Examining the Impact of Artificial Intelligence on Cybersecurity within the Internet of Things

Mayur Rele
IT and Cybersecurity
Parachute Health
Princeton, New Jersey
mayur.rele@parachutehealth.com

Dipti Patil
Graduate School of Business
University of Cumberlands
Williamsburg, Kentucky
dpatil2618@ucumberlands.edu

Abstract— **The explosive growth of the Internet of Things (IoT) has created unprecedented cybersecurity challenges and opportunities. As the Internet of Things expands to include more connected devices, it becomes more difficult to safeguard the security and privacy of sensitive data. In this context, artificial intelligence (AI) has become a potent instrument for enhancing the security of Internet of Things (IoT) devices. This article seeks a greater understanding of how artificial intelligence may support cybersecurity in the IoT ecosystem. To reduce vulnerabilities, identify threats, and enhance the overall resilience of Internet of Things (IoT) systems, this paper examines the application of AI techniques. The proposed research investigates the numerous applications of AI in IoT cybersecurity, such as threat intelligence, behavioral analysis, anomaly detection, and predictive modeling. The study will include a summary of current AI-driven IoT security methods and algorithms and an evaluation of their strengths and limitations. In addition, it will underscore the importance of combining AI with other cybersecurity technologies, such as blockchain and cloud computing, to construct a robust defense system. Additionally, the paper discusses the ethical implications of AI use in IoT cybersecurity. It will discuss potential issues such as biases in AI algorithms, privacy concerns, and the need for accountability and transparency in decision-making. In conclusion, this article provides valuable insights into AI's role in IoT cybersecurity and its potential to alter IoT system defense fundamentally.**

Keywords— Internet of Things (IoT), Artificial intelligence (AI), Cybersecurity, Anomaly detection, Threat Intelligence, Behavioral analysis.

I. INTRODUCTION

The Internet of Things (IoT), which enables seamless connectivity and communication between various items and systems, has completely changed how we interact online [1]. The Internet of Things (IoT) has significantly impacted numerous aspects of our everyday lives, which offers ease, efficiency, and improved decision-making [2]. Numerous applications, including wearable technology, smart homes, industrial automation, and smart cities, can demonstrate this effect. To guarantee data confidentiality and authenticity throughout transmission and processing, it is essential to handle the many security issues that develop due to connected Internet of Things (IoT) devices. The attack surface for potential cyber threats has risen tremendously due to the development of Internet of Things (IoT) devices [3]. [4] It can be challenging to adjust traditional security strategies created for conventional computing systems to the changing threat environment and particular traits of Internet of Things (IoT) devices. Due to intrinsic resource limitations, Internet of Things (IoT) devices often have constrained processor speed, memory size, and energy resources. Additionally, they frequently function in multiple contexts and rely on operating systems, firmware, and communication protocols [5]. These factors seriously impede the successful adoption of solid security measures throughout the Internet of Things (IoT) ecosystem. A significant challenge is posed by the prompt detection and mitigation of Internet of Things (IoT) security risks [6]. Novel methodologies are needed for practical analysis and detection of potential security breaches due to the enormous amount of data created by connected devices and their diverse and dispersed design. Conventional security methods may need help adjusting to the dynamic and regularly changing landscape of Internet of Things (IoT) security hazards due to their use of static regulations and recognizing patterns. Therefore, it is crucial to research cutting-edge methods that successfully use Artificial Intelligence (AI) to enhance Internet of Things (IoT) security. Artificial intelligence has a significant potential to address Internet of Things (IoT) security challenges because of its capacity to evaluate massive amounts of data, spot patterns, and make defensible conclusions [7]. Incorporating AI approaches into IoT security frameworks has improved real-time reactions to changing assaults, increased anomaly detection, and proactive threat identification and mitigation. By assisting in the detection of unusual behavioral patterns, the detection of intrusion attempts, and the autonomous reaction to potential security breaches, artificial intelligence (AI) has the potential to increase the overall security of Internet of Things (IoT) systems. The Internet of Things (IoT) connects gadgets and allows seamless communication and data sharing, revolutionizing several industries. Nevertheless, the security threats and vulnerabilities brought on by this interconnectedness are significant. Researchers have looked into various strategies for increasing the security of IoT apps and devices to address these problems. (1) ease of use when formatting individual papers, (2) The discussed papers illuminated several IoT application and device security-related issues. The study's authors [8] comprehensively analyze Internet of Things (IoT) application security threats. To identify potential vulnerabilities in IoT systems and enhance their security, they propose solutions to mitigate these risks. In addition, the article compares and contrasts various IoT systems according to their robustness, self-organization, access control, anonymity, confidentiality, and privacy. By analyzing these distinct elements, the authors provide beneficial insights into the security issues and advantages and disadvantages of various IoT systems. The authors of [9] recommend deep learning models to identify Distributed Denial of Service (DDoS) attacks in IoT systems. The CICIDS2017 dataset is utilized to train and evaluate their proposed models. Deep learning has the potential to efficiently identify and thwart DDoS attacks in IoT devices, as shown by the high accuracy rate of the results. Utilizing the capabilities of deep learning algorithms, the authors contribute to improving the security and resistance of IoT networks to such assaults.

