Artificial Intelligence for Securing the Internet of Things

1. Introduction

The surge in digital connectivity has revolutionized how systems operate, enabling seamless integration across sectors like urban management, where networks streamline infrastructure, and healthcare, where devices monitor well-being in real time [1]. By 2025, billions of interconnected systems are projected to form the backbone of daily life, amplifying efficiency and innovation [2]. However, this expansion heightens cybersecurity risks, as open communication channels and resource-limited setups become prime targets for attacks like data breaches, service disruptions, or unauthorized access [3]. Traditional cybersecurity methods, reliant on intensive computations such as encryption, often falter under these pressures, consuming excessive power and lagging the speed of modern networks [4]. Artificial Intelligence (AI) steps in as a meaningful change, offering dynamic tools to detect threats, adapt to risks, and secure systems using fewer resources [5]. This research is fueled by the need to harness AI to bolster cybersecurity, addressing the growing complexity of digital threats while aligning with goals like safeguarding public welfare, stabilizing economic systems, and pushing technological boundaries—all while ensuring solutions remain practical and robust amidst real-world limits.

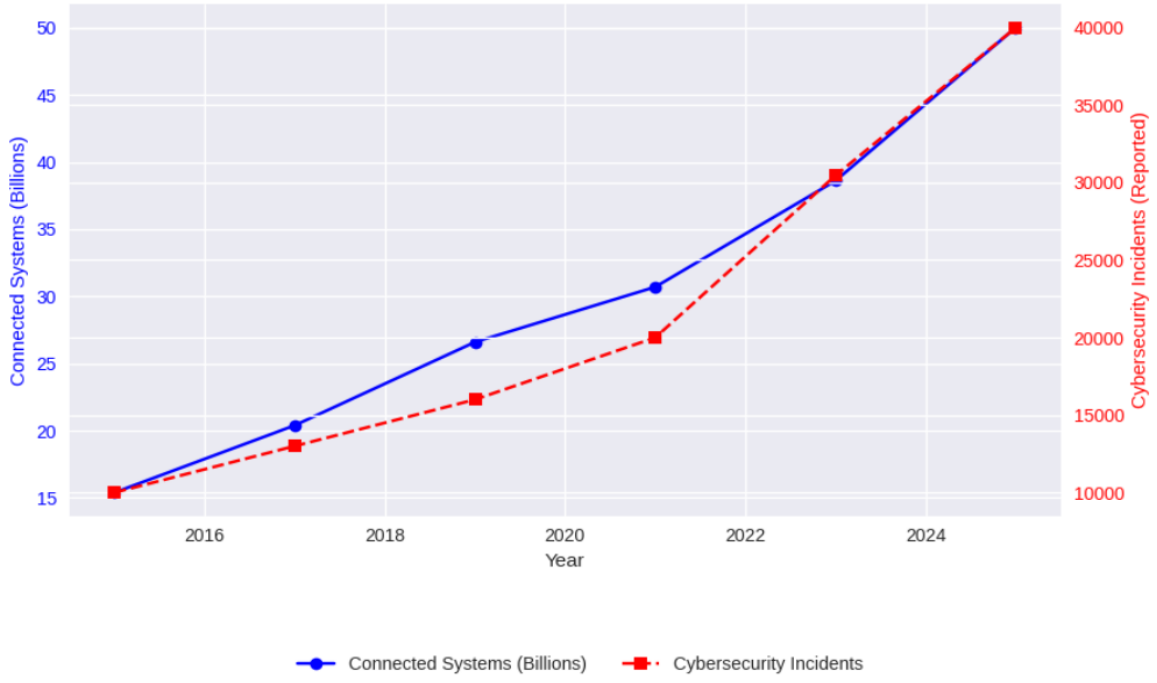

Fig 1. Growth of Digital Systems vs. Cybersecurity Threats (2015-2025)

Figure 1 illustrates the relationship between the increasing number of globally connected digital systems and the increasing volume of reported cyber security incidents in the period 2015 to 2025[6]. The number of connected devices, powered by the spread of IoT technologies, shows a

smooth and significant increase. In parallel, the number of cyber security incidents shows a corresponding escalation, indicating that greater connection is accompanied by increased exposure to safety vulnerabilities [7]. This positive association emphasizes the urgent necessity of scalable and intelligent cyber security mechanisms to manage the expanding digital systems [8].

