International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Literature Survey on Portable Raspberry PI-Based LAN Defense System.

EDWIN DOMINIC
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
edwindominic7878@gmail.com

ABHINANDH P NARAYAN
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
abhinandhpnarayan@gmail.com

ELIZEBATH JESLIN
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
elizebathjeslin75@gmail.com

MOHAMMED ADNAN
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
zaynadnan014@gmail.com

MAFNITHA KK
Assistant Professor
Department of Computer Science and Engineering (Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
mafnitha@vjec.ac.in

***Abstract*—The rapid growth of connected devices in homes, offices, and academic environments has expanded the risk surface for cyberattacks, often leaving small networks unprotected against sophisticated threats. To address this gap, DefenderPi is proposed as a lightweight, portable, and cost-effective security appliance built on Raspberry Pi 4. Operating in Wi-Fi Access Point mode, DefenderPi functions as an inline security gateway that not only routes traffic but also inspects, filters, and mitigates malicious activity in real time. Unlike conventional monitoring tools that are limited to passive logging, DefenderPi integrates firewall enforcement, intrusion detection, DNS anomaly analysis, phishing and malware protection, and honeypot-based deception within a fully automated system. The solution further enhances usability through a Flask-based dashboard for live threat visualization and instant alerting via email or Telegram, requiring no advanced technical expertise from end users. With its plug-and-play design, AI-driven anomaly detection modules, and modular add-on capabilities, DefenderPi demonstrates a practical and scalable approach to democratizing network defense, making enterprise-grade protection feasible for small organizations, IoT ecosystems, and personal networks.**

I. INTRODUCTION

The rapid growth of IoT and small-scale networks has increased vulnerability to cyberattacks such as ARP spoofing, DDoS, malware, and unauthorized access. Traditional IDS and firewall solutions are often costly and resource-intensive, making them impractical for small networks.

Raspberry Pi has emerged as a low-cost, portable platform for implementing lightweight security solutions. Approaches include machine learning-based IDS, deep learning models, flow-based traffic analysis, and honeypots to detect known and zero-day attacks. Real-time alerting, anomaly detection, and distributed deployment enhance network monitoring while minimizing computational overhead.

The DefenderPi project builds on these concepts by combining ARP spoofing detection, rogue DHCP detection, port scan monitoring, DNS anomaly detection, honeypot logging, and real-time alerts into a single portable system. Its modular, low-cost design makes it suitable for IoT, home, and small office networks, demonstrating that effective cybersecurity can be achieved without expensive enterprise-grade hardware.

II. LITERATURE SURVEY

[1] This paper presents a Raspberry Pi-based Intrusion Detection System (IDS) integrated with the Telegram API for real-time alerts. Designed for small-scale and resource-constrained networks, it addresses limitations of traditional IDSs such as slow response, high false positives, and complex setup.

The system monitors network traffic using tools like `tcpdump`, with data preprocessing and feature selection. Detection uses a hybrid machine learning approach:

- Random Forest (supervised) for known attacks
- K-Means clustering (unsupervised) for anomalies and zero-day threats

Suspicious activity triggers instant Telegram notifications for rapid response.

Performance highlights include 96.5% detection accuracy, 1.9% false-positive rate, and 110 ms reaction time. The system reliably detects attacks such as DDoS, malware, insider threats, and phishing. Its design allows scalable deployment with multiple Raspberry Pi units and remains cost-effective compared to enterprise IDS solutions. Limitations include dependence on Telegram and constrained resources under

