AI-enabled Cybersecurity in the Internet of Things

David Wu
Mount Paran Christian School
Kennesaw, GA USA
dwu26@mpcstudent.com

Vijay Anand, Amelia Estwick, Honghui Xu
Department of Information Technology
Kennesaw State University
Kennesaw, GA USA
{vanand1, aestwick, hxu10}@kennesaw.edu

***Abstract*—The Internet of Things (IoT) is transforming industries such as healthcare, smart cities, and industrial systems by enabling interconnected devices to generate and process vast amounts of data. However, the proliferation of IoT introduces significant challenges related to privacy and security due to resource constraints, heterogeneous architectures, and the evolving threat landscape. In recent years, AI has been deeply employed to address IoT Cybersecurity. This paper provides a comprehensive overview of AI and Machine Learning (ML) enabled IoT cybersecurity, covering topics from traditional machine learning, deep learning, federated learning, Large Language Model (LLM) to edge computing in addressing IoT security. This review strives to present a snapshot of the most recent advancement in AI-enabled IoT cybersecurity literacy.**

***Index Terms*—Internet of Things, Cybersecurity.**

I. Introduction

The rapid proliferation of the IoT has revolutionized industries such as healthcare [1], manufacturing [2], smart cities [3], and energy systems [4] by enabling seamless connectivity and data-driven decision-making. IoT systems integrate diverse devices and sensors to generate, process, and exchange vast amounts of data, fostering innovation and operational efficiency. These advancements have led to breakthroughs in applications such as remote patient monitoring, predictive maintenance, intelligent transportation systems, and smart microgrids, offering unprecedented convenience and scalability across multiple domains.

However, the widespread adoption of IoT technologies has introduced significant privacy and security challenges [5]. IoT devices often operate in heterogeneous environments with constrained computational resources, making them vulnerable to various attacks, including adversarial threats, ransomware, and data breaches [6]. The integration of legacy systems into modern IoT architectures further exacerbates these vulnerabilities by exposing critical infrastructure to advanced persistent threats (APTs) [7]–[9]. Additionally, the decentralized and interconnected nature of IoT ecosystems creates unique challenges in ensuring data integrity, privacy, and security while maintaining system scalability and performance [10], [11].

To address these challenges, emerging technologies such as AI [12], [13], blockchain [14], [15], and edge computing [16], [17] have been proposed to enhance IoT cybersecurity. AI enables model training to improve data privacy without exposing raw data, while blockchain enhances trust and transparency through immutable ledgers. Edge computing brings computation closer to the source, reducing latency and offloading tasks from centralized servers.

In this paper, we provide a comprehensive survey of the literacy of applying AI for IoT cybersecurity, focusing on privacy and security challenges, emerging technologies, and innovative solutions to address these issues, with a significant focus on the Large Language Models (LLMs) for IoT cybersecurity.

The remainder of this paper is organized as follows. Section II summarizes IoT security essentials. Then, Section III comprehensively presents various AI models used to address IoT cybersecurity. Finally, this paper is concluded in Section IV.

II. Cybersecurity Essentials in IoT

In this section, we review critical security and privacy issues in IoT growth, focusing on vulnerabilities, mitigation strategies, and mechanisms to foster trust and resilience in IoT ecosystems.

A. Security in IoT

The rapid growth of IoT devices has exposed numerous security vulnerabilities across consumer, commercial, and industrial domains [7]. These include threats such as DoS attacks and data breaches, which require scalable cybersecurity frameworks capable of handling the vast amounts of information generated by IoT systems [8]. Advanced authentication mechanisms, such as iris-based biometric methods, have been proposed to replace traditional text-based credentials. These methods, utilizing multi-algorithm fusion, demonstrate high accuracy and negligible processing delay, offering both enhanced security and user convenience [9]. However, their integration into IoT systems requires extensive testing for compatibility with various protocols, network conditions, and concurrent user scenarios to ensure scalability and reliability.