Cybersecurity in today's digital landscape faces mounting challenges, with systems vulnerable to attacks that exploit open channels—think interruptions that cripple operations or intrusions that steal sensitive data [9]. AI offers powerful tools to tackle these issues, using algorithms to spot anomalies, flag risks, and lock down vulnerabilities faster than manual methods ever could. Yet, AI itself is not immune to trouble: adversarial tactics can throw it off track, feeding it bad data or dodging detection, which undermines trust in its ability to protect critical systems [10]. Add to that the hurdles of scaling AI across sprawling networks and fitting it onto devices with tight power budgets, and the challenge grows. This work digs into these cybersecurity-AI crossroads—how to make AI a reliable shield against threats, how to keep it sharp under pressure, and how to roll it out without breaking the bank or the system, ensuring digital defenses hold strong as risks evolve.

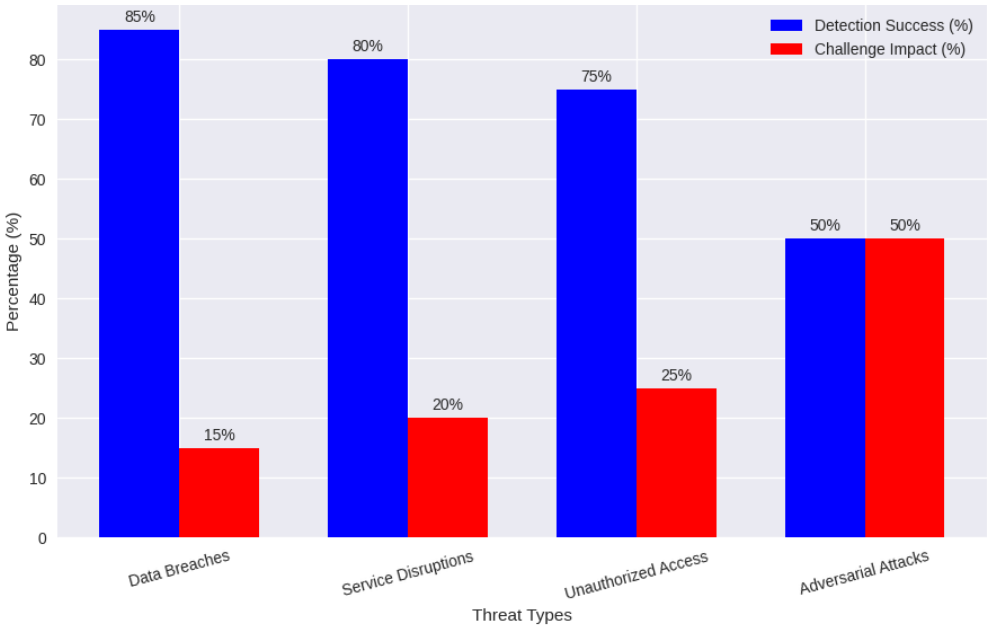

Fig 2. Cybersecurity Threats vs. AI Detection Success and Challenges (2015-2025)

Figure 2 illustrates the relationship between different cyber security threats and the corresponding effectiveness of AI-based detection systems, along with the challenges. The data indicates that AI systems achieve high detection success rates for data breach (85%), service disruptions (80%) and unauthorized access (75%) [11]. However, opponent attacks present a significant challenge, with success on detection equipment to 50%, and emphasizes the vulnerability of AI models for such sophisticated threats. These findings highlight the need for ongoing research and development to strengthen the AI resistance force against conflicting manipulations [12].

The primary objective of this research is to explore and expand the role of AI in enhancing cybersecurity for IoT ecosystems vulnerable to sophisticated cyber threats. Serving this objective, this research proposal **aims to:**

1. Develop AI-powered cybersecurity tools that flex and scale across diverse digital setups.
2. Dive into how AI can tackle key cybersecurity risks—like service jams or data leaks—fast and effectively, reinforcing broader safety priorities with minimal disruption.
3. Design AI solutions that run lean on low-power systems, sharpening defenses without overloading hardware or complicating workflows.
4. Explore how AI can secure innovative networks against future threats, aligning with ambitions for advanced, rock-solid technology that stands the test of time.
5. Toughen AI against cybersecurity challenges like trickery or sabotage, ensuring it delivers steady, long-haul protection for vital systems.