Reference	Description	Advantages	Disadvantages
[1]	• Raspberry Pi-based IDS with Telegram alerts. • Uses Random Forest + K-Means for hybrid detection. • Focuses on scalability and low cost.	• High accuracy (96.5%), low false positives. • Real-time alerts via Telegram.	• Depends on Telegram for notifications. • Limited resources in complex networks.
[2]	• Raspberry Pi-based IDS for IoT. • Lightweight anomaly detection. • Monitors device behavior and traffic.	• Portable, affordable. • Good detection with low false positives.	• Struggles under heavy traffic. • Requires frequent model updates.
[3]	• Flow-based IDS for IoT. • Uses IPFIX data collection. • Random Forest classifiers (binary + multi-class).	• 95% accuracy for binary detection. • Adaptable across datasets.	• Multi-class weaker for DDoS/Theft. • Training is resource-heavy.
[4]	• PIPOT Raspberry Pi honeypot. • Simulates SSH, FTP, HTTP, etc. • Distributed trust dissemination.	• Low cost, portable. • Detects various attacks with logs + alerts.	• Needs more advanced analytics. • Limited against evasive attacks.
[5]	• Deep Learning-based NIDS. • Evaluates SNN, DNN, CNN, Attention. • Tested on NSL-KDD, Kyoto, UNSW-NB15.	• Very high accuracy (up to 99.9%). • Detects known + unknown intrusions.	• High computational demand. • Requires large datasets.
[6]	• RF-based IDS for SCADA/ICS. • Feature selection + ensemble trees. • Real-time attack classification.	• High accuracy (98.4%+). • Low false positives.	• Needs hybrid/deep learning for advanced threats. • Limited zero-day adaptability.
[7]	• Raspberry Pi with Kali Linux for Wi-Fi testing. • Uses Aircrack, Kismet, Reaver, Wireshark. • Simulates real-world Wi-Fi attacks.	• Portable, low-cost auditing device. • Practical recommendations for Wi-Fi security.	• Limited by Pi hardware. • Focus only on Wi-Fi vulnerabilities.
[8]	• RF-based supervised NIDS for IoT. • Uses KDDCUP99 and NSL-KDD datasets. • Feature reduction from 41 to 10.	• 99.9% accuracy, fast execution. • Low false positives.	• Evaluated on datasets only. • Needs real-world deployment.
[9]	• Raspberry Pi ARP spoof detection + mitigation. • Real-time monitoring of ARP tables. • Auto-block malicious MACs.	• Accurate detection, quick mitigation. • Portable and affordable.	• Focused only on ARP spoofing. • Lacks ML integration for accuracy.
[10]	• Snort vs Suricata IDS on Raspberry Pi. • Evaluates SYN, Smurf, UDP flood. • Compares accuracy, CPU, RAM usage.	• Snort = lightweight, efficient. • Suricata = scalable, multi-threaded.	• Resource constraints on Pi. • Suricata overheats under load.
[11]	• Snort-based IDS/IPS improvements. • Uses SnortSam, Snort-inline, BASE. • Rule optimization for efficiency.	• Low-cost, flexible. • Active prevention possible.	• Limited against zero-day threats. • Needs ML integration.

Reference	Description	Advantages	Disadvantages
[12]	• Raspberry Pi-based firewall for SOHO. • Uses iptables/netfilter. • Provides NAT, routing, port blocking.	• Affordable SOHO firewall. • Reliable under moderate load.	• Not suited for enterprise traffic. • Lacks IDS/IPS integration.
[13]	• RPiDS: Raspberry Pi IDS framework. • Uses libpcap + anomaly detection. • Includes simple web interface.	• Portable, low power. • Good for education & labs.	• Limited scalability. • Static rules → poor zero-day detection.
[14]	• Pi-IDS comparative study. • Runs Snort & Suricata on Raspberry Pi. • Evaluates port scan, SYN, UDP, ICMP floods.	• Snort = accurate + lightweight. • Suricata = higher throughput.	• Bottlenecks under heavy load. • Limited scalability.
[15]	• Multifunctional Raspberry Pi platform. • Combines IDS, honeypot, packet analyzer. • Captures forensic logs for analysis.	• Comprehensive in one device. • Good for SOHO & research.	• High load reduces performance. • Vulnerable to evasion techniques.

complex traffic. Future work involves exploring additional machine learning models, integrating threat intelligence, and enhancing continuous monitoring.

Overall, this work demonstrates a practical, low-cost, and efficient IDS combining edge computing, machine learning, and real-time alerting for proactive cyber defense.

[2] This paper proposes a Raspberry Pi-based Intrusion Detection System (IDS) to secure IoT environments cost-effectively and efficiently. With the rapid growth of IoT devices, which often lack strong security, the system aims to protect against threats like botnets, DDoS, and data exfiltration.

The design combines packet capture (`tcpdump`) and lightweight traffic analysis to monitor both device behavior and network anomalies. A machine learning-based anomaly detection approach enables identification of novel threats. Feature extraction considers traffic volume, protocol usage, and abnormal access patterns.