To further strengthen IoT security, practical testbeds have been introduced, incorporating hybrid architectures of Ethernet, wireless, and SDN. These testbeds enable hands-on exploration of IoT vulnerabilities through exercises such as anomaly detection, honeypot implementation, and network traffic analysis. This hands-on approach bridges the gap between theoretical insights and real-world applications, fostering innovation in IoT security [18].

B. Privacy in IoT

Privacy is a critical concern in IoT, particularly in smart environments, where sensitive data is collected and transmitted.

979-8-3315-7111-5/26/$31.00 ©2026 IEEE

Ensuring data anonymization and secure multi-party computation is essential for building user trust, which is vital for the broader adoption of IoT technologies [19]. Mechanisms such as multi-stage AI systems have been proposed to enhance privacy by analyzing bandwidth usage and categorizing device behavior while safeguarding sensitive information [20]. These approaches aim to minimize privacy leakage by incorporating robust object identification and tracking systems.

However, addressing privacy challenges in IoT requires overcoming issues like false positives, resource limitations, and real-time data streams. Dynamic testing facilities are crucial for evaluating how privacy-preserving algorithms interact with other system components, ensuring effectiveness without compromising performance or scalability. By focusing on privacy preservation, IoT systems can prevent leakage of sensitive information, thereby fostering trust and enabling secure integration into diverse applications.

C. Penetration Testing

Penetration testing is essential for addressing IoT vulnerabilities. IoT-PEN, a tailored framework, tackles multi-host, multi-stage attack paths using a client-server architecture. Using the National Vulnerability Database (NVD) and target graphs, it maps exploitation routes and simulates real-world attacks like the Mirai botnet, offering actionable insights to strengthen defenses. Its modular and scalable design ensures applicability across diverse IoT deployments [21].

In addition, fuzzing complements IoT penetration testing by identifying vulnerabilities through malformed input injections that expose system weaknesses. Despite challenges like resource constraints and diverse architectures, fuzzing has proven effective in sectors such as automotive and medical devices. Advancing automated tools and lifecycle integration can further enhance their utility to secure IoT systems [22].

III. AI for IoT Cybersecurity

The ever-evolving landscape of IoT security demands adaptive, intelligent solutions capable of addressing the complexity of threats in real time. Machine learning (ML), deep learning (DL), Large Lanuage Model (LLMs) and edge computing are emerging as indispensable technologies, enhancing the detection, prevention, and mitigation of cyber threats across IoT ecosystems [23], [24]. These technologies offer significant advantages in dynamically adapting to new threats while addressing the unique constraints of IoT devices, such as computational limitations and heterogeneous architectures [25]. This section briefly reviews the use of AI models in IoT security, with an expanded examination of LLMs, as they are the latest AI advancement.

A. Machine Learning in IoT Cybersecurity

Machine learning plays a pivotal role in securing IoT systems, offering both *device-oriented* and *network-oriented* approaches. Device-oriented strategies leverage the unique physical characteristics of IoT devices, while network-oriented methods focus on protecting communication channels and data exchanges [12]. Transparency in ML models is essential to ensure forensic analysis, improve trust in AI-driven systems, and support robust cybersecurity solutions [26].

Intrusion detection systems (IDS) are a cornerstone of IoT security, relying on ML techniques to identify and mitigate threats. IDS models are categorized into *signature-based*, *anomaly-based*, and *hybrid* systems. Signature-based systems detect threats using predefined patterns, anomaly-based systems flag deviations from expected behavior, and hybrid systems combine both approaches for improved accuracy [27]. Distributed IDS solutions, such as those leveraging hybrid deep learning and optimization algorithms, have demonstrated significant success in detecting botnets and distributed denial-of-service (DDoS) attacks [28].