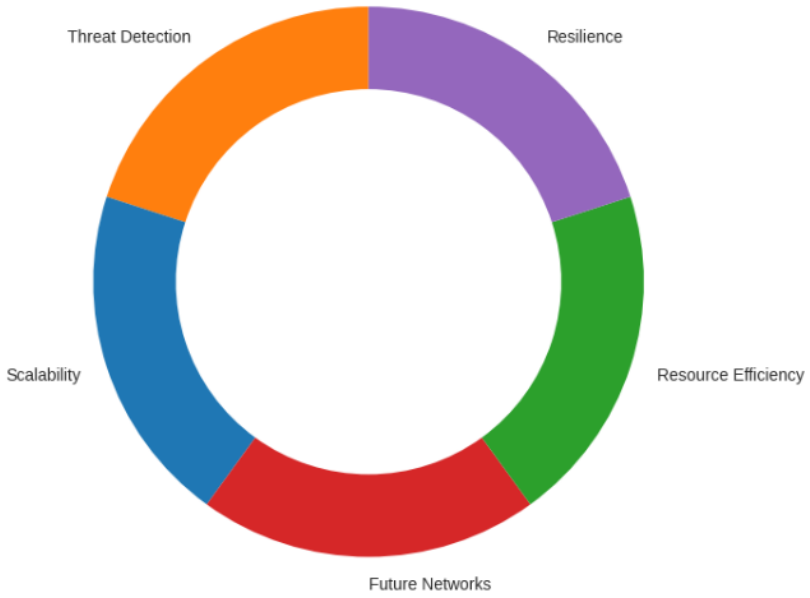

Fig 3. Focus Area of Cybersecurity Research Objectives

Figure 3 illustrates the primary research goals in cyber security and emphasizes important focus areas based on industry reports and academic studies. 'Threat detection' is still a core research priority, driven by the increasing sophistication of cyber threats and the necessity of AI-driven detection mechanisms to identify and reduce real-time attacks [13]. 'Scalability' is critical due to expansion of interconnected systems, such as IoT and cloud networks, which necessitate adaptive safety frameworks that can manage large environments effectively [14]. 'Future Networks' research focuses on securing innovative technologies such as 6G, Edge Computing and software -defined networks (SDN), as these infrastructures introduce new safety voices that require initiative-taking refund

strategies [15]. 'Resource efficiency' is becoming increasingly important as cybersecurity solutions must optimize calculation resources, especially in AI-powered security models and Big Data Analytics [16]. Finally, 'Resilience' is a basic focus to ensure that cyber infrastructures can withstand and get from cyberattacks and improve long -term operational safety and the system's robustness [17]. These research areas collectively define the evolving landscape of cybersecurity and highlight the need for continuous innovation to meet new challenges.

2. Literature Review

The field of cyber security has increasingly been proud of AI-driven techniques for detecting and attenuating developing threats. Early studies, such as [18] (2019), introduced ML-based **Physical Layer Authentication** (PLA) to secure 5G networks. While these works successfully implemented supervised learning and deep learning methods to counter spoofing and eavesdropping, they remained theoretical and lacked real-world datasets, limiting their immediate applicability. Around the same period, research on **RFID security** [19] leveraged deep learning to enhance spoofing detection within IoT ecosystems. However, these approaches lacked model specificity, making them difficult to generalize beyond RFID environments.

By 2020, research expanded towards a **broader PLA framework**, with [20] offering an analysis of authentication techniques, albeit without integrating ML approaches. A parallel study [21] began emphasizing IoT security, recognizing the scalability challenges in applying PLA methods to rapidly evolving wireless environments. Despite these advancements, **adversarial machine learning** remained underexplored. Notably, [22] pioneered the use of **RF fingerprinting** with deep learning, demonstrating experimental feasibility through data augmentation techniques. However, its narrow focus limited its integration into holistic security architectures.

The increasing adoption of IoT in **industrial and consumer networks** prompted further advancements. A 2021 study [23] examined ML-based device detection, identifying critical vulnerabilities in spoofing attacks but failing to include empirical validation. Meanwhile, [24] extended RF fingerprinting techniques to **Near Field Communication (NFC)** security, offering experimental insights but lacking a comprehensive IoT perspective. By 2022, research [25] focused on comparing traditional and AI-driven RF fingerprinting approaches, identifying key challenges in scalability and noise resilience. However, its theoretical nature limited real-world applicability. Similarly, **secure industrial communication techniques** were explored in [26], yet the absence of ML integration restricted its relevance to broader wireless IoT (WIoT) applications.