Evaluation shows high detection accuracy with minimal false positives, demonstrating the system's capability to handle real-world IoT attacks without overloading the Raspberry Pi hardware. Key advantages include portability, affordability, and scalability, allowing deployment of multiple units across networks. Limitations involve resource constraints under heavy traffic and the need for continuous model updates.

Future work includes incorporating advanced AI, threat intelligence sharing, and extending support for heterogeneous IoT devices. Overall, the study illustrates that Raspberry Pi-based IDS provides a practical, lightweight, and scalable security solution for IoT environments.

[3] This paper presents a flow-based Intrusion Detection System (IDS) optimized for IoT environments using Raspberry Pi. With the growing number of IoT devices and inherent vulnerabilities, the system uses the IP Flow Information Export (IPFIX) protocol to collect traffic data and applies machine learning for attack detection.

The architecture includes two models:

- *Multi-class classifier* for differentiating attack types
- *Binary classifier* for separating benign and malicious traffic

Both models use `Random Forest` for robustness and resistance to overfitting. Techniques such as lazy loading, oversampling/undersampling, and configurable parameters allow efficient operation on Raspberry Pi with limited resources.

Evaluation on CIC-IDS2017, CIDDS-001, NF-BoT-IoT, and NF-ToN-IoT datasets shows:

- Multi-class classification macro-accuracy: 77%, lower for DDoS and Theft classes
- Binary classification accuracy: 95%, reliably separating benign and malicious traffic
- Random Forest outperforms SVC, KNN, and XGBoost in both accuracy and efficiency

The system demonstrates flexibility and scalability across IoT scenarios and datasets. Resource tests confirm Raspberry Pi can handle IDS and data collection without major performance degradation, though model training is resource-intensive. The prototype also serves as an educational tool, illustrating IoT security and data flow analysis. The study concludes that flow-based IDS on Raspberry Pi offers a practical, affordable solution for IoT security, despite hardware and dataset limitations.

[4] This paper introduces PIPOT, a cost-effective Raspberry Pi-based honeypot framework for intrusion detection, attacker monitoring, and real-time alerts. Developed using Python, it emulates vulnerable services such as SSH, Telnet, FTP, HTTP, and VNC to lure attackers and log their activities, including IP addresses, commands, and exploited ports. Alerts are sent instantly via email or on-screen notifications.

PIPOT incorporates distributed trust and reputation management by deploying multiple Raspberry Pi honeypots across

network nodes using four trust dissemination strategies: Neighbor-based (NTD), Honeypot Neighbor-based (HNTD), Cluster-based (CTD), and Cluster Neighbor-based (CNTD). The system uses tools like Cowrie, Honeyd, and Dionaea for service simulation and log analysis to identify reconnaissance attempts, brute-force attacks, DoS activities, and port scans.

Key contributions include:

- Low-cost, portable, and stealthy honeypot deployment
- Real-time monitoring with automated alerts
- Detailed log analysis for attacker behavior and vulnerabilities
- Scalable distributed deployment for broader visibility
- Lightweight design suitable for small businesses, IoT, and personal networks

Experimental results demonstrate effective detection of diverse attack types with minimal resource usage. PIPOT enhances network defense capabilities in small-scale and IoT environments. Future improvements include advanced analytics, centralized dashboards, and automated incident response to handle evolving threats.

[5] This paper presents a deep learning-based Network Intrusion Detection System (NIDS) for accurately detecting and classifying cyberattacks. Traditional rule-based IDSs suffer from high false positives, slow responses, and limited adaptability. The authors propose a flexible framework using four deep learning architectures — Shallow Neural Network (SNN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), and attention-based models — evaluated on NSL-KDD, Kyoto 2006, and UNSW-NB15 datasets.

The methodology includes data preprocessing, feature selection, and label encoding. Relevant traffic features such as packet size, protocol usage, flow duration, and connection states are extracted to improve accuracy and reduce computational overhead. Each model is trained to detect both known and previously unseen intrusions. Key features of each architecture:

- **SNN** — lightweight, fast training, suitable for real-time detection.
- **DNN** — multi-layered, captures complex patterns in large datasets.
- **CNN** — spatial feature extraction to identify sophisticated attack signatures.
- **Attention Model** — emphasizes important features, improving classification accuracy.

Evaluation results:

- NSL-KDD: attention-based and SNN achieved 99.9% accuracy.
- Kyoto 2006: attention model reached 98.45% testing accuracy.
- UNSW-NB15: CNN achieved 93.46% testing accuracy.