The paper focuses on using Artificial Neural Networks (ANNs) for IoT data anomaly detection [10]. To improve the overall security of IoT networks, the authors recommend employing ANNs in gateway devices to analyze data collected from the periphery. By teaching ANNs to recognize patterns of typical activity, it is possible to detect potential anomalies or security threats. This method enhances the security of IoT environments and enables the proactive detection of suspicious behavior. The authors of [11] propose a control strategy based on AI for identifying, estimating, and mitigating intrusions in industrial IoT systems. Utilizing AI techniques such as machine learning and data analytics, the authors intend to enhance the security and resilience of industrial IoT systems. The proposed method enables the detection of intrusions in real-time, estimating their potential impact, and implementing the necessary countermeasures to mitigate their effects. This AI-based control strategy for industrial IoT systems strengthens their security measures. In [12], the authors present a ubiquitous detection strategy for IoT environments that incorporates adversarial attacks and countermeasures and employs various detection techniques. Using network-based, host-based, and application-based detection, the authors enhance the overall security of Internet of Things (IoT) systems. In addition, they contribute to developing effective detection methods and proactive protection strategies against new threats in IoT environments by researching adversarial attacks and developing effective defense mechanisms. This chapter examines the evolution of AI decision-making in cyber-physical systems, focusing on integrating IoT devices. They highlight the systems' increasing reliance on AI algorithms for decision-making. This reliance is due to AI's ability to process vast data swiftly and intelligently. Examining the pros and cons of AI decision-making, the authors shed light on the evolving cyber-physical system landscape and the incorporation of IoT devices into decision-making processes. The article [14], which focuses on IoT networks in industrial contexts, discusses novel approaches to risk analytics utilizing AI and machine learning techniques. The authors investigate how machine learning and AI could be used to analyze IoT network data to identify and mitigate threats effectively. Utilizing the capabilities of AI and machine learning algorithms, industrial settings can improve their risk management practices and enhance the security and resilience of their IoT networks. To develop standardized standards for cybersecurity in the IoT sector, the authors of [15] concentrate on capturing and evaluating IoT-device-related cybersecurity threats. They discuss techniques for rapidly detecting and avoiding threats in IoT systems. By developing standardized standards, stakeholders can improve the security of Internet of Things (IoT) systems and foster a more secure and robust IoT ecosystem. This research contributes to the development of methods for identifying and addressing IoT device cybersecurity vulnerabilities consistently and efficiently. As IoT devices grow, ensuring their security becomes increasingly tricky. The expanding attack surface of a network of interconnected devices necessitates implementing advanced security measures. On the other hand, traditional approaches need help to keep up with the continuously shifting threat environment and the unique characteristics of IoT devices. The practical analysis of the vast and diverse data generated by IoT devices necessitates applying innovative techniques for identifying and mitigating emergent threats in real time. In addition, the distributed nature of IoT systems and the resource limitations of these devices make it more challenging to implement robust security measures. This study's comprehensive literature review focuses on incorporating Artificial Intelligence (AI) strategies within the context of Internet of Things (IoT) security. Data privacy, confidentiality, and integrity concerns have been raised due to the IoT's rapid growth and associated security flaws. Experts have therefore resorted to AI-based solutions to enhance the security of IoT devices. The review commences with a summary of the fundamental concepts underlying IoT security and the challenges it poses.

The rest of the paper is structured as follows: Section 2 presents a comprehensive summary of the research that is currently accessible. In Section 3, we devote a significant amount of time to discussing the role of artificial intelligence in cybersecurity. Section 4 will present a state-of-the-art of the impact of AI on cybersecurity within IoT systems. The document's conclusion includes a summary and any concluding thoughts.

