Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

A COMPREHENSIVE REVIEW OF IOT VULNERABILITY SCANNING: ACTIVE, PASSIVE, AND HYBRID METHODOLOGIES

[1]Muhammad Hamza Hayat, [*2]Asad Liaqat, [3]Laiba Shoaib, [4]Abdul Rehman Chishti

[1-4]Department of Information and Communication Engineering, Islamia University of Bahawalpur, Bahawalpur, Pakistan
*[*2]asad2liaqat@gmail.com*

Keywords
IoT Security, Vulnerability Scanning, Active Probing, Machine Learning, MQTT, RTSP.

Article History
Received on 29 March, 2026
Accepted on 17 April, 2026
Published on 19 April, 2026

Corresponding Author:
Asad Liaqat

Abstract
The Internet of Things (IoT) is a rapidly emerging paradigm that has led to billions of devices being exposed to exploitation because there has not been a standard security protocol to regulate the IoT. Compared to conventional IT assets, IoT devices that have limited resources usually do not have inbuilt antivirus features, necessitating vulnerability assessment at the network level. This paper reviews the most recent state-of-the-art IoT security scanning mechanisms published between 2020 and 2025. We distinguish two main taxonomies of existing methods: Active Scanning (where deterministic probing (e.g. Nmap, Shodan) is used to quickly enumerate devices) and Passive Monitoring (where Machine Learning (ML) is used to identify traffic anomalies). Although the ML-based Intrusion Detection Systems (IDS) are highly accurate, our analysis indicates that there is a high computational overhead, which prevents its use on edge gateways. On the other hand, active scanning methods offer lightweight real-time risk analysis with the difficulties of network overload and protocol heterogeneity, such as MQTT and RTSP. This analysis reveals some of the most critical research gaps such as the absence of real-time and lightweight tools for edge deployment, and the inconsistency of protocol detection in the modern world. Lastly, we provide the future directions of scalable and secure IoT ecosystems.

Introduction

The Internet of Things (IoT) has become a new technological paradigm that unites physical objects and digital systems to support real-time data collection and autonomous decision-making [1]. This ecosystem is growing exponentially; according to the International Data Corporation (IDC), the number of connected IoT endpoints is expected to grow to 41.6 billion by 2025, generating approximately 79.4 zettabytes of data annually [2]. While estimates vary depending on whether broad edge-computing nodes are included in the metric, other analyses indicate even stronger growth, with up to 75.44 billion device connections by 2025, representing a compound annual growth rate (CAGR) of 28.7% [3]. This rapid expansion is driven by the integration of IoT into diverse sectors such as intelligent manufacturing, healthcare, and smart cities [4].

Projected exponential growth of IoT connected devices from 2020 to 2025 .

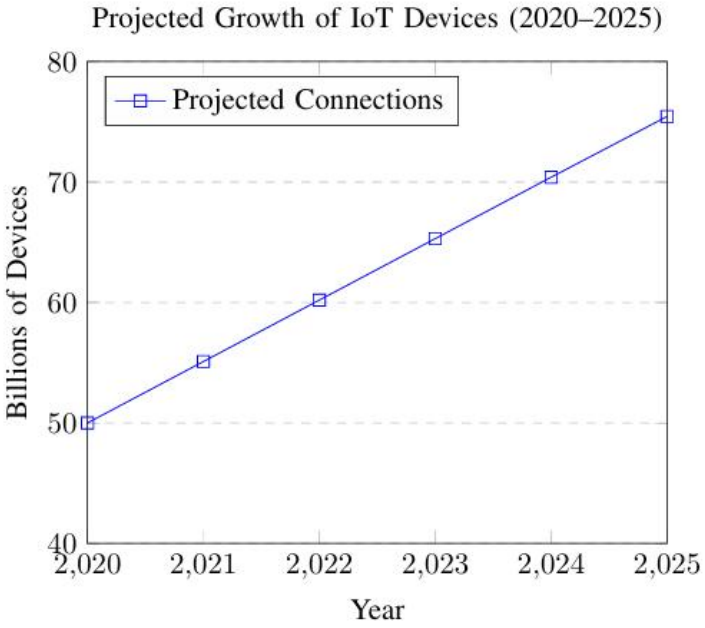

Figure 1: Projected exponential growth of IoT connected devices from 2020 to 2025 [3].