The framework detects a wide range of attacks including DoS, probes, malware injection, brute-force, and APTs, while maintaining computational efficiency. Key contributions include a flexible NIDS supporting multiple deep learning models, high detection accuracy with low false positives, and scalability for large-scale network traffic. Future enhancements involve real-time detection pipelines, explainable AI, and privacy-preserving federated learning for distributed networks.

[6] This paper proposes a network intrusion detection method for securing power system communication networks using the Random Forest (RF) algorithm. Power systems, relying on SCADA and ICS, exchange large volumes of sensitive data, making them vulnerable to network attacks. Traditional IDS solutions often suffer from low detection accuracy, high false positives, and limited adaptability. The authors develop a model combining statistical traffic analysis with machine learning-based classification to detect both known and unknown intrusions.

The methodology involves three stages: data preprocessing, feature selection, and classification. Network traffic parameters such as packet size, protocol type, session duration, and flow patterns are analyzed to detect anomalies. Feature selection reduces computational complexity while maintaining accuracy. The RF algorithm builds an ensemble of decision trees, with final classification determined via majority voting, improving robustness and reliability.

Evaluation on benchmark and real-world power system traffic demonstrates:

- High detection accuracy exceeding 98.4
- Low false-positive rate, ensuring system stability.
- Effective detection of known attacks and zero-day anomalies.
- Strong adaptability to evolving intrusion patterns.

The approach provides a scalable, efficient, and reliable IDS suitable for critical infrastructure, offering real-time threat detection without heavy computational demands. Future work includes integrating deep learning, developing hybrid frameworks, and implementing automated response mechanisms to strengthen resilience against sophisticated cyberattacks.

[7] This paper analyzes security vulnerabilities in public Wi-Fi networks using Raspberry Pi and Kali Linux. With the widespread use of public Wi-Fi for personal, academic, and business communications, such networks are vulnerable due to open architecture, weak encryption, and minimal authentication. The study develops a portable, cost-effective, and efficient framework for real-time detection, analysis, and exploitation of insecure wireless networks.

The methodology employs Raspberry Pi configured with Kali Linux as a lightweight penetration testing platform. Tools used include Aircrack-ng for packet capturing and WPA/WPA2 key analysis, Kismet for network discovery and rogue AP detection, Reaver for WPS PIN brute-force attacks, and Wireshark for deep packet inspection. Experiments simulate real-world attacks such as evil twin, deauthentication,

MAC spoofing, and man-in-the-middle exploits to demonstrate how weak security allows interception of sensitive information, including usernames, passwords, and session tokens.

Key contributions of the study are:

- Demonstrates Raspberry Pi as a portable, low-cost Wi-Fi security testing and auditing device.
- Provides practical simulations of real-world attacks and identifies critical vulnerabilities in public networks.
- Evaluates the efficiency and effectiveness of commonly used penetration testing tools on resource-constrained hardware.
- Offers practical recommendations for minimizing wireless vulnerabilities and mitigating common attack vectors.

The findings highlight the need for stronger security measures, such as WPA3 encryption, robust authentication, regular monitoring, and intrusion detection systems. The study also suggests integrating Raspberry Pi-based portable testing platforms into enterprise and public networks for continuous security assessments, enabling proactive detection of vulnerabilities and prevention of large-scale data breaches.

[8] This paper presents a supervised machine learning-based Network Intrusion Detection System (NIDS) for IoT environments, where resource constraints and diverse protocols increase vulnerability. Traditional rule-based IDSs struggle with zero-day attacks and high false-positive rates. The authors propose a lightweight framework using a Random Forest (RF) classifier to enhance detection accuracy while minimizing computational overhead.

Data preprocessing was performed on KDDCUP99 and NSL-KDD datasets, including normalization, encoding, removal of duplicates, and feature selection, reducing 41 features to 10 relevant attributes. The RF classifier constructs multiple decision trees and performs majority-vote classification to detect known and unseen attacks effectively.

Key results include:

- Accuracy of 99.9% (KDDCUP99) and 98.1% (NSL-KDD).
- Low false-positive rates and fast training (1.78s) and prediction (0.28s) times.
- Outperforms KNN, Naive Bayes, Decision Tree, and Logistic Regression in detection and efficiency.