Machine learning-based IDS frameworks integrate supervised and unsupervised learning techniques, with deep learning models showing great promise for high-accuracy threat detection [29]. However, challenges like computational costs and false positive rates remain critical, particularly for resource-constrained IoT devices. The security of healthcare IoT systems is especially vital due to their diverse and life-critical applications. Adaptive ML-based frameworks using evolutionary game theory provide dynamic responses to threats by modeling attacker-defender interactions and optimizing resource allocation [30]. Such frameworks enhance resilience by predicting and countering cyber threats in real time, ensuring the safety of healthcare systems.

B. Deep Learning in IoT Cybersecurity

Deep learning introduces advanced capabilities in IoT security, enabling more robust detection mechanisms and predictive analysis. Energy auditing, for instance, uses dual deep learning models to monitor power consumption, detect anomalies, and identify potential cyber or physical attacks [13]. This lightweight and non-intrusive approach bridges the gap between cybersecurity and physical security, making it well-suited for resource-constrained IoT devices.

In IIoT environments, biologically inspired neural networks, such as Random Neural Networks (RaNN), efficiently detect and mitigate threats like DoS attacks while maintaining low computational overhead [31]. RaNN-based intrusion detection systems (IDS) combine high accuracy, lightweight architecture, and real-time capabilities, making them ideal for securing critical infrastructure [32].

Additionally, ML and DL models, including feedforward neural networks, analyze traffic patterns to differentiate between legitimate and malicious activity. These models, tested on datasets such as CICDDoS2019, demonstrate high accuracy and precision in detecting real-time threats, underscoring their scalability and adaptability [33].

C. Federated Learning for IoT Security

Federated learning (FL) is highlighted as a transformative approach for securing IoT systems by keeping data localized on devices and aggregating only model updates. This method

enhances privacy by preventing the exposure of raw data and addressing scalability challenges in distributed IoT networks [34]. FL demonstrates potential for cyber threat detection across IoT environments, but challenges such as non-IID data and adversarial attacks require robust, scalable solutions tailored to IoT-specific constraints.

D. LLMs for IoT Security

The latest developments in large language models have revealed fresh avenues in enhancing cybersecurity for the Internet of Things (IoT). Unlike existing machine learning models, which rely on structured inputs and tasks, these large language models undergo massive pretraining across multiple sources, resulting in deeper contextual understanding, which is highly relevant in the IoT realm, where devices interact in complex ways.

1) Benefits and Challenges of LLMs for IoT Security: LLMs have the potential to be used for various aspects of IoT security, such as threat identification, incident analysis, policy enforcement, and auto-response generation. LLMs can process unstructured data such as network traces, system notifications, configuration files, and security reports, helping detect malicious activity and identify corresponding events in highly distributed IoT networks. The reasoning power of LLMs helps them to overcome the limitation of existing intrusion detection systems, which follow statistical variations and signatures.

LLMs can serve as intelligent security agents with natural language interfaces, which assist administrators in scanning systems, identifying vulnerabilities, and developing remediation plans. This can simplify operations, making it faster to respond to threats, especially in massive environments. The challenges, however, that still need to be overcome are computational expense, privacy, as well as securing deployment within environments that lack resources [35].

Despite the benefits, several challenges arise when applying LLMs to IoT cybersecurity. The computational complexity and storage requirements of such models are restrictive factors for resource-constrained IoT devices, thereby making edge, fog, cloud, or even multi-cloud computing a necessary consideration for LLM implementations. Then, of course, the issue of IoT data privacy needs consideration, especially when such private IoT data is processed by LLMs. The challenges need to be overcome to make LLM-based cybersecurity solutions scalable, reliable, and regulatory-compliant. In conclusion, large language models are a novel category of AI methods that go beyond the realm of classical machine learning methods in IoT cybersecurity. The potential of these models to reason with contextual knowledge, heterogeneous data, and adaptable security workflows makes them a potential complement to existing detection and mitigation methods. Further research is necessary to assess the robustness, efficiency, and implications of these models on IoT networks. [36]