Despite its transformative potential, the IoT environment faces unique security threats unlike traditional IT networks [5]. While conventional infrastructure relies on standardized security measures, IoT is characterized by high heterogeneity, with devices from various manufacturers using different protocols and architectures [6]. Furthermore, a lack of uniform security standards has led to fragmented implementations, resulting in widespread network vulnerabilities [7]. These challenges are compounded by the resource constraints of IoT devices, which often lack the processing power, memory, and energy required for traditional security mechanisms [8].

The primary issue addressed in this review is the failure of traditional antivirus and anti-malware software on IoT devices [9]. Lacking the resources for deep packet inspection or large signature databases, these devices are often deployed with minimal internal defenses

[10]. Consequently, perimeter-based defenses are insufficient, necessitating a shift toward network-based scanning and intelligent Intrusion Detection Systems (IDS) that can detect traffic anomalies without overburdening the devices.

Scope and Methodology: To ensure relevance to the current threat landscape, this review focuses on peer-reviewed literature and industrial reports published between 2020 and 2025. Primary databases including IEEE Xplore, ACM Digital Library, and SpringerLink were queried using keywords such as "IoT Vulnerability Scanning," "Active Probing," "Machine Learning IDS," and "IoT Protocol Security." The selection criteria prioritized studies that offered empirical comparisons of scanning overhead or introduced novel hybrid architectures, while purely theoretical models lacking deployment metrics were excluded.

The remainder of this paper is organized as follows. Section II analyzes active vulnerability scanning approaches, including prominent tools like Shodan and Nmap. Section III examines passive monitoring techniques, focusing on the integration of Machine Learning (ML) and Deep Learning (DL) for anomaly detection. Section IV details specific protocol vulnerabilities in MQTT and RTSP that challenge standard scanning methods. Section V identifies critical research gaps, particularly the lack of lightweight tools for edge devices. Finally, Section VI provides a comparative analysis of recent studies, and Section VII concludes the paper.

Active Vulnerability Scanning Approaches

Active vulnerability scanning falls under the category of pre-exploitation penetration testing mechanisms, assuming an aggressive posture toward regular network inspection to identify potential vulnerabilities in advance [11]. The technical core of this process is active probing, where specialized software initiates carefully designed network probes or HTTP requests to remote host ports to evoke a valid response [12]. Upon receiving a response, the system employs fingerprinting techniques to capture "banners" text advertised by services and compares them against databases of known signatures to determine the vendor, device model, and firmware version [13].

Prominent Tools

- **Nmap:** An open-source utility popular for network reconnaissance and service discovery, supported by ping-based scanning and banner grabbing to determine the applications and services running on particular ports [14].
- **Shodan:** Commonly referred to as a cyberspace search engine, it continuously probes the whole IPv4 space to add decoded responses to a large searchable database of Internet-facing devices.

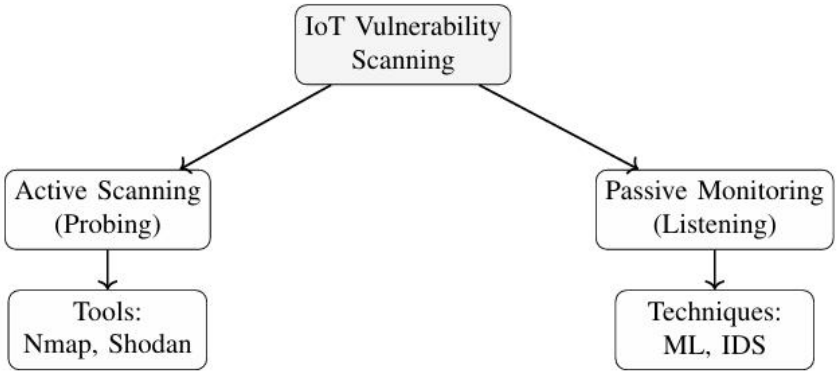

Fig. 2. Taxonomy of IoT vulnerability scanning methodologies: Active Probing vs. Passive Monitoring.