The study highlights the framework's suitability for real-time IoT environments, detecting multiple attack types including DoS, probes, U2R, and R2L exploits. Limitations include evaluation on benchmark datasets rather than live IoT traffic. Future work involves real-time deployment, automated mitigation, and predictive threat modeling.

In conclusion, the Random Forest-based IDS provides a scalable, lightweight, and effective solution for securing IoT networks while balancing accuracy and computational efficiency.

[9] This paper presents a low-cost, efficient mechanism to protect wireless LANs from Address Resolution Protocol (ARP) spoofing attacks using a Raspberry Pi as a portable detection and mitigation device. ARP spoofing, a common man-in-the-middle attack, allows attackers to intercept or modify network traffic by sending falsified ARP responses. Traditional detection methods are often expensive, resource-intensive, or unsuitable for small networks.

The proposed Raspberry Pi system performs real-time ARP spoofing detection and mitigation. It continuously monitors network packets, inspects ARP tables, and identifies inconsistencies between IP and MAC addresses. Upon detecting suspicious activity, the system automatically blocks malicious MAC addresses and restores correct ARP entries. The implementation relies on open-source tools, making it easy to deploy and customize for small and medium-sized networks.

Experimental evaluation shows that the system:

- Detects ARP spoofing attempts accurately in real-time.
- Uses minimal resources, suitable for portable deployment.
- Responds quickly to prevent data interception.

Compared to traditional tools, the system is portable, affordable, and easy to integrate. Future enhancements include incorporating machine learning to improve detection, extending protection to other network attacks, and enabling centralized monitoring of multiple Raspberry Pi nodes.

In conclusion, Raspberry Pi-based solutions provide an effective, low-cost defense against ARP spoofing, securing wireless LANs without expensive hardware.

[10] This paper presents a comparative study of two open-source Intrusion Detection Systems (IDSs), Snort and Suricata, deployed on Raspberry Pi devices to evaluate their effectiveness as low-cost network security solutions. With enterprise-grade IDS often being expensive and resource-intensive, Raspberry Pi offers a practical platform balancing detection accuracy, performance, and resource usage.

Two Raspberry Pi devices were deployed in a VLAN-based testbed with Snort on one and Suricata on the other. Real-world attacks, including SYN Flood, Smurf, and UDP Flood, were simulated using hping3. Metrics such as detection accuracy, packet capture rate, CPU and memory usage, and system stability were analyzed.

Key findings include:

- Snort achieves high detection accuracy (up to 93%) for SYN Flood and Smurf attacks with lower CPU usage.
- Suricata handles UDP Flood attacks better (packet capture rate 99.9%) due to its multi-threaded architecture but consumes more CPU and RAM.
- Snort is ideal for resource-constrained environments, while Suricata suits high-bandwidth scenarios.

The study highlights the trade-off between detection efficiency and resource consumption on Raspberry Pi. Future enhancements include integrating machine learning for adaptive

detection, optimizing multi-threaded IDS resource allocation, and scaling for larger networks.

In conclusion, Raspberry Pi-based IDSs offer affordable, practical security for small and medium networks, with Snort providing lightweight detection and Suricata delivering better performance for high-volume traffic.

[11] This paper analyzes Snort-based intrusion detection and prevention techniques to enhance network security against modern threats. Snort, a widely used open-source IDS/IPS, employs a rule-driven architecture for detecting attack signatures, but achieving high accuracy with low false positives remains challenging in dynamic or high-traffic networks. The study evaluates Snort configurations, preprocessor tuning, and integration with complementary tools to improve efficiency and usability.

Experiments were conducted in a controlled setup using simulated attacks and benchmark datasets. Optimized rule sets, advanced preprocessors, and add-ons such as SnortSam (for automated blocking), Snort-inline (for active prevention), and BASE (for visualization) were assessed on detection accuracy, packet processing speed, resource usage, and stability.

Findings show that optimized rules enhance throughput without sacrificing accuracy, SnortSam reduces response time by blocking malicious hosts, Snort-inline prevents intrusions by dropping harmful packets, and BASE improves usability through clear dashboards and alerts. However, Snort is limited against zero-day threats. The study recommends combining it with anomaly detection or hybrid ML-based models, optimizing rule management, and adapting it for IoT or lightweight environments.

In conclusion, carefully tuned and extended Snort remains a powerful, flexible, and affordable IDS/IPS—well-suited for small to medium networks, education, and research, while offering a foundation for future ML/AI-driven improvements.