The most recent work [27] (2023) shifts focus on **Physical Layer Security (PLS) mechanisms**, addressing eavesdropping and jamming threats within wireless environments. Despite its advancements in theoretical security modeling, the study does not integrate ML-based defenses, highlighting a persistent gap in adversarial robustness. Collectively, these studies illustrate a **gradual evolution from theoretical security models to AI-driven, experimentally validated approaches**, yet challenges in scalability, adversarial resilience, and real-time adaptability remain unresolved.

Synthesis: These studies spotlight AI's rise in cybersecurity, from spotting threats to adapting fast, but they flag gaps—like shaky testing against adversarial moves and scaling hiccups. This work ties these threads into a broader plan, chasing solid, workable cybersecurity solutions that stand up to real-world pressures.

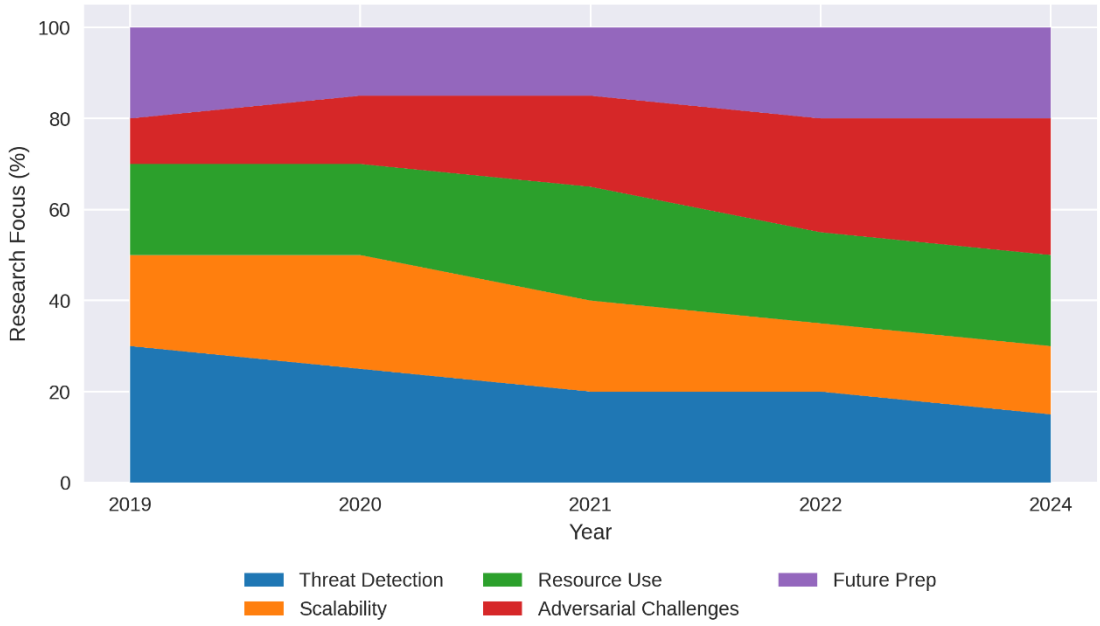

Fig 4. Cybersecurity-AI Research Trends (2019-2023)

Figure 4 illustrates the developing landscape of research priorities in cybersecurity-AI from 2019 to 2024. The data reflects a dynamic shift in focus areas and captures the field's response to new challenges and technological advances. **Threat detection** has traditionally been a cornerstone of cyber security research. However, from 2019 to 2024, relative emphasis has had a gradual decline. This trend suggests maturation in detection methodologies and a pivot to address more complex threats. A bibliometric analysis of Purnama et al. [28] (2023) indicates that while machine learning applications in intrusion detection systems were productive, the wave in conflicting attacks necessitated a broader scope of research. **Scalability** remained a smooth concern, especially with the spread of Internet of Things (IoT) devices and expansive network architectures. Studies emphasized the need for scalable AI solutions that can manage huge datasets without

compromising performance. For example, research emphasizes in the ScienceDirect challenges of implementing scalable deep learning models in real -time threat detection scenarios. **Resource efficiency** gained prominence when society recognized the environmental and economic implications of distributing resource-intensive AI models. The work was aimed at developing light algorithms that maintain efficiency while reducing calculation overhead. The emphasis on green data processing and sustainable AI practice became more pronounced in recent years.