Figure 2: Taxonomy of IoT vulnerability scanning methodologies: Active Probing vs. Passive Monitoring.

- **Nessus:** A specialized vulnerability scanner that connects directly to systems to discover vulnerabilities by correlating network probe responses with a database of predefined profiles, rules, and signatures [15].

Active scanning offers high speed and supports device discovery in large, heterogeneous networks. These tools automatically enumerate services and ports to identify exposed Industrial Control Systems (ICS) and smart building components that might otherwise remain hidden due to non-standard port usage. Furthermore, active probing enables fine-grained firmware version identification, which is critical for detecting specific "N-day" vulnerabilities.

However, active scanning faces serious technical and ethical constraints. The process generates significant traffic, potentially causing congestion and latency that disrupt high-throughput environments [16]. More critically, active probing can crash fragile IoT devices that lack the processing capacity to handle high-volume requests or malformed packets [17]. To mitigate these risks, researchers often limit probes to non-mutating requests and avoid automated authentication attempts. Additionally, scanners like Shodan may provide outdated information, as they rely on cached snapshots rather than real-time network states.

Proposed Academic Frameworks

- **PLCHound:** An automated ICS asset discovery tool that employs an optimization algorithm to generate cross-protocol queries and time-resistant signatures for locating field-deployed devices [18].
- **LSTM-EVI:** A deep learning-powered penetration testing architecture that combines Nessus, Scapy, and Zeek to conduct reconnaissance and detect scanning attacks with high precision [19].
- **IoT-PEN:** A scalable, client-server penetration testing framework that automates vulnerability detection by cross-referencing IoT node states with the National Vulnerability Database (NVD) [20].
- **IoT-Scan:** A modular, software-defined radio (SDR) reconnaissance tool designed to enumerate and evaluate IoT gadgets

communicating via non-IP protocols, including ZigBee, Z-Wave, and Bluetooth Low Energy (BLE) [21].

Passive Monitoring and Machine Learning Methods

Passive monitoring is a non-intrusive security approach that evaluates network health and identifies threats without injecting packets or disrupting device operations [22]. The core principle relies on traffic analysis and behavior fingerprinting, where specialized sensors monitor network traces to derive statistical information. Passive systems determine the source device and its purpose by calculating flow-level characteristics, including packet sizes, inter-arrival times (IAT), and transmission order [23]. Contemporary surveys note that this method is especially useful for locating "headless" devices or those with low resources that store data internally rather than transmitting it frequently.

To convert observed patterns into actionable security intelligence, recent studies have incorporated various Machine Learning (ML) and Deep Learning (DL) architectures:

Integrated Architectures

- **Random Forest (RF):** Frequently employed for its robustness against data variance, RF uses a collection of decision trees to provide high classification rates in detecting botnet activities and Denial-of-Service (DoS) attempts [24].
- **Support Vector Machines (SVM):** SVMs are renowned for handling high-dimensional data, using kernel-based methods to identify the optimal hyperplane for differentiating between normal behavior and malicious outliers [25].
- **Deep Learning (DL):** Advanced architectures, including Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM), are unique in their ability to learn hierarchical and temporal patterns in network traffic from large-scale, complex datasets [26].

