A SYSTEMATIC LITERATURE REVIEW OF RASPBERRY PI-BASED INTRUSION DETECTION SYSTEMS

by

AKINYEMI FAYANKINNU

B.Sc., University of Ado-Ekiti, 2006

M.B.A., Obafemi Awolowo University, 2012

M.S., National University, 2019

M.S., Kennesaw State University, 2023

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2026

A systematic literature review of Raspberry Pi-based intrusion detection systems

Akinyemi Fayankinnu, *Middle Georgia State University, akinyemi.fayankinnu@mga.edu*

Abstract

The rapid digitalization of the global economy has led to an increased dependence on interconnected computer systems, thereby expanding the attack surface available to malicious actors. This study synthesizes a collection of peer-reviewed articles to evaluate the potential of the Raspberry Pi as a viable component in network security architecture. The study identifies a significant methodological shift from traditional signature-based detection and passive honeypots toward hybrid architectures that integrate machine learning (ML) for anomaly detection. By systematically analyzing the architectural constraints and performance capabilities of the Raspberry Pi in intrusion detection and monitoring applications, the findings aim to inform both researchers and practitioners on the feasibility of integrating these low-cost single-board computers into layered network defense strategies.
Keywords: Raspberry Pi, intrusion detection, intrusion prevention, honeypot, IDS

Introduction

The digitalization of the global economy has resulted in an increasing reliance on computer systems and interconnected networks. Major infrastructure installations, such as electricity grids, water supply systems, air traffic control systems, and telecommunications networks, depend on computer networks to function properly. Similarly, essential services such as healthcare, education, banking, and e-commerce also rely on the internet. While this has resulted in increased productivity, it has also led to the creation of a potential attack vector that adversaries can exploit to wreak havoc indiscriminately (Montgomery, 2018).

Further, cyberattacks are becoming increasingly complex and challenging to detect (Hacılar et al., 2024), and their impacts are growing exponentially (Hiller et al., 2024). Moreover, attackers have relatively low initial costs to launch these attacks, while the cost of defending against them can be enormous (Hiller et al., 2024). The global economic impact of cybercrime is projected to exceed $10.5 trillion annually by 2025, which represents a remarkable 15 percent annual growth rate over the preceding five years (Salzman, 2023).

To combat cyberattacks, intrusion detection systems (IDSs) are widely used to detect network intrusions originating from both internal and external sources. However, most IDS techniques are inadequate due to the complex and rapidly evolving nature of cyberattacks (Ozkan-Okay et al., 2021). Therefore, it is imperative to develop new methods and enhance current technologies in this field. This paper focuses on the current state of research into IDS based on the Raspberry Pi. The Raspberry Pi is low-cost, credit card-sized computer that is easily deployable and energy efficient, making it an ideal platform for IDS research.

The growing number of network attacks in recent times has resulted in increased interest and research in alternative security measures, particularly IDS (Ozkan-Okay et al., 2021). However, research on Raspberry Pi-based IDS remains fragmented and largely focused on proof-of-concept. While many researchers have demonstrated the feasibility of Raspberry Pi-based IDS, the viability of these systems has not been rigorously validated. There is a significant disconnect between the controlled environments used for these experimental setups and the reality of modern, high-throughput network environments with diverse endpoints. A systematic analysis of these architectural constraints and performance metrics can demonstrate the Raspberry Pi's viability as a platform for enhancing the security architecture of enterprise-grade networks, rather than just a hobbyist tool.

The proposed research builds on the prior work to construct a taxonomy of Raspberry Pi-based IDS and honeypots. By going beyond descriptive analysis, this research aims to answer the following research question:

RQ1. How do the predominant Raspberry Pi–based intrusion detection techniques perform under the platform's hardware limitations, and to what extent can emerging technologies, such as edge and fog computing architectures, enhance their accuracy, efficiency, and scalability?