2) LLMs for IoT Frameworks and System Security: In light of the architectural work on incorporating LLMs into IoT frameworks, there are contemporary developments aimed at developing comprehensive frameworks in which LLMs can be used to secure IoTs. The aim is to leverage LLMs' reasoning skills to develop an end-to-end threat detection and prevention solution for IoTs. Such systems generally use light-weight transformer-based language models that are fine-tuned on IoT-focused datasets such as IoT-23 and TON IoT to analyze network traffic and detect malicious activity. Instead of merely relying on a single classification problem solution for intrusion detection, LLMs are used to analyze overall network traffic within a certain operational context, thereby helping in more accurate detection of malicious activity. The detection modules are also deeply integrated with prevention systems, which are generally rule-based/decision-tree systems that convert LLM predictions to real-time responses such as traffic filtering, isolation, and rate limiting on the edge.

To make such systems scalable and reproducible, they use a containerized execution paradigm that supports edge and cloud evaluations. The performance is then measured in terms of metrics such as detection accuracy, latency, inference rate, and energy cost under various simulated IoT scenarios. The experimental results show that with advancements in fine-tuned lightweight LLMs, detection precision with computational efficiency can be obtained [37].

3) Agentic LLMs for IoT Security Inference: Recently, there have been attempts to apply large language models as interactive security helpers in IoT domains, with a focus on structured reasoning rather than on automated detection pipelines. The solutions leverage Chain-of-Thought reasoning to break down IoT vulnerability issues into understandable units, such as type, location, impact, and user context. By modeling the reasoning process, LLM-based assistants can provide targeted, context-sensitive, and role-based IoT security recommendations for users with diverse skill levels. The experimental results clearly show that IoT-oriented Chain-of-Thought reasoning helps LLMs produce more accurate, relevant, and applicable security advice than raw LLM responses, especially in vulnerability analysis and remediation tasks. It should be noted that such systems do not replace existing intrusion detection systems but rather assist human-AI collaboration with more understandable reasoning in IoT domains [38].

More recent research introduces the use of security assistants for IoT that leverage retrieval-augmented generation as a means to couple large language models with the latest developments in IoT threat intelligence. Instead of relying on the knowledge that pre-training provides, these models are capable of retrieving relevant information from a diverse set of IoT security sources such as vulnerability databases, exploit databases, threat reports, as well as cybersecurity labeling tasks, to make generated responses better grounded in evidence. The incorporation of adaptive retrieval, metadata-driven filtering, and user role-driven generation into these assistants enables them to condition security advice on a diverse set of users, from consumers to experts. The experimental results available show that retrieval augmentation leads to improved relevance, correctness, and technical detail of generated responses compared to standard LLMs, especially in vulnerability analysis and threat interpre-

tation [39].

4) LLMs for Automated IoT Security Decision Making: Extending existing research on the application of LLMs to develop security assistants for advisory and decision support, recent studies have investigated the use of LLMs to enhance active vulnerability scanning for IoT systems via protocol-aware fuzzer development. The ChatHTTPFuzz approach uses LLMs to decode the structure of the HTTP protocol, analyze the backend service's logic, and thereby develop valid, semantically rich test cases for IoT web interfaces. The approach uses labeled fields in the protocol, modifies seed templates based on code-directed packet construction, and employs an optimized Thompson sampling approach for directed mutations, resulting in significant efficiency gains in the fuzzer. Comparison experiments on real-world IoT devices have shown that LLM-fuzzing approaches result in a significant increase in vulnerability identifications, including previously undisclosed CVEs, compared to existing black-box fuzzers [40].