The primary advantage of passive monitoring is its stealth; since it transmits no active probes, it remains transparent to attackers and independent of the target hardware. Moreover, ML-based anomaly detection can identify zero-day exploits that signature-based approaches miss by detecting minor deviations from established behavioral baselines [27]. This enables the identification of advanced attacks, such as Man-in-the-Middle (MitM) and volumetric DDoS, before they cause system downtime.

However, passive ML-based solutions face significant implementation hurdles. A major challenge is the computational cost; training and executing complex deep learning models often requires high-performance GPUs and memory resources unavailable on standard edge gateways. Furthermore, these systems frequently suffer from high False Positive Rates (FPR), where benign but rare network signals are misclassified as malicious, leading to alert fatigue [28]. Finally, effective model training requires massive, heterogeneous, and well-labeled datasets such as the recently published CIC-IoT 2023—to ensure generalization across diverse environments [29]. Future research must focus on streamlining these algorithms into lightweight frameworks deployable on edge nodes.

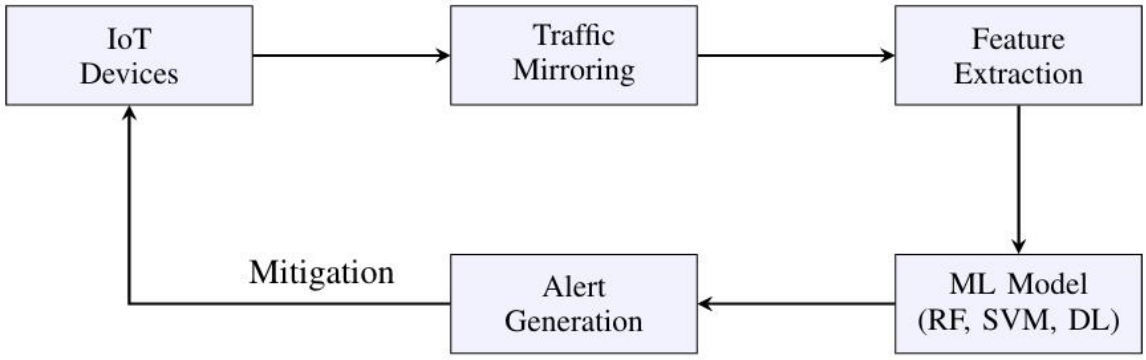

Figure 3: Workflow of a Passive Machine Learning-based Intrusion Detection System (IDS).

IoT Protocol Vulnerabilities

The Internet of Things is often designed with lightweight, low-power constraints rather than robust security, making standard application layer protocols highly vulnerable. Two of the most critical protocols, Message Queuing Telemetry Transport (MQTT) and Real-Time Streaming Protocol (RTSP), are vital for data flow but contain significant security loopholes when misconfigured.

Security Risks of Unencrypted MQTT (Port 1883)

MQTT is designed for minimal data overhead. While the protocol natively supports SSL/TLS encryption on Port 8883, IoT manufacturers frequently omit authentication and default to the unencrypted Port 1883 to save processing power [30]. In this standard configuration, usernames and passwords are transmitted in plaintext, allowing attackers to intercept credentials using packet analysis tools like Wireshark. Furthermore, the protocol's feature set includes "wildcard" subscriptions (e.g., "#"), which unauthorized actors can exploit to subscribe to all data flows passing through a broker or retrieve sensitive system metrics via the "$SYS" topic [31]. Since Port 1883 lacks integrity checks, attackers can also inject spoofed packets to manipulate sensor readings or send malicious control commands to actuators [32].

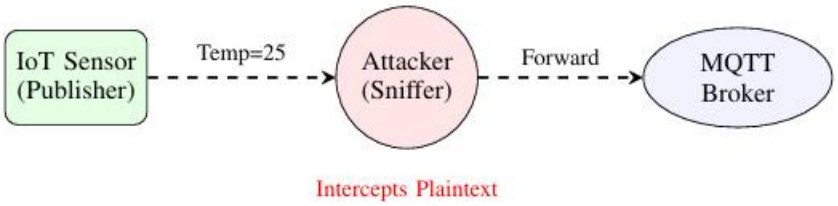

Figure 4: Attack Scenario: An attacker intercepting unencrypted MQTT traffic on Port 1883.

