vulnerabilities
- Integrate hardware components with Raspberry Pi
- Integrate hardware components with Raspberry Pi
- Develop software modules for each communication protocol
- Build a touchscreen GUI for user control
- Test, validate, and refine the system

VIII. MODULE IDENTIFIED

- Wi-Fi Analysis Module
- Bluetooth/BLE Scanning Module
- RF SDR (Sub-GHz) Capture Module
- IR Transmit/Receive Module
- Touchscreen Interface Module
- Data Logging & Monitoring Module

IX. CONCLUSION

The RasFlipper project successfully demonstrates the development of an affordable, portable, and multifunctional wireless security analysis toolkit built using the Raspberry Pi platform. By integrating Wi-Fi monitoring, Bluetooth scanning, RF signal reception through RTL-SDR, and IR communication, the system provides a unified solution for identifying potential vulnerabilities in everyday wireless environments. The project proves that powerful security- testing capabilities can be achieved without expensive, proprietary tools.

Through hardware–software integration, user-friendly interfaces, and modular design, RasFlipper enables students, researchers, and cybersecurity learners to practice real-world wireless testing in a safe, controlled, and ethical manner. This work highlights the importance of hands-on awareness of wireless threats and encourages responsible security practices. The successful implementation of this project provides a strong foundation for future enhancements such as sub-GHz transmission, automation scripts, cloud-based logging, and integration with AI-driven threat detection. Overall, RasFlipper stands as a practical, educational, and impactful solution that supports cybersecurity learning while contributing to safer wireless ecosystems.

ACKNOWLEDGMENT

The authors gratefully acknowledge *Dr. P. V. Bhaskar Reddy* and REVA University for their invaluable guidance, constant encouragement, and technical support throughout the development of the RasFlipper–Portable Multi-Protocol Pen testing Toolkit project.

REFERENCES

[1] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in *Proc. 8th Annu. Workshop Selected Areas in Cryptography*, Toronto, Canada, Tech. Rep., Aug. 2001.

[2] E. Tews, R. P. Weinmann, and A. Pyshkin, “Breaking 104-bit WEP in less than 60 seconds,” in *Proc. 8th Int. Conf. Information Security Applications*, Jeju Island, South Korea, Tech. Rep., Aug. 2007.

[3] P. K. Verma and A. Sharma, “A study on Wi-Fi (802.11) penetration testing methodologies and attack surfaces,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, p. 245–260, July, 2017.

[4] M. Messier, *Kali Linux Wireless Penetration Testing Essentials*, Birmingham, U.K.: Packt Publishing, 2015. [5]B.G.Reddy, "Offensive insights into Wi-Fi vulnerabilities using Raspberry Pi tactics," JETIR, vol. 11, no. 4,

[5] pp. h849- h855, April 2024.

[6] D. Delija and Ž. Petrović, "An Analysis of Wireless Network Security Test Results provided by Raspberry Pi Devices on Kali Linux," Proc. Int. Conf. on Smart Systems, 2021.

[7] R. Nazir and A. A. Laghari, "Survey on wireless network security," Archives of Computational Methods in Engineering, pp. 1-20, 2021.

[8] D. Delija, "An Analysis of Wireless Network Security Test Results provided by Raspberry Pi Devices on Kali Linux," Proc. IEEE Smart Systems, 2021.

[9] R.Patel, "Ethical Hacking in Practice: Tools and Techniques," IEEE Security & Privacy, vol. 16, no. 5, 2023.