In parallel with system-level research, more recent surveys have investigated the overall relevance of LLMs within the IoT paradigm, focusing on security use cases, architectures, and feasibility. LLMs are viewed as a brain-inspired layer that improves the overall security of IoT systems by providing a means to conduct context-aware analyses of a diverse set of inputs such as logs, network activity, vulnerability reports, and device attributes. In essence, this facilitates tasks such as anomaly analysis, threat interpretation, policy verification, and decision support systems in application domains such as smart cities, healthcare, and industrial IoT. In contrast to classical ML solutions that leverage models specifically aimed at detecting a particular attribute, the LLM-focused perspectives are centered on semantics, inter-layer connections, as well as improved interpretability of corresponding events. At the same time, however, these surveys highlight the pre-existing challenges that are exhibited when applying such models that are inherently resource-hungry in a distributed environment, particularly with respect to latency, computational, energy, transmission, as well as overall feasibility issues in terms of reliability, corresponding hallucinations, and other safety-critical issues. Additional challenges pertaining to overall LLM incorporation from a security perspective, as well as overall data, trust, and management, are also illustrated, especially when LLMs are treated as a means for decision support, semi-autonomous systems, and passive analytical components. It is, in essence, a convergence of use cases on the one hand, with existing challenges, which overall provides a particular perspective on how LLM-friendly mechanisms may efficiently leverage existing IoT infrastructure, while concurrently identifying overall research directions with respect to a trustworthy, scalable, as well as generally secure LLM IoT incorporation [41].

Recent work has investigated the use of large language models (LLM) for autonomous threat detection in Internet of Things (IoT) networks, with LLM regarded as reasoning components that co-exist with, or are built upon, existing intrusion detection systems. Unlike existing solutions that rely on engineered traffic features and pre-determined classification models, LLM-based threat detectors are used for interpreting network event data, notifications, and corresponding metadata, with the aim of autonomously discovering malicious behavior with minimal prior knowledge of threat signatures. The use of pre-trained language models in LLM-based threat detectors has been shown to facilitate reasoning on diverse inputs, cross-temporal association of multiple network events, as well as accommodation of zero-day, polymorphic, and other dynamically changing threat behaviors that are inherently difficult to address with static models. Experimental results support the use of LLMs for improved robustness in threat detection within dynamic IoT networks, especially when dealing with complex, low-rate threats, as well as improved interpretability in making autonomous security decisions based on LLM-driven semantic analysis of behavior. This research thread, on the other hand, also draws attention to the challenges of inference efficiency, scalability, as well as secure implementation, especially in the context of very large IoT networks that employ autonomous threat detection capabilities [42].

E. AI in IoT Edge Security

Edge computing enhances IoT security by decentralizing data processing and bringing computation closer to the source. A novel concept, MIMIC, reimagines traditional Man-In-The-Middle (MITM) attacks as proactive cybersecurity tools. MIMIC acts as a fog computing agent, intercepting and processing IoT data at the edge to improve Quality of Service (QoS) by reducing latency and increasing data transmission rates [17]. Its applications in smart cities and industrial IoT show a balance between efficiency and security. Additional measures, such as cryptographic keys and dynamic configuration, further bolster edge security [43]. Edge computing also reduces the IoT attack surface by embedding cybersecurity tools into edge infrastructures and offloading computational tasks to virtualized nodes [44]. These mechanisms enhance system performance while minimizing risks associated with centralized data processing.

Moreover, edge computing decentralizes data processing, bringing it closer to where data is generated. This significantly reduces latency, enables real-time threat detection, and enhances resource efficiency, making it a powerful tool for IoT security [16]. By deploying lightweight AI algorithms at the edge, IoT systems can proactively detect and thwart threats while managing resource limitations. Edge computing supports zero-trust architectures, ensuring that no device or entity is trusted by default. Real-time analytics integrated at the edge provide a proactive approach to cybersecurity, shifting security practices from reactive to preventive. This is particularly effective for constrained IoT devices, as edge processing minimizes the need for extensive cloud communication, reducing both latency and bandwidth requirements. Edge computing also addresses vulnerabilities in IoT communication processes by distributing processing across local nodes. AI-enabled configurations, such as secure Administrator Console (AC) and Data Center Console

(DC) ports, improve fault detection and optimize resource allocation in communication protocols. These measures enhance the overall security and reliability of IoT networks.