Vulnerabilities in RTSP (Port 554) and IP Cameras

RTSP, commonly used in IP surveillance, is frequently compromised due to misconfigured access controls rather than inherent protocol flaws. Attackers can often hijack live video streams by accessing the stream URL directly because vendors fail to enforce basic authentication mechanisms during initial setup [33]. Additionally, RTSP services often expose unauthenticated web interfaces for initial device configuration, leaving them open to

remote takeover. Legacy surveillance servers using RTSP also remain susceptible to known protocol vulnerabilities if firmware is unpatched [34].

Protocol Targeting by Botnets

These protocol vulnerabilities are actively weaponized by botnets like Mirai, which target devices using hardcoded or default passwords particularly on IP cameras and routers. MQTT and RTSP services are frequent targets for automated credential-stuffing attacks. Once infected, these devices are coordinated to launch massive volumetric DDoS attacks, leveraging their stable uptime and bandwidth to disrupt critical internet infrastructure. Default ports (1883 and 554) allow attackers to programmatically locate millions of vulnerable endpoints via search engines like Shodan, facilitating rapid botnet scaling [35].

Challenges and Future Research Directions

Gap 1: Lightweight, Deterministic Tools for Edge Devices

A primary research challenge is the lack of lightweight, deterministic scanners capable of running on typical edge devices. Current advanced vulnerability detection models largely rely on Deep Learning (DL) architectures that demand significant memory, storage, and processing power resources often unavailable on standard IoT gateways [36]. While some lightweight models exist, they often rely on simplified operations that fail to detect multi-phase attack vectors. There is an urgent need for resource-efficient algorithms that achieve high detection fidelity within the energy and hardware constraints of field-deployed edge nodes.

Gap 2: Inconsistency in Modern IoT Protocol Detection

Modern IoT protocols are highly heterogeneous, leading to significant inconsistencies in detection by current scanners [37]. While standard tools effectively handle HTTP and MQTT, they lack robust implementations for specialized or low-power protocols such as CoAP, AMQP, Zigbee, and Bluetooth Low Energy (BLE). Furthermore, temporally varying probe responses caused by changing firmware versions or user configurations can lead to static discovery signatures undercounting the vulnerable population by up to 37 times. Future studies must develop temporally resistant signatures capable of identifying devices across diverse protocols as network characteristics evolve.

Gap 3: The Trade-off Between Scan Speed and Accuracy

Automated IoT security faces a fundamental trade-off between scan speed and accuracy [38]. Superficial scanners offer internet-scale enumeration speeds but lack the depth to detect intricate firmware bugs. Conversely, analytical techniques like emulation-based firmware analysis provide high-fidelity evidence of exploitability but are too computationally intensive for continuous edge operation [39]. This imbalance often results in high false positive rates or the inability to detect unknown zero-day exploits in time-sensitive environments [40].

Future Direction: Hybrid Active Scanning Engine

To address these structural gaps, a hybrid active scanning engine is required one that combines distinct detection paradigms into a unified framework [41]. Such an engine could

deliver high-fidelity security intelligence without the prohibitive latency of deep inspection by integrating deterministic, signature-based threat detection with adaptive machine learning for anomaly identification [42]. This mixed methodology is crucial for achieving real-time threat detection and scalable protection in the fragmented and rapidly changing IoT ecosystem [43].