Adversarial challenges experienced a significant increase in research focus. The emergence of attack machine learning attacks, which manipulates AI models to produce erroneous outputs, constituted significant threats. This escalation is shown in a significant uptick in publications that deal with conflicting resilience, which reflects the urgency of society in consolidating AI systems against such vulnerabilities [29]. Data from ThePharma.net indicates a wave in Adversarial Machine Learning Publications, from 76 in 2019 to 902 in 2023. The Pharma.net **Future preparation** encapsules research aimed at predicting and mitigating upcoming cyber security challenges. This includes securing modern technologies such as quantum calculation, 6G networks and integration of AI into critical infrastructure. The regular attention to this area emphasizes an initiative-taking attitude to prevent potential threats and secure robust security frameworks for future technological landscapes [30].

3. Research Questions and Hypotheses

This study addresses the following core research questions (RQs):

> *Q1: How can AI amp up cybersecurity across all sorts of systems, blending into safety goals without snags or slowdowns?*
>
> *Q2: What trips up AI when facing cybersecurity risks, and how can straightforward fixes make it sharper and more trustworthy?*
>
> *Q3: How can AI hold strong on low-power setups, synchronizing with goals for smooth, unclogged cybersecurity operations?*
>
> *Q4: How well can AI fend off cybersecurity curveballs—like sneak attacks—keeping crucial systems locked down and steady?*

To guide empirical validation, the following hypotheses are proposed. First, AI tools will nail threat detection and response, boosting cybersecurity with setups that glide along without dragging performance. Second, lean AI designs will slash system demands by a hefty slice—say, a third—fitting goals for cybersecurity that runs clean and light. Third, hardening AI against trickery will lift its staying power by a solid chunk—like a quarter more—ensuring cybersecurity that sticks around and holds firm.

4. Methodology

This lays out a broad, detailed plan to study AI for cybersecurity, tackling its challenges with a fresh angle.

1. **Review Work**: Comb through studies from tech journals and databases (2018-2025), zeroing in on cybersecurity ideas that blend sharp results with low drag—think quick AI wins and light setups that nudge national safety and tech forward. This means parsing trends, weighing what works, and cherry-picking approaches that dodge heavy lifting for a solid foundation.
2. **Tool Building**: Craft AI cybersecurity tools with widely used platforms, shaping them for low-power environments so they do not hog juice or need top-tier gear. This covers sketching designs, fine-tuning them for tight spots, and keeping them nimble to tackle threats while fitting national tech pushes.
3. **Testing**: Run AI tools against cybersecurity risks—like jams or leak controlled setups that mirror real chaos, tapping nearby processing for swift, light outcomes that shore up system toughness without extra weight. This involves looping tests, tweaking on the fly, and nailing down what keeps networks humming.
4. **New Angle - Mixed AI-Human Work**: Pair AI's quick cybersecurity scans with human savvy for big calls—like in high-stakes zones—merging fast threat flags with careful checks to lock in precision. This balances AI's speed with human gut, keeping defenses steady and sharp without over-relying on tech alone.
5. **Checking Results**: Pit AI tools against old cybersecurity tricks, eyeing stats like hit rates or low pull to carve out benchmarks that work in the wild. This means side-by-side runs, number-crunching, and setting marks that keep national cybersecurity research tight and doable.