Review of the Literature

The Raspberry Pi is an effective prototyping device popular among researchers and developers due to its affordability, user-friendly setup, and adaptability for various projects, including data acquisition, control systems, simulation, and modeling (Mathe et al., 2024). Researchers have increasingly utilized these low-cost devices to address cybersecurity challenges primarily through two distinct yet complementary mechanisms: deceptive honeypots and IDS. Figure 1 depicts a Raspberry Pi 5 which is equipped with a Broadcom 2.4GHz quad-core 64-bit Arm Cortex-A76 Central Processing Unit (CPU). It also features dual 4Kp60 HDMI displays, up to 16GB of SDRAM, dual-band 802.11ac Wi-Fi, Bluetooth 5.0 and Bluetooth Low Energy (BLE), a microSD card slot, multiple USB ports, and Gigabit Ethernet (Raspberry Pi, 2025).

Figure 1
Image of a Raspberry Pi 5 Board

Note. From Raspberry Pi 5 product brief, Raspberry Pi Ltd., https://pip-assets.raspberrypi.com/categories/892-raspberry-pi-5/documents/RP-008348-DS-4-raspberry-pi-5-product-brief.pdf?disposition=inline

Raspberry Pi as a Honeypot

Honeypots have been deployed on Raspberry Pi as early warning systems and indicators of compromise (IoCs) for both internal and external threats (Catherine & Kumawat, 2020). However, implementations vary significantly in complexity and purpose. While Catherine & Kumawat (2020) primarily used the Raspberry Pi as a host for traditional Linux-based network monitoring tools, Omar et al. (2024) took a different approach by integrating a Field-Programmable Gate Array (FPGA) on a Raspberry Pi for the detection of threats at the hardware level. Their low-interaction honeypot simulated an administrator login webpage and log session information, including the client's IP address, request type, entered values, and connection port. This approach prioritized resource scalability and efficiency, allowing for the deployment of multiple honeypots across a large IoT network. The results demonstrated that lightweight honeypots can accurately detect hardware-level threats such as hardware Trojans and malicious connection attempts.
Conversely, Bistarelli et al. (2020) utilized a more data-intensive approach to assess the security of IoT devices. The authors set up three distinct honeypots: Cowrie, Dionaea, and Whaler, on a Raspberry Pi, employing various virtualization techniques. Unlike Omar et al. (2024), who focused on hardware threats, this study applied the Elasticsearch, Logstash, and Kibana (ELK) stack for log analysis, processing, and

visualization. The researchers analyzed the frequency and geographical distribution of attacks on IoT services, demonstrating the platform's ability to handle complex log processing despite its relatively small size. (Bistarelli et al., 2020).
However, this implies that while Raspberry Pi can effectively manage advanced logging, simultaneously using it for data capture and visualization (e.g., Kibana) could introduce constraints. Consequently, it may not be ideal for real-time monitoring during active attack scenarios involving large volumes of data.

Raspberry Pi as a Lightweight Intrusion Detection System

A lightweight portable intrusion detection system (LPIDS) was implemented by deploying two string-matching algorithms on the WiFi Pineapple and Raspberry Pi (Nykvist et al., 2020). While this approach proved effective in detecting known threats, other studies have utilized machine learning algorithms to identify complex network attacks and data collection (Soe et al., 2020). Additionally, machine learning algorithms have been employed for flow-based intrusion detection and predicting attacks (Katonová et al., 2023).
In both medical and industrial settings, researchers have increasingly adopted anomaly-based detection on Raspberry Pi platforms, demonstrating its potential to identify emerging threats despite hardware constraints (Tirumala et al., 2022; Zachos et al., 2025). A low-cost intelligent cyber-defense system (iCDS) for SME networks was implemented on a Raspberry Pi 4, evaluating the performance of the network interfaces and their ability to manage high volumes of network traffic (Tirumala et al., 2022). An anomaly-based IDS was developed to monitor Internet of Medical Things (IoMT) devices and networks. This design utilized novelty detection and outlier detection algorithms for identifying security events (Zachos et al., 2025).
Similarly, an IDS incorporating a deep learning algorithm that progressively learns features from data at multiple levels was deployed on a Raspberry Pi. Idrissi et al. (2022) demonstrated that by using Google's TensorFlow Lite, a Raspberry Pi could achieve 99.52% prediction accuracy, overcoming the hardware limitations that previously restricted deep learning deployment. In another study, an IDS that employed a Dynamic Access Control (DAC) algorithm was implemented on a Raspberry Pi to enhance security and usability for Internet of Things (IoT) devices. The researchers achieved high detection accuracy and low false positive rates using this approach, further validating the Raspberry Pi's capability to handle advanced logic (Alazab et al., 2024).
Likewise, Stolz et al. (2024) developed a lightweight IDS that utilizes both signature-based and anomaly-based techniques. Incorporating machine learning algorithms, their design successfully detected attacks such as the Ping of Death, SYN Flood, and SSH brute-force attempts. To train their model, the authors selected the top 20 contributing features using the Random Forest classifier algorithm. This approach significantly reduces the processing power required for training detection models, making it suitable for resource-constrained devices like the Raspberry Pi. However, the reported CPU usage of 54.3% (snort) and 73.3% (python3) during testing may pose challenges in high-throughput environments, potentially causing the IDS to fail or drop packets it was intended to examine.
Furthermore, Gombao (2025) and Wijethilaka et al. (2025) both demonstrated the effectiveness of sophisticated, machine learning-based network intrusion detection systems (NIDS) on the Raspberry Pi. These studies prioritized real-time processing and computational efficiency to meet the needs of modern networks, particularly Small and Medium Enterprises (SMEs) and enterprise broadcast environments where on-premises server infrastructure may be unavailable. Moving away from signature-based detection, the authors adopted adaptive machine learning models that can identify evolving threats, such as zero-day attacks and complex denial-of-service (DoS) attacks, while maintaining a low false-positive rate through optimized data handling. While Gombao (2025) focused on broadcast network environments, Wijethilaka et al. (2025) adopted a broader and more algorithmically diverse machine learning framework, including Random Forest, LSTM, ANN, XGBoost, and Naive Bayes, to classify inbound and outbound traffic on a Raspberry Pi.