IV. Conclusion

In this paper, we provide a comprehensive survey on emerging technologies and cybersecurity challenges in IoT systems, highlighting their implications and potential solutions across domains such as healthcare, industrial IoT (IIoT), smart cities, and energy systems. We examine foundational technologies, including federated learning, edge computing, blockchain, and adaptive cybersecurity frameworks, emphasizing their ability to enhance privacy, scalability, and resilience in resource-constrained IoT environments. Additionally, we analyze critical vulnerabilities such as adversarial attacks, ransomware targeting legacy systems, and the inherent risks in distributed IoT networks, while exploring advanced mitigation strategies like lightweight encryption, intrusion detection systems, and dynamic configuration.

Our discussion underscores the importance of integrating sustainability considerations into IoT security, balancing energy efficiency with robust protection to address environmental and operational concerns. Furthermore, the survey highlights the role of collaborative research efforts among academia, industry, and regulatory bodies in addressing scalability, interoperability, and evolving cyber threats. By providing a holistic overview of current advancements and challenges, this survey aims to guide future research and the development of secure, scalable, and sustainable IoT ecosystems that align with the growing demands of an interconnected world.

References

[1] Mostafa Haghi Kashani, Mona Madanipour, Mohammad Nikravan, Parvaneh Asghari, and Ebrahim Mahdipour. A systematic review of iot in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, 192:103164, 2021.

[2] Hui Yang, Soundar Kumara, Satish TS Bukkapatnam, and Fugee Tsung. The internet of things for smart manufacturing: A review. *IISE transactions*, 51(11):1190–1216, 2019.

[3] Abbas Shah Syed, Daniel Sierra-Sosa, Anup Kumar, and Adel Elmaghraby. Iot in smart cities: A survey of technologies, practices and challenges. *Smart Cities*, 4(2):429–475, 2021.

[4] Guneet Bedi, Ganesh Kumar Venayagamoorthy, Rajendra Singh, Richard R Brooks, and Kuang-Ching Wang. Review of internet of things (iot) in electric power and energy systems. *IEEE Internet of Things Journal*, 5(2):847–870, 2018.

[5] Yang Lu and Li Da Xu. Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2):2103–2115, 2018.

[6] Joseph Squillace and May Bantan. A taxonomy of privacy, trust, and security breach incidents of internet-of-things linked to f (m). aang corporations. In *2022 IEEE World AI IoT Congress (AIIoT)*, pages 591–596. IEEE, 2022.

[7] Rahul Shokeen, Bharanidharan Shanmugam, Krishnan Kannoorpatti, Sami Azam, Mirjam Jonkman, and Mamoun Alazab. Vulnerabilities analysis and security assessment framework for the internet of things. In *2019 Cybersecurity and Cyberforensics Conference (CCC)*, pages 22–29. IEEE, 2019.

[8] Dhuha Khalid Alferidah and NZ Jhanjhi. Cybersecurity impact over bigdata and iot growth. In *2020 International Conference on Computational Intelligence (ICCI)*, pages 103–108. IEEE, 2020.

[9] Ramadan Gad, Ahmed A Abd El-Latif, Sherif Elseuofi, Hany M Ibrahim, Mahmoud Elmezain, and Wael Said. Iot security based on iris verification using multi-algorithm feature level fusion scheme. In *2019 2nd international conference on computer applications & information security (ICCAIS)*, pages 1–6. IEEE, 2019.

[10] Vadym Malinovskyi, Leonid Kupershtein, and Vitaliy Lukichov. Cybersecurity and data stability analysis of iot devices. In *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, pages 259–264. IEEE, 2022.

[11] Surakarn Duangphasuk, Pruegsa Duangphasuk, and Chalee Thammarat. Review of internet of things (iot): security issue and solution. In *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 559–562. IEEE, 2020.

[12] Azzedine Boukerche and Rodolfo WL Coutinho. Design guidelines for machine learning-based cybersecurity in internet of things. *IEEE Network*, 35(1):393–399, 2020.