[12] This paper presents the design of a low-cost firewall system for SOHO networks using Raspberry Pi. The motivation arises from the need for affordable security where enterprise firewalls are too expensive or resource-heavy. With the growth of internet-connected devices in small networks, Raspberry Pi offers a lightweight yet capable solution for firewall and packet-filtering functions.

The system configures Raspberry Pi with `iptables` and `netfilter` to provide packet filtering, NAT, routing, port blocking, packet inspection, and bandwidth monitoring. A SOHO testbed was built to evaluate filtering accuracy, latency, resource usage, and stability.

Results showed that the Raspberry Pi firewall effectively blocked unauthorized connections, enforced rules, and maintained stable operation with minimal latency and manageable resource usage. While scalability under heavy traffic and advanced attack detection remain limitations, Raspberry Pi proves to be a practical alternative for SOHO users.

In conclusion, Raspberry Pi can serve as an efficient and affordable firewall for small networks, offering reliable protection and flexibility. Though not a full replacement for enterprise systems, its ease of deployment and low cost make it suitable for homes, labs, and small offices.

[13] This paper introduces RPiDS, a Raspberry Pi–based intrusion detection framework designed to deliver affordable, lightweight, and portable security monitoring for small-scale networks. Traditional IDS are often costly and resource-intensive, making them unsuitable for small organizations, labs, and home users. Leveraging Raspberry Pi's low power use, compact size, and open-source support, RPiDS demonstrates its viability as a cost-effective IDS platform.

RPiDS functions as a monitoring node, capturing and analyzing packets via `libpcap` with rule-based detection and lightweight anomaly monitoring. It identifies threats such as port scans, brute-force attempts, DoS traffic, and unauthorized access. A web interface supports log management and real-time visualization. Experiments with simulated attacks (e.g., SYN floods, port probes) evaluated detection accuracy, packet capture, CPU/memory usage, and system stability.

Results show RPiDS effectively detects common intrusions with accurate scan and brute-force detection, stable performance under moderate traffic, and reasonable resource consumption. Limitations include reduced performance under heavy traffic and dependence on static rules, restricting detection of novel attacks. Future enhancements involve machine learning integration, distributed Pi clusters, and automated alerting.

In conclusion, RPiDS highlights Raspberry Pi's potential as a practical, low-cost IDS for SOHO, academic, and research environments, offering resource-efficient intrusion detection and valuable educational use.

[14] This paper presents Pi-IDS, a study on the feasibility of running open-source Intrusion Detection Systems (IDS) on Raspberry Pi devices as low-cost alternatives to traditional security appliances. The motivation arises from the need for affordable network security in small offices, home networks, and educational labs, where enterprise IDS solutions are often impractical due to cost and resource demands.

The methodology involved deploying Raspberry Pi with IDS tools such as Snort and Suricata in a testbed network. Simulated attacks included port scans, SYN floods, UDP floods, and ICMP-based attacks. Performance was evaluated in terms of detection accuracy, packet handling, CPU and memory usage, and stability under varying traffic loads. Key findings show that Snort achieved high accuracy in detecting port scans and SYN floods with relatively low CPU usage, while Suricata handled UDP floods more effectively due to its multithreaded design. Both systems, however, experienced packet loss and performance bottlenecks under heavy traffic. Despite these constraints, Raspberry Pi remained stable for

moderate traffic, validating its role as a low-cost IDS platform.

The study concludes that Raspberry Pi-based IDS is suitable for SOHO and educational environments, offering affordability, portability, and low power usage. Limitations include scalability challenges, reduced performance under high traffic, and dependence on predefined rule sets. Future improvements could include configuration optimization, hardware acceleration, machine learning integration, and testing on newer Raspberry Pi models.

[15] This paper highlights the versatility of Raspberry Pi as a low-cost cybersecurity platform that integrates intrusion detection, honeypot deployment, and packet analysis. The motivation arises from the need for affordable security in small networks, educational setups, and research labs, where traditional solutions are often expensive and resource-heavy. Leveraging Raspberry Pi's portability and open-source ecosystem, the study demonstrates a lightweight yet practical approach to proactive defense.