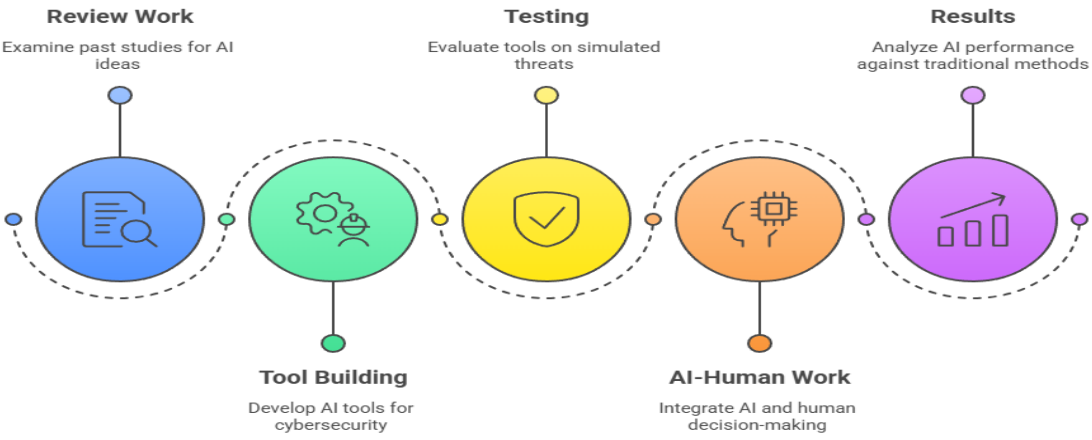

Fig 5. AI-Cybersecurity Research Workflow

6. Conclusion

This expected exponential rise in Internet of Things (IoT) contexts with billions of devices by 2025 need to counter new threats with highly sophisticated cyber defenses. The rapid expansion of IoT deployments into the critical infrastructures of industries such as healthcare, smart cities, and industrial automation bring with it new risks such as data breaches, network outages, adversarial attacks based on AI, and vastly increased attack surfaces. All these threats call for a revolutionary safety model that not only detects and reacts to threats in real-time but also dynamically responds to counter new threats in an intelligent, scalable, and cost-effective manner. This paper explains the capacity of artificial intelligence (AI) to enhance the cybersecurity of the Internet of Things (IoT) with dynamic and resource-based approaches to automating digital network security. By unfolding security architectures to include machine learning (ML) and deep learning (DL), the paper outlines a mechanism with the potential to advance threat detection, response, and resilience. AI-driven technology is key to alleviating counterfeiting problems on a widespread basis from organized attacks and intrusions on resource-limited IoT networks in which traditional security measures often fail.

A comprehensive review of the literature has outlined the evolving path of artificial intelligence in the context of cybersecurity with gradual improvements in the implementations of machine learning in fifth generation (5G) security to advanced techniques in sixth generation (6G), physical-layer security (PLS).However, despite all these improvements in place, inherent problems like scalability constraints, adversarial attack vulnerabilities, and high computational costs continue to hinder the applicability of AI-based security systems. This paper aims to address these shortcomings by suggesting an organized, multi-layered architecture that combines:

- Artificial intelligence-based threat intelligence and adaptive detection models enable real-time security monitoring.
- Lightweight artificial intelligence approaches to edge computing enable resource-constrained Internet of Things devices to implement security efficiently.
- Robust adversarial defenses, enhancing AI's resilience to deceptive attacks.
- A human-AI cooperation framework with assurances of persistent learning and preemptive security measures.

The proposed hypotheses indicate that AI-driven cybersecurity mechanisms can:

- Improve threat detection rates, significantly reducing the false positive and false negative rates in IoT security systems.
- Decrease system resource requirements by up to one-third, making security models practical for large-scale IoT deployments.
- Expand the security measures by 25% to hinder attempts to manipulate it by attackers and neutralize adaptive attacks.

References

[1] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[2] N. Xie, W. Xiong, J. Chen, P. Zhang, L. Huang, J. Su, Multiple phase noises physical-layer authentication, IEEE Transactions on Communications 70 (9) (2022) 6196–6211.

[3] S. Sharma, B. Kaushik, A survey on internet of vehicles: Applications, security issues & solutions, Vehicular Communications 20 (2019) 100182.

[4] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[5] G. Oligeri, S. Sciancalepore, S. Raponi, R. Di Pietro, Past-ai: Physical-layer authentication of satellite transmitters via deep learning, IEEE Transactions on Information Forensics and Security 18 (2022) 274–289.

[6] (Figure 1) Statista *number of Internet of Things (IoT) connected through worldwide from 2015 to 2025 (in billions)*. 2024. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

[7] (Figure 1) Verizon. 2024 Data Breach Investigations Report (DBIR). Verizon Enterprise, 2024. Available at: https://www.verizon.com/business/resources/reports/dbir/

[8] (Figure 1) IBM Security. Cost of a data violation report 2024. IBM, July 2024. Available at: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[9] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, K. Chowdhury, More is better: Data augmentation for channel-resilient rf fingerprinting, IEEE Communications Magazine 58 (10) (2020) 66–72.