While the detection rates in these studies are commendable, there are gaps in reporting detection latency. Due to the resource constraints of the Raspberry Pi, it's crucial to determine if it can detect malicious traffic in real-time while running machine learning algorithms.

Raspberry Pi as an Intrusion Detection System and Honeypot (Hybrid)

Researchers have also implemented a combination of intrusion detection (Snort), honeypot (Cowrie), and packet analyzer (TShark) on a Raspberry Pi. These authors were able to detect unauthorized connection attempts, log brute force attacks, and capture network traffic on the device. The captured packets were analyzed for indicators of malicious activity and to gain an understanding of the attackers' methods (Tripathi & Kumar, 2018). However, the literature is quite limited on testing these hybrid systems against Denial of Service (DOS) and Distributed Denial of Service (DDoS) attacks, where resource exhaustion is the primary aim of the attacker.

Synthesis and Gaps

The existing literature strongly supports the use of Raspberry Pi as a compelling and cost-effective tool for decentralized cybersecurity. It has been applied successfully as both a scalable early-warning system (honeypot) and a lightweight IDS. Research has shown that, despite its hardware limitations, IDSs based on the Raspberry Pi can achieve high predictive accuracy using optimized frameworks like TensorFlow Lite, especially in IoT and medical environments. While the feasibility of these systems is well-documented, significant operational uncertainties persist regarding their resilience in hostile, complex real-world networks. This systematic literature review aims to address these gaps by correlating reported architectural types with performance metrics to determine the actual operational limits of Raspberry Pi-based IDSs.

Methodology

The proposed research builds on the identified research gaps by adopting a qualitative systematic literature review (SLR) based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 framework to ensure methodological rigor, transparency, and repeatability. The methodology outlines the processes examining the use of Raspberry Pi as an IDS or honeypot.

Research Design

This study employed a systematic literature review to examine how Raspberry Pi devices have been utilized, evaluated, and optimized for intrusion detection and network security. The design was selected to synthesize disparate findings from experimental, comparative, and applied research, while providing a comprehensive overview of the current state of knowledge in this field. The review focused on:

(i) The effectiveness of Raspberry Pi-based IDS
(ii) Performance limitations and challenges (e.g., CPU, memory utilization, throughput)
(iii) Types of IDS implementations used (signature-based, anomaly-based, hybrid)
(iv) Techniques for improving detection accuracy or resource efficiency

This structured approach facilitates a comprehensive understanding of how Raspberry Pi contributes to low-cost, energy-efficient intrusion detection architectures.

Systematic Review Method

The review process adheres to the PRISMA 2020 guidelines to ensure transparency and rigor in selecting and analyzing literature. As outlined by Page et al. (2021), PRISMA 2020 consists of four phases: identification, screening, eligibility, and inclusion.