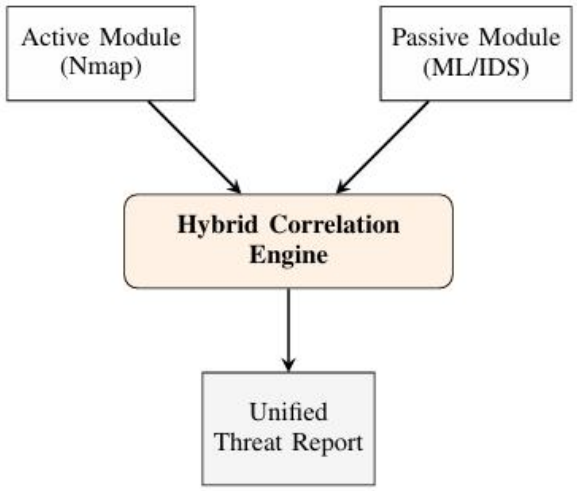

Figure 5: Proposed architecture for a Hybrid Active Scanning Engine.

Comparative Study of Key IoT Security Research

Table I presents a comparative analysis of ten pivotal studies from the literature, highlighting their primary techniques, contributions, and limitations.

Comparative Analysis of Key IoT Security Studies (2023–2025)

Ref.	Technique	Key Contribution	Limitation
	1D CNN	Scalable IDS for real-time threat detection using CIC IoT-DIAD 2024.	Requires substantial labeled training data; struggles with highly mutated zero-day attacks.
	Framework	Theoretical framework for vulnerability scanning in smart homes.	Lacks direct empirical validation in live environments.
	Active Probing	Algorithm for automated inference of field-deployed PLCs.	Relies on cached search engine snapshots.
	Passive Sensing	System to fingerprint concealed IoT devices via unintentional emanations.	Limited detection range; coarse localization.
	SBOM Scan	Solution to monitor inconsistencies in SBOM vulnerability scanners.	Restricted by delays in vulnerability database updates.

Ref.	Technique	Key Contribution	Limitation
	k-NN	Euclidean distance methods for MQTT-based intrusion detection.	Extremely limited device diversity (4 devices tested).
	Shodan Recon	Framework centered on Shodan to identify smart building vulnerabilities.	Cannot identify non-Internet-facing components.
	DL Models	Defense mechanism using deep learning on the CIC-IoT23 dataset.	Requires very high computational resources for training.
	LSTM	Temporal characteristics to detect malicious code in data flows.	High training complexity and slower execution times.
	Auth Protocols	Energy-efficient authentication model for resource-constrained nodes.	Authentication servers can create performance bottlenecks.

Conclusion

The investigation into IoT security mechanisms reveals a critical tension between the accuracy of resource-intensive machine learning models and the efficiency of deterministic active scanning. While active probing remains the most feasible approach for immediate device enumeration on edge-level hardware, its vulnerability to outdated signatures and protocol heterogeneity limits long-term efficacy. Conversely, passive monitoring provides a stealthy alternative but demands computational resources far exceeding the capabilities of standard domestic gateways. To address the rapidly evolving threat landscape, future research must prioritize the development of hybrid engines that unify signature-based detection with adaptive behavioral analysis. Such systems will enable real-time, lightweight security audits that are essential for securing the fragmented IoT ecosystem.

References

1) Amro, Ahmed. "IoT vulnerability scanning: A state of the art." *International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems*. Cham: Springer International Publishing, 2020. https://link.springer.com/chapter/10.1007/978-3-030-64330-0_6
2) Raghuvanshi, Abhishek, et al. "Internet of Things: Security vulnerabilities and countermeasures." *Electrochemical Society Transactions* 107.1 (2022): 15043-15052. https://iopscience.iop.org/article/10.1149/10701.15043ecst/meta
3) Statista. (2022). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*. Statista Research Department. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
4) NIST. (2020). *Foundational Cybersecurity Activities for IoT Device Manufacturers* (NISTIR 8259). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259
5) Williams, P., et al. (2022). A survey on security in internet of things with a focus

on the impact of emerging technologies. *Internet of Things, 19*, 100564. https://doi.org/10.1016/j.iot.2022.100564