[13] Fangyu Li, Yang Shi, Aditya Shinde, Jin Ye, and Wenzhan Song. Enhanced cyber-physical security in internet of things through energy auditing. *IEEE Internet of Things Journal*, 6(3):5224–5231, 2019.

[14] S Mohammadali Zanjani, Hossein Shahinzadeh, Jalal Moradi, Zohreh Rezaei, Bahareh Kaviani-Baghbaderani, and Sudeep Tanwar. Securing the internet of things via blockchain-aided smart contracts. In *2022 13th International Conference on Information and Knowledge Technology (IKT)*, pages 1–8. IEEE, 2022.

[15] Jiannan Wei, Qinchuan Zhu, Qianmu Li, Laisen Nie, Zhangyi Shen, Kim-Kwang Raymond Choo, and Keping Yu. A redactable blockchain framework for secure federated learning in industrial internet of things. *IEEE Internet of Things Journal*, 9(18):17901–17911, 2022.

[16] Mansoor Farooq and Mubashir Hassan Khan. Artificial intelligence-based approach on cybersecurity challenges and opportunities in the internet of things & edge computing devices. *International Journal of Engineering and Computer Science*, 12(07):25763–25768, 2023.

[17] Lorenzo Incipini, Alberto Belli, Lorenzo Palma, Roberto Concetti, and Paola Pierleoni. Mimic: A cybersecurity threat turns into a fog computing agent for iot systems. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 469–474. IEEE, 2019.

[18] Jay Thom, Tapadhir Das, Bibek Shrestha, Shamik Sengupta, and Engin Arslan. Casting a wide net: An internet of things testbed for cybersecurity education and research. In *2021 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, pages 1–8. IEEE, 2021.

[19] Inggit Putri Naria, Selo Sulistyo, et al. Security and privacy issue in internet of things, smart building system: A review. In *2022 International Symposium on Information Technology and Digital Innovation (ISITDI)*, pages 177–180. IEEE, 2022.

[20] Saurabh Lahoti. The internet of things privacy is provided through object identification. In *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, pages 1130–1134. IEEE, 2023.

[21] Geeta Yadav, Kolin Paul, Alaa Allakany, and Koji Okamura. Iot-pen: A penetration testing framework for iot. In *2020 International Conference on Information Networking (ICOIN)*, pages 196–201. IEEE, 2020.

[22] Maialen Eceiza, Jose Luis Flores, and Mikel Iturbe. Fuzzing the internet of things: A review on the techniques and challenges for efficient vulnerability discovery in embedded systems. *IEEE Internet of Things Journal*, 8(13):10390–10411, 2021.

[23] Mujaheed Abdullahi, Yahia Baashar, Hitham Alhussian, Ayed Alwadain, Norshakirah Aziz, Luiz Fernando Capretz, and Said Jadid Abdulkadir. Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2):198, 2022.

[24] I Lee. Internet of things (iot) cybersecurity: Literature review and iot cyber risk management. future internet, 12 (9), 157, 2020.

[25] Murat Kuzlu, Corinne Fair, and Ozgur Guler. Role of artificial intelligence in the internet of things (iot) cybersecurity. *Discover Internet of things*, 1(1):7, 2021.

[26] Tehseen Mazhar, Dhani Bux Talpur, Tamara Al Shloul, Yazeed Yasin Ghadi, Inayatul Haq, Inam Ullah, Khmaies Ouahada, and Habib Hamam. Analysis of iot security challenges and its solutions using artificial intelligence. *Brain Sciences*, 13(4):683, 2023.

[27] Abbas Jamalipour and Sarumathi Murali. A taxonomy of machine-learning-based intrusion detection systems for the internet of things: A survey. *IEEE Internet of Things Journal*, 9(12):9444–9466, 2021.