Inclusion and Exclusion Criteria

Developing a set of predefined inclusion and exclusion criteria ensures the review's focus, relevance, and methodological rigor. The selection prioritized peer-reviewed studies published in English between 2010 and 2025 that provide empirical results, performance analyses, architectural designs, or theoretical contributions aligned with the review's research question. Therefore, publications that do not directly address Raspberry Pi's use in network intrusion detection or fail to provide substantial insights were excluded. The selection criteria is presented in Table 1.

Table 1

Inclusion and Exclusion Criteria

Criteria	Inclusion Criteria	Exclusion Criteria
Publication Type	Peer-reviewed articles published between 2010 and 2025	Abstracts, blogs, reviews, and non-peer reviewed articles
Language	English	Articles published in a language other than English
Research Domain	Articles focusing on Raspberry Pi usage for intrusion detection	Papers unrelated to intrusion detection or prevention

Databases

The search was conducted across four major technical and scientific databases relevant to computer science, cybersecurity, and embedded systems. These databases were selected due to their extensive coverage of computing, networking, broadcast technologies, robotics and control systems, and applied research involving IoT devices and embedded platforms.

- Google Scholar
- IEEE Xplore
- ScienceDirect
- SpringerLink

Search Strategy

Boolean operators and a combination of targeted keywords were utilized to ensure variations in terminology are captured. The following search strings were used for all the selected databases:

- "Raspberry Pi" AND ("intrusion detection system" OR "IDS")
- "Raspberry Pi" AND ("intrusion prevention system" OR "IPS")
- "Raspberry Pi" AND ("network Intrusion detection system" OR "NIDS")
- "Raspberry Pi" AND ("network intrusion prevention system" OR "NIPS")

Searches were conducted for peer-reviewed articles published in English between 2010 and 2025. Articles were initially screened for relevance to Raspberry Pi-based intrusion detection or honeypot systems. Studies that utilized the Raspberry Pi only as an IoT sensor or data collection device were excluded.

Data Extraction and Synthesis

Data extraction and synthesis were carried out using Taguette, an open-source qualitative analysis tool designed to identify and organize recurring concepts across multiple studies. By extracting, labeling, and categorizing key themes related to Raspberry Pi–based intrusion detection and prevention systems, Taguette ensured a consistent and transparent approach to analyzing patterns in the literature. The extracted data included author(s), publication year, implementation type (IDS, IPS or honeypot) and key findings. These are presented in Table 2.

Table 2

Authors and Annotations

S/N	Author(s)	Publication Year	Implementation	Key Findings	Category
1	Alazab et al.	2024	LSTM-based Intrusion Detection System (IDS) with a Dynamic Access Control (DAC) algorithm to detect and defend against network intrusion	97.16% validation accuracy reported	IDS
2	Bistarelli	2020	Implemented three honeypots - Cowrie, Dionaea, and Whaler running in Doker containers on a Raspberry Pi. The study utilized the ELK stack for log analysis, processing, and visualization	The frequency and geographical distribution of attacks on IoT services, showcasing the platform's capability to manage intricate log processing despite its relatively small size	Honeypot
3	Catherine & Kumawat	2020	Implemented a low-interaction honeypot on Raspberry Pi 4 to monitor the traffic on small networks	Used Snorts as IDS, Cowrie and Dionaea as honeypot and Tshark for packet analysis	Honeypot
4	Gombao	2025	Utilized the Isolation Forest machine learning algorithm for anomaly detection in broadcast networks	Detection accuracy of 83.5% reported	NIDS
5	Idrissi et al.	2022	Implemented a low-interaction honeypot on Raspberry Pi 4 to monitor the traffic on small networks	Up to 99.74% accuracy reported	Honeypot
6	Omar et al.	2024	Low-interaction honeypot for the detection of hardware-level threats such as hardware Trojans and malicious connection attempts	Hardware honeypots can provide a flexible and robust defense layer against hardware trojan attacks	Honeypot