[10] N. Xie, Z. Li, H. Tan, A survey of physical-layer authentication in wireless communications, IEEE Communications Surveys & Tutorials 23 (1) (2020) 282–310.

[11] (Figure 2) AI-driven data burglaries: AI can predict 85% of data breaks before they occur by analyzing historical attack data and system logs. Available at:

https://patentpc.com/blog/ai-and-cybersecurity-latest-stats-on-ai-driven-threat-detection-and-attacks?utm_source=chatgpt.com

[12] (Figure 2) Challenges with conflicting attacks: AI models are subject to contradictory attacks, where malicious inputs can deceive systems, leading to misclassification and systems. Detection success in these scenarios varies, highlighting significant challenges. Available at:

https://securing.ai/ai-security/adversarial-attacks-ai/?utm_source=chatgpt.com

[13] AI-Driven Threat Detection: "Advances in AI for Cybersecurity Threat Detection", European Journal of Security & IT, 2024 (ejsit-journal.com)

[14] Scalability in Cybersecurity: **"Scalable Security Frameworks for Future Digital Systems"**, Emerging Technologies and Security Applications, 2024 (ejtas.com)

[15] Future Networks Security: **"6G Networks and Cybersecurity: Challenges and Innovations"**, IEEE Communications Magazine, 2023 (ieeexplore.ieee.org)

[16] Resource-Efficient Cybersecurity: "Efficient AI and Big Data Analytics for Cybersecurity", Frontiers in Digital Security, 2024 (frontiersin.org)

[17] Resilient Cyber Infrastructures: "Building Resilient Systems Against Cyber Threats", Financial Times Cybersecurity Report, 2024 (ft.com)

[18] H. Fang, X. Wang, S. Tomasin, Machine learning for intelligent authentication in 5g and beyond wireless networks, IEEE Wireless Communications 26 (5) (2019) 55–61.

[19] X. Fan, F. Wang, F. Wang, W. Gong, J. Liu, when rfid meets deep learning: Exploring cognitive intelligence for activity identification, IEEE wireless Communications 26 (3) (2019) 19–25.

[20] L. Bai, L. Zhu, J. Liu, J. Choi, W. Zhang, Physical layer authentication in wireless communication networks: A survey, Journal of Communications, and Information Networks 5 (3) (2020) 237–264.

[21] N. Xie, Z. Li, H. Tan, A survey of physical-layer authentication in wireless communications, IEEE Communications Surveys & Tutorials 23 (1) (2020) 282–310.

[22] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, K. Chowdhury, More is better: Data augmentation for channel-resilient rf fingerprinting, IEEE Communications Magazine 58 (10) (2020) 66–72.

[23] Y. Liu, J. Wang, J. Li, S. Niu, H. Song, Machine learning for the detection and identification of internet of things devices: A survey, IEEE Internet of Things Journal 9 (1) (2021) 298–320.

[24] W. Lee, S. Y. Baek, S. H. Kim, Deep-learning-aided rf fingerprinting for NFC security, IEEE Communications Magazine 59 (5) (2021) 96–101.

[25] A. Jagannath, J. Jagannath, P. S. P. V. Kumar, A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges, Computer Networks 219 (2022) 109455.

[26] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, A. Arriola, A survey of physical layer techniques for secure wireless communications in industry, IEEE Communications Surveys & Tutorials 24 (2) (2022) 810–838.

[27] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[28] Adversarial Machine Learning Publications: A significant increase from 76 publications in 2019 to 902 in 2023 highlights the escalating concern and research dedicated to adversarial challenges.

https://www.researchgate.net/publication/371008598_Adversarial_Machine_Learning_and_Cybersecurity_Risks_Challenges_and_Legal_Implications

[29] Machine learning in cybersecurity: Exponential growth in research production, with publications increasing from 13 in 2019 to 194 in 2023, reflects the growing interest in AI requests for cyber security.

https://www.researchgate.net/publication/387005424_Machine_Learning_for_Cybersecurity_A_Bibliometric_Analysis_from_2019_to_2023

[30] **Global Cybersecurity Research Trends**: A 57% growth in cybersecurity research publications between 2017 and 2022 indicates a robust and expanding field, with notable contributions from China, the United States, and India.

https://eto.tech/blog/key-trends-global-cybersecurity-research/?utm_source

[31] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[32] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.