[28] Kaushiv Garg, Kanwarpartap Singh Gill, Rahul Chauhan, Devyani Rawat, and Deepak Banerjee. Distributed denial of services (ddos) botnet attack prevention in internet of things (iot) devices using ai. In *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, pages 1–5. IEEE, 2023.

[29] Omar Azib Alkhudaydi, Moez Krichen, and Ans D Alghamdi. A deep learning methodology for predicting cybersecurity attacks on the internet of things. *Information*, 14(10):550, 2023.

[30] Svetlana Boudko and Habtamu Abie. Adaptive cybersecurity framework for healthcare internet of things. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, pages 1–6. IEEE, 2019.

[31] Shahid Latif, Zhuo Zou, Zeba Idrees, and Jawad Ahmad. A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE access*, 8:89337–89350, 2020.

[32] Zil E Huma, Shahid Latif, Jawad Ahmad, Zeba Idrees, Anas Ibrar, Zhuo Zou, Fehaid Alqahtani, and Fatmah Baothman. A hybrid deep random neural network for cyberattack detection in the industrial internet of things. *IEEE access*, 9:55595–55605, 2021.

[33] Rashid Mustafa, Nurul I Sarkar, Mahsa Mohaghegh, and Shahbaz Pervez. A cross-layer secure and energy-efficient framework for the internet of things: A comprehensive survey. *Sensors (Basel, Switzerland)*, 24(22):7209, 2024.

[34] Bimal Ghimire and Danda B Rawat. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, 9(11):8229–8249, 2022.

[35] Mingyu Zong, Arvin Hekmati, Michael Guastalla, Yiyi Li, and Bhaskar Krishnamachari. Integrating large language models with internet of things: applications. *Discover Internet of Things*, 5(1):2, 2025.

[36] Saeid Jamshidi, Negar Shahabi, Amin Nikanjam, Kawser Wazed Nafi, Foutse Khomh, and Carol Fung. The role of large language models in iot security: A systematic review of advances, challenges, and opportunities. *Internet of Things*, page 101735, 2025.

[37] Yazan Otoum, Arghavan Asad, and Amiya Nayak. Llm-based threat detection and prevention framework for iot ecosystems. *arXiv preprint arXiv:2505.00240*, 2025.

[38] Mingfei Zeng, Ming Xie, Xixi Zheng, Chunhai Li, Chuan Zhang, and Liehuang Zhu. Large language model-driven security assistant for internet of things via chain-of-thought. *IEEE Internet of Things Journal*, 2025.

[39] Ye Dong, Yan Lin Aung, Sudipta Chattopadhyay, and Jianying Zhou. Chatiot: Large language model-based security assistant for internet of things with retrieval-augmented generation. *arXiv preprint arXiv:2502.09896*, 2025.

[40] Zhe Yang, Hao Peng, Yanling Jiang, Xingwei Li, Haohua Du, Shuhai Wang, and Jianwei Liu. Chathttpfuzz: large language model-assisted iot http fuzzing. *International Journal of Machine Learning and Cybernetics*, pages 1–22, 2025.

[41] Kushal Khatiwada, Jayden Hopper, Joseph Cheatham, Ayan Joshi, and Sabur Baidya. Large language models in the iot ecosystem–a survey on security challenges and applications. *arXiv preprint arXiv:2505.17586*, 2025.

[42] Jing Zhang. Leveraging large language models for autonomous threat detection in iot networks. In *Proceedings of the 2024 8th International Conference on Electronic Information Technology and Computer Engineering*, pages 545–550, 2024.

[43] Muzafer H Saračević, Saša Z Adamović, Vladislav A Miškovic, Mohamed Elhoseny, Nemanja D Maček, Mahmoud Mohamed Selim, and K Shankar. Data encryption for internet of things applications based on catalan objects and two combinatorial structures. *IEEE Transactions on Reliability*, 70(2):819–830, 2020.

[44] Phillip Williams, Indira Kaylan Dutta, Hisham Daoud, and Magdy Bayoumi. A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things*, 19:100564, 2022.