Table 2 (Continued)
Authors and Annotations

S/N	Author(s)	Publication Year	Implementation	Key Findings	Category
7	Soe et al.	2020	Implemented a lightweight correlation-based feature selection (CFS) machine learning algorithm on Raspberry Pi for intrusion detection	Feature selection algorithms like CFS can lead to improved efficiency	IDS
8	Stolz et al.	2024	Implemented lightweight IDS using anomaly-based and signature-based techniques and ML	Trained model using feature selection. Detection accuracy of 98.1% reported	IDS
9	Tirumala et al.	2022	Evaluated the performance of the Raspberry Pi's network interfaces and their ability to manage high volumes of network traffic. Implemented a lightweight machine learning-based malware detection	Classification accuracy of 92.1% reported.	IDS
10	Tripathi and Kumar	2018	A combination of intrusion detection (Snort), honeypot (Cowrie), and packet analyzer (TShark) on Raspberry Pi	The Raspberry Pi can be deployed as an inexpensive, lightweight security monitoring tool	NIDS
11.	Wijethilak et al.	2025	Leveraged machine learning algorithms including Random Forest, Long Short-Term Memory (LSTM) networks, Artificial Neural Networks (ANN), XGBoost, and Naive Bayes to classify both inbound and outbound traffic	96.5 % detection accuracy on the NF-UQ-NIDS dataset	NIDS
12.	Zachos et al.	2025	Implemented an anomaly-based IDS for Internet of Medical Things (IoMT) devices leveraging Novelty Detection and Outlier Detection algorithms	96.5% accuracy, 99% precision, and 89.62% recall reported	IDS

Results

The systematic analysis of the selected literature unveiled important trends and challenges in implementing Raspberry Pi-based IDSs.

Trade-offs between detection accuracy and hardware limitations

A central theme in research on Raspberry Pi-based IDS revolves around the performance limitations inherent in single-board computers. Researchers must find a balance between intrusion detection capabilities and the physical constraints of edge hardware. While machine learning algorithms enable high detection accuracy, they frequently push the hardware to its operational limits, leading to potential failures. In a bid to reduce the computational power required for training machine learning algorithms used in Raspberry Pi-based IDSs, researchers often resort to pruning training datasets to the top 20 features. While this approach enables such designs to run on the Raspberry Pi, it poses a risk of missing attack patterns that depend on the omitted features.

Architectural configurations for optimal throughput

To maximize throughput from Raspberry Pi-based IDSs, integrating Raspberry Pi nodes with Field-Programmable Gate Arrays (FPGAs) enables the deployment of a distributed network of detection nodes. The FPGA efficiently handles computationally intensive tasks, making it suitable for resource-constrained environments. Its adaptability allows for easy scaling and widespread deployment, resulting in broader coverage and increased aggregate throughput.

Best practices for scalable real-world deployment

Combining lightweight signature-based detection methods for known threats with anomaly-based machine learning algorithms for zero-day attack detection offers a robust layered defense strategy. Feature selection algorithms such as Random Forest help identify and select the most significant features from training data, removing less relevant ones. This process improves detection accuracy, reduces false positives, and minimizes computational overhead.

Discussion

The results section covered significant trends and challenges in implementing Raspberry Pi-based IDSs. The findings offer valuable insights into the trade-offs between detection accuracy and the inherent hardware limitations of Raspberry Pi. This discussion will focus on the most prevalent detection techniques, examine the performance implications of hardware constraints, and explore how emerging technologies such as edge computing and fog computing can enhance performance and scalability.

As it relates to the most predominant approach, it currently involves combining signature-based detection with anomaly-based detection. This approach ensures comprehensive coverage for both known and zero-day threats. Machine learning algorithms such as One Class Support Vector Machine (OCSVM) and Isolation Forest have been utilized to classify network traffic with high accuracy exceeding 94% (Zachos et al., 2025).

Concerning the impact of hardware limitations, the computational overhead required for running intrusion detection processes often exceeds the capabilities of the Raspberry Pi. Stolz et al. (2024) conducted load tests and reported CPU usage of 54.3% for Snort and 73.3% for their machine learning anomaly detection algorithm. Without deploying additional processing capacity, this could lead to packet dropping or network overload, potentially causing the IDS to fail.

Relating to edge computing and fog computing, which bring processing capabilities closer to the network edge. These technologies enhance scalability by distributing data processing, storage, and

networking closer to the data source (Mahmud & Toosi, 2022). Integrating them into Raspberry Pi-based IDSs will eliminate the need to transmit large amounts of data to centralized cloud servers, thereby reducing latency, optimizing bandwidth, and improving detection response times.