6) Anand, P., et al. (2020). IoT vulnerability assessment for sustainable computing: Threats, current solutions, and open challenges. *IEEE Access, 8*, 168825–168853. https://doi.org/10.1109/ACCESS.2020.3022842
7) ISO/IEC. (2022). *Internet of things (IoT) – Cybersecurity and privacy guidelines* (ISO/IEC 27400:2022). https://www.iso.org/standard/74147.html
8) Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors, 21*(5), 1809. https://www.mdpi.com/1424-8220/21/5/1809
9) Matheu, S. N., Robles, T., & Skarmeta, A. F. (2020). A survey of cybersecurity certification for the Internet of Things. *IEEE Access, 8*, 182701-182736. https://doi.org/10.1109/ACCESS.2020.3027639
10) Shodan. (2025, February 10). *The search engine for the Internet of Things*. https://www.shodan.io/
11) Verma, Shikhar, Yuichi Kawamoto, and Nei Kato. "A smart Internet-wide port scan approach for improving IoT security under dynamic WLAN environments." *IEEE Internet of Things Journal* 9.14 (2021): 11951-11961. https://ieeexplore.ieee.org/abstract/document/9634163/
12) Gvozdenovic, Stefan, et al. "IoT-scan: Network reconnaissance for Internet of Things." *IEEE Internet of Things Journal* 11.8 (2023): 13091-13107. https://ieeexplore.ieee.org/abstract/document/10299538/
13) OWASP. (2024). *OWASP IoT top 10 vulnerabilities and mitigation strategies*. https://owasp.org/www-project-iot-top-10/
14) Lyon, G. (2024). *Nmap network scanning: The official Nmap project guide*. Insecure.com LLC. https://nmap.org/book/
15) Tenable. (2024). *Nessus vulnerability scanner product guide*. Tenable, Inc. https://docs.tenable.com/nessus/
16) Rachit, Shobha Bhatt, and Prakash Rao Ragiri. "Security trends in Internet of Things: A survey." *SN Applied Sciences* 3.1 (2021): 121. https://link.springer.com/article/10.1007/s42452-021-04156-9
17) SonicWall. (2023). *2023 SonicWall Cyber Threat Report*. (Provides real data on the spike in IoT malware attacks). https://www.sonicwall.com/threatreport
18) Pickren, C., et al. (2024). PLCHound: Automated inference of field-deployed PLCs. *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 145–159. https://doi.org/10.1145/3658644
19) Koroniotis, N., et al. (2021). A deep learning-based penetration testing framework for IoT. *IEEE 20th TrustCom*, 1–8.

https://doi.org/10.1109/TrustCom53322.2021.00032

20) Lounis, K., & Roig, C. (2020). A penetration testing methodology for IoT. *In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20)*, 1-10. https://doi.org/10.1145/3407023.3409062

21) Rizvi, Syed, et al. "Threat model for securing internet of things (IoT) network at device-level." *Internet of Things* 11 (2020): 100240. https://www.sciencedirect.com/science/article/pii/S2542660520300731

22) Alsoufi, M. A., et al. (2021). Anomaly-based intrusion detection systems in IoT using deep learning. *Applied Sciences, 11*(18), 8383. https://doi.org/10.3390/app11188383

23) Ferrag, M. A., et al. (2020). Deep learning for cyber security intrusion detection. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

24) Tahaei, H., et al. (2022). A survey on intrusion detection systems for IoT. *IEEE Communications Surveys & Tutorials, 24*(1), 153–196. https://doi.org/10.1109/COMST.2021.3134954

25) Siwakoti, Yuba Raj, et al. "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures." *IEEE Internet of Things Journal* 10.13 (2023): 11224-11239. https://ieeexplore.ieee.org/abstract/document/10059147/

26) Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information*, 11(5), 279. https://doi.org/10.3390/info11050279