The proposed system combines three functions: (i) IDS to detect attacks such as port scans, brute force, and DoS, (ii) a honeypot to attract and log adversarial activity, and (iii) packet analysis with tools like `tcpdump` for forensic insights. Experiments with simulated attacks showed that the IDS reliably detected intrusions, the honeypot recorded malicious interactions, and packet inspection revealed suspicious traffic. Resource usage remained manageable, though performance degraded under heavy loads.

Limitations include scalability issues, vulnerability to advanced evasion, and dependence on frequent rule updates. Future enhancements may involve ML-based adaptive detection, distributed Pi nodes for scalability, and automated alerting for real-time response. In conclusion, Raspberry Pi proves to be a cost-effective, multifunctional tool for IDS, honeypot, and traffic analysis, making it valuable for both defense and security education.

III. Conclusion

The literature confirms that Raspberry Pi–based systems provide a low-cost platform for intrusion detection, prevention, and deception. Studies highlight the effectiveness of Snort/Suricata for IDS, Pi-hole for DNS filtering, honeypots for attacker analysis, and ML/DL models for improved accuracy, though most prior works remain fragmented and limited by hardware constraints.

DefenderPi addresses this gap by unifying IDS/IPS, DNS filtering, iptables blocking, honeypots, and real-time alerts into a single plug-and-play Wi-Fi appliance. Lightweight AI modules like Isolation Forest and K-Means enhance anomaly detection and device profiling without exceeding resource limits, making it practical for homes, labs, and small offices. While limitations such as throughput ceilings, partial Wi-Fi attack coverage, and inability to stop RF jamming remain, DefenderPi provides a strong, deployable foundation. It translates research into a user-friendly, real-world solution and opens pathways for future work in scalability, WPA3 adoption, advanced traffic analysis, and adaptive AI-driven detection.

References

[1] G. Chamundeeswari, Y. P. Sai Reddy, Y. Mahesh, and Y. G. Priyanka, "Raspberry pi-enhanced intrusion detection system with messenger api integration," in *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2024, pp. 636–642.

[2] T. Garalov and M. Elhajj, "Enhancing iot security: Design and evaluation of a raspberry pi-based intrusion detection system," in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, 2023, pp. 1–7.

[3] E. A. Katonova´, P. Nehila, P. FeciˇlAk, O. Kainz, M. Michalko, F. Jakab, and R. Petija, "Implementation of ids functionality into iot environment using raspberry pi," in *2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2023, pp. 289–294.

[4] A. Bhardwaj, L. Sapra, and V. Sapra, "Unique raspberry pi-based honeypot," in *2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, 2023, pp. 1–6.

[5] A. Rathee, P. Malik, and M. Kumar Parida, "Network intrusion detection system using deep learning techniques," in *2023 International Conference on Communication, Circuits, and Systems (IC3S)*, 2023, pp. 1–6.

[6] G. ZHU, H. YUAN, Y. ZHUANG, Y. GUO, X. ZHANG, and S. QIU, "Research on network intrusion detection method of power system based on random forest algorithm," in *2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, 2021, pp. 374–379.

[7] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H, and S. Alrabaee, "Discovering public wi-fi vulnerabilities using raspberry pi and kali linux," in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, 2020, pp. 1–4.

[8] D. Rani and N. C. Kaushal, "Supervised machine learning based network intrusion detection system for internet of things," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, pp. 1–7.

[9] H. Imad and M. Abdulridha Hussain, "Defending a wireless lan against arp spoofing attacks using a raspberry pi," *Basrah Researches Sciences*, vol. 48, pp. 123–135, 2022.

[10] M. COS¸ AR and H. E. KIRAN, "Performance comparison of open source idss via raspberry pi," in *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, 2018, pp. 1–5.

[11] R. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in kali linux environment," in *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2017, pp. 10–15.

[12] M. Cos¸ar and S. Karasartova, "A firewall application on soho networks with raspberry pi and snort," in *2017 International Conference on Computer Science and Engineering (UBMK)*, 2017, pp. 1000–1003.

[13] A. Sforzin, F. G. Ma´rmol, M. Conti, and J.-M. Bohli, "Rpids: Raspberry pi ids — a fruitful intrusion detection system for iot," in *2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, 2016, pp. 440–448.

[14] A. K. Kyaw, Y. Chen, and J. Joseph, "Pi-ids: evaluation of open-source intrusion detection systems on raspberry pi 2," in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, 2015, pp. 165–170.

[15] S. Tripathi and R. Kumar, "Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer," in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 2018, pp. 80–85.