Limitations

The objective of this systematic literature review was to create a taxonomy of Raspberry Pi-based IDSs and honeypots. Due to the rapid pace of technology advancements in recent times, only peer-reviewed journals accessible through selected academic databases and published in English between 2010 and 2025 were considered. This may have inadvertently excluded relevant research published in languages other than English or in databases not included in the search.

Furthermore, the reviewed studies showed variations in experimental design, hardware configurations, datasets, and evaluation metrics, thereby making a direct comparison of results challenging. Most of the studies reviewed relied on small-scale experimental setups and simulated network traffic, which may not fully represent the complexities of real-world enterprise networks with diverse endpoints.

Lastly, since the review synthesizes previously published research rather than conducting empirical testing, the conclusions are contingent on the quality, scope, and methodological rigor of the included studies. These limitations underscore the need for more standardized evaluation frameworks and large-scale experimental deployments in future research on Raspberry Pi–based IDSs and honeypots.

Conclusion and recommendations for future research

This research demonstrates the evolution of the Raspberry Pi from a hobbyist tool to a sophisticated and cost-effective tool for decentralized network security. The synthesis of contemporary literature reveals that the most predominant and effective IDS implementations utilize hybrid architectures that combine machine learning with signature-based detection and anomaly-based detection. These systems effectively counter modern threats like SYN Flood attacks, SSH brute-force attempts, and circuit-level Hardware Trojans.

However, hardware limitations remain a significant concern for live deployments of Raspberry Pi-based IDSs. The computational overhead required to run multiple detection engines concurrently can exceed the Raspberry Pi's CPU capabilities. To address this, recent research has shifted towards architectural approaches such as edge computing and fog computing. By distributing data processing across clusters and focusing analysis on the most impactful features, researchers have achieved high detection accuracy in high-throughput environments. Ultimately, the Raspberry Pi has the potential to become a vital tool for network monitoring and intrusion detection within the modern cybersecurity ecosystem.

For the Raspberry Pi-based IDSs to become truly resilient network security monitoring tools, future research should further explore the use of FPGAs to significantly reduce the high CPU usage currently observed in hybrid systems. Additionally, further experimentation is needed to enhance the integration of fog and edge computing for real-time network monitoring, efficient data processing, quicker detection response times, and scalability. Furthermore, research is required to determine the frequency of retraining these lightweight machine learning models to maintain their effectiveness against constantly evolving threats in live networks.

Furthermore, additional research should be conducted to assess the feasibility of deploying distributed, containerized IDSs based on Raspberry Pi. Multi-device deployments of Raspberry Pi-based IDSs and honeypots enable concurrent execution of multiple intrusion detection processes. Collecting, logging, and analyzing network traffic across different physical devices and processes can significantly reduce the CPU load, thereby enabling more robust detection techniques and algorithms to be installed on Raspberry Pi. Containerization ensures that the IDS or honeypot instances are logically isolated, enhancing security through the separation of processes and file systems. This safeguards against potential attacks and facilitates the seamless provisioning, deprovisioning, and maintenance of IDSs.

References

Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., & Alturki, R. (2024). A novel IDS with a dynamic access control algorithm to detect and defend intrusion at IoT nodes. *Sensors*, *24*(7), 2188. https://doi.org/10.3390/s24072188

Bistarelli, S., Bosimini, E., & Santini, F. (2020). A report on the security of home connections with IoT and Docker honeypots. *ITASEC*, *60*. https://ceur-ws.org/Vol-2597/paper-06.pdf

Catherine, M., & Kumawat, A. (2020). Securing a small network by using Raspberry Pi honeypot. *International Journal of Innovative Technology and Exploring Engineering*, *9*(7), 773–778. https://doi.org/10.35940/ijitee.F4561.059720

Gombao, J. (2025). BCAST IDS: A novel network intrusion detection system for broadcast networks. *IEEE Access*, *13*, 110289–110306. https://doi.org/10.1109/ACCESS.2025.3582893

Hacılar, H., Dedeturk, B. K., Bakir-Gungor, B., & Gungor, V. C. (2024). Network anomaly detection using deep autoencoder and parallel artificial bee colony algorithm-trained neural network. *PeerJ Computer Science*, *10*, e2333. https://doi.org/10.7717/peerj-cs.2333