27) Elkhadir, Z., & Begdouri, M. A. (2025). Enhancing iot security: A comparative analysis of preprocessing techniques and classifier performance on iot23 and cic iot 2023 datasets. *IAENG International Journal of Computer Science, 52*(4). https://www.iaeng.org/IJCS/issues_v52/issue_4/IJCS_52_4_11.pdf

28) Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646-1685. https://ieeexplore.ieee.org/document/10103444

29) Neto, E. C. P. (2023). CICIoT2023: A real-time dataset for IoT cybersecurity. *2023 IEEE International Conference on Big Data*, 340–349. https://www.unb.ca/cic/datasets/iotdataset-2023.html

30) Rajmohan, Tanusan, Phu H. Nguyen, and Nicolas Ferry. "A decade of research on patterns and architectures for IoT security." *Cybersecurity* 5.1 (2022): 2. https://link.springer.com/article/10.1186/s42400-021-00104-7

31) Meziane, H., & Ouerdi, N. (2023). A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems. *Scientific reports, 13*(1), 21255. https://www.nature.com/articles/s41598-023-46640-9

32) Hindy, H., Brosset, D., Bures, M., Bellekens, X., & Michaeli, C. (2020). A taxonomy of IoT malware and MQTT attacks. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1-8. https://doi.org/10.1109/CyberSA49311.2020.9139644

33) Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A review of security and privacy concerns in the internet of things (IoT). *Journal of sensors*, *2022*(1), 5724168. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/5724168

34) Ibrahim, M., Continella, A., & Bianchi, A. (2023, July). Aot-attack on things: A security analysis of iot firmware updates. In *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)* (pp. 1047-1064). IEEE. https://ieeexplore.ieee.org/abstract/document/10190484/

35) Khadka, G., Ray, B., Karmakar, N. C., & Choi, J. (2022). Physical-layer detection and security of printed chipless RFID tag for Internet of Things applications. *IEEE Internet of Things Journal*, *9*(17), 15714-15724. https://ieeexplore.ieee.org/abstract/document/9714268/

36) Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S., Rehman, A., & Bharany, S. (2024). Navigating IoT security: insights into architecture, key security features, attacks, current challenges and AI-driven solutions shaping the future of connectivity. *Computers, Materials, & Continua*, *81*(3), 3499. https://www.researchgate.net/profile/Ateeq-Rehman-20/publication/386210978_Navigating_IoT_Security_Insights_into_Architecture_Key_Security_Features_Attacks_Current_Challenges_and_AI

37) Microsoft Security. (2024). *IoT device heterogeneity and security management*. https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/

38) Khalil, U., Malik, O. A., & Hussain, S. (2022). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. *IEEE Access*, *10*, 76805-76823. https://ieeexplore.ieee.org/abstract/document/9827661/

39) Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of things: Security and solutions survey. *Sensors*, *22*(19), 7433. https://www.mdpi.com/1424-8220/22/19/7433

40) Mazhar, M. S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M. H., Rehman, A. U., ... & Hamam, H. (2022). Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, *11*(7), 1126. https://www.mdpi.com/2079-9292/11/7/1126

41) Irshad, R. R., Sohail, S. S., Hussain, S., Madsen, D. Ø., Zamani, A. S., Ahmed, A. A. A., ... & Alwayle, I. M. (2023). Towards enhancing security of IoT-Enabled healthcare system. *Heliyon*, *9*(11).

https://www.cell.com/heliyon/fulltext/S2405-8440(23)09544-0

42) Safkhani, M., et al. (2021). A novel lightweight authentication protocol. *IEEE Internet of Things Journal*, *8*(6), 4820–4832. https://doi.org/10.1109/JIOT.2020.3023246

43) Bou-Harb, E., et al. (2021). On the accuracy of IoT search engines. *IEEE Communications Magazine*, *59*(12), 100–106. https://doi.org/10.1109/MCOM.001.2100345