Hiller, J., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*, *61*(1), 5–29. https://doi.org/10.1111/ablj.12238

Idrissi, I., Azizi, M., & Moussaoui, O. (2022). A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT. *International Journal of Computing and Digital Systems*, *11*(1), 209–216. https://doi.org/10.12785/ijcds/110117

Katonová, E. A., Nehila, P., Feciľak, P., Kainz, O., Michalko, M., Jakab, F., & Petija, R. (2023). Implementation of IDS functionality into IoT environment using Raspberry PI. *2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 289–294. https://doi.org/10.1109/ICETA61311.2023.10343741

Mahmud, R., & Toosi, A. N. (2022). Con-Pi: A distributed container-based edge and fog computing framework. *IEEE Internet of Things Journal*, *9*(6), 4125–4138. https://doi.org/10.1109/JIOT.2021.3103053

Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). A comprehensive review on applications of Raspberry Pi. *Computer Science Review*, *52*, 100636. https://doi.org/10.1016/j.cosrev.2024.100636

Montgomery, M. (2018). Proliferation of cyberwarfare under international law: Virtual attacks with concrete consequences. *S. Cal. Interdisc. LJ*, *28*, 499.

Nykvist, C., Larsson, M., Sodhro, A. H., & Gurtov, A. (2020). A lightweight portable intrusion detection communication system for auditing applications. *International Journal of Communication Systems*, *33*(7), e4327. https://doi.org/10.1002/dac.4327

Omar, A. H. E., Soubra, H., Moulla, D. K., & Abran, A. (2024). An innovative honeypot architecture for detecting and mitigating hardware Trojans in IoT devices. *IoT*, *5*(4), 730–755. https://doi.org/10.3390/iot5040033

Ozkan-Okay, M., Samet, R., Aslan, O., & Gupta, D. (2021). A comprehensive systematic literature review on intrusion detection systems. *IEEE Access*, *9*, 157727–157760. https://doi.org/10.1109/ACCESS.2021.3129336

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Raspberry Pi Ltd. (2025, December). *Raspberry Pi 5 product brief*. https://pip-assets.raspberrypi.com/categories/892-raspberry-pi-5/documents/RP-008348-DS-4-raspberry-pi-5-product-brief.pdf?disposition=inline

Salzman, N. (2023). The cybersecurity framework's most vulnerable user: small business. *Journal of Information Warfare*, *22*(4), 53–71. International Security & Counter Terrorism Reference Center.

Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Implementing lightweight IoT-IDS on Raspberry Pi using correlation-based feature selection and its performance evaluation. In L. Barolli, M. Takizawa, F. Xhafa, & T. Enokido (Eds.), *Advanced Information Networking and Applications* (Vol. 926, pp. 458–469). Springer. https://doi.org/10.1007/978-3-030-15032-7_39

Stolz, C., Li, F., & Zhang, J. (2024). Implementing lightweight intrusion detection system on resource constrained devices. *2024 Cyber Awareness and Research Symposium (CARS)*, 1–6. https://doi.org/10.1109/CARS61786.2024.10778716

Tirumala, S. S., Nepal, N., & Ray, S. K. (2022). Raspberry Pi-based intelligent cyber defense systems for SMEs and smart-homes: An exploratory study. *EAI Endorsed Transactions on Smart Cities*, *6*(18), e4. https://doi.org/10.4108/eetsc.v6i18.2345

Tripathi, S., & Kumar, R. (2018). Raspberry Pi as an intrusion detection system, a honeypot and a packet analyzer. *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 80–85. https://doi.org/10.1109/CTEMS.2018.8769135

Wijethilaka, R. W. K. S., Yapa, K., & Siriwardena, D. (2025). A cost effective machine learning based network intrusion detection system using Raspberry Pi for real time analysis. *PLOS One*, *20*(12), e0331123. https://doi.org/10.1371/journal.pone.0331123

Zachos, G., Mantas, G., Porfyrakis, K., Manuel Camões Sobral De Bastos, J., & Rodriguez, J. (2025). Anomaly-based intrusion detection for IoMT networks: design, implementation, dataset generation, and ML algorithms evaluation. *IEEE Access*, *13*, 41994–42028. https://doi.org/10.1109/ACCESS.2025.3547572