II. IOT SYSTEM FOR CYBERSECURITY

The Internet of Things (IoT) has changed how we communicate and share data. Interconnected physical devices with sensors, software, and other technologies to collect and send data [16]. Despite its promise to improve ease, automation, and efficiency in many areas, the IoT faces serious cybersecurity issues. IoT cybersecurity risks include the amount and variety of network-connected devices [17]. Billion-plus gadgets, from industrial sensors to smart household appliances, have different specs and weaknesses, making security challenging. Malicious actors target IoT devices because they have limited resources, require extensive security measures, and often use outdated software [18]. IoT devices' interconnection raises cyber threats' attack surface [19]. A network-wide vulnerability from one device could put other devices and vital infrastructure at risk. IoT devices create a lot of data, including sensitive personal data, raising privacy and access concerns [20]. The IoT ecosystem must overcome many critical problems. Device makers must use robust authentication, encryption, and software updates. Organizations and individuals must also implement network configuration, monitoring, and vulnerability remediation. The Internet of Things stores and processes data on the cloud, requiring strict cloud security standards. Protecting cloud data requires data encryption, secure communication methods, and access control systems. With IoT, cybersecurity must evolve. Anomaly detection, threat intelligence, and automated response systems may require AI and ML. Uniform security frameworks and legislation require industry, lawmaker, and researcher collaboration. As shown in Fig. 1, IoT-connected systems have a multidimensional attack surface, stressing the importance of cybersecurity. IoT systems must be protected from multiple attack vectors. IoT devices, networks, communication channels, and apps are attack vectors [21]. IoT systems must be adequately cyber-protected to secure the linked ecosystem's availability, confidentiality, and integrity.

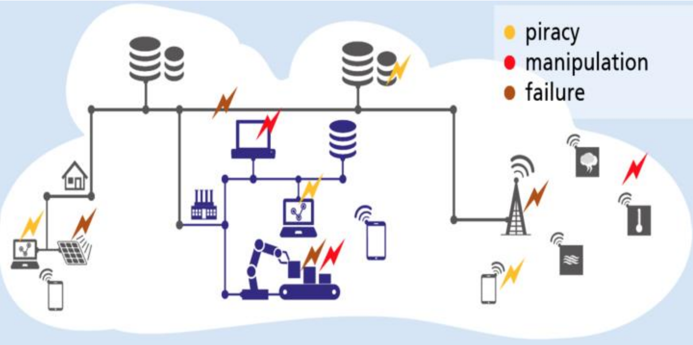

Fig. 1: Attack Vectors in IoT Connected Systems.

Cybersecurity must be addressed to protect IoT devices and networks' privacy, integrity, and robustness [22]. IoT's many linked devices, diverse communication protocols, and resource limits present cybersecurity issues. It requires a comprehensive plan that addresses device, network, and data security. Strong authentication, secure firmware and software upgrades, and data encryption are needed to secure IoT devices [23]. Physical attacks can be prevented through secure launch methods, hardware-based security measures, and tamper-resistant designs. Continuous monitoring and vulnerability management are needed to find and fix new security concerns. IoT system security ensures safety. Robust access control, network segmentation, and secure communication protocols prevent illegal access and data breaches. Anomaly detection, traffic monitoring, and intrusion detection and prevention systems identify and mitigate real-time threats. Regular security assessments may help identify network infrastructure issues [24]. IoT cybersecurity also requires data security. This requires keeping all IoT data secure, intact, and accessible [25]. Encryption, safe data storage, and strict access controls protect sensitive data [26]. Data authentication and integrity verification also detect unlawful data alteration. IoT cybersecurity requires collaboration among stakeholders such as device makers, network providers, cybersecurity experts, and regulatory bodies [27]. Information sharing, industry standards, and best practices are needed to secure the Internet of Things. Secure practices and cybersecurity education can also improve IoT ecosystem security. IoT cybersecurity risks develop. New threats and weaknesses require ongoing research and innovation. Proactive cybersecurity, cutting-edge technologies like AI and machine learning, and a security culture can create a durable and secure IoT system.

III. Artificial Intelligence in Cybersecurity

Artificial intelligence has become an invaluable asset in the field of cybersecurity, particularly for intrusion detection [28]. By assessing traffic patterns and identifying suspicious activities, AI algorithms such as decision trees, k-nearest neighbors (KNN), support vector machines (SVM), and artificial neural networks (ANN) augment the capabilities of cybersecurity systems in protecting IoT environments. AI enhances defense mechanisms through continuous learning and adaptation, facilitating real-time detection and threat response. This AI integration allows cybersecurity systems to secure vital systems and data, mitigating cyber-attack risks and ensuring higher security in IoT ecosystems [29].

A. *Machine Learning*

Machine learning is essential to cybersecurity because it enables the creation of intelligent systems that can efficiently detect and prevent cyber-attacks. Machine learning techniques analyze massive amounts of data produced by IoT devices, networks, and human interactions in the context of Internet of Things (IoT) security [30]. The use of machine learning techniques in IoT cybersecurity is highlighted in this paragraph.

B. *Decision Trees*

Cybersecurity professionals utilize decision trees frequently for categorization and anomaly detection tasks. Decision trees can evaluate IoT security factors, including user behavior, network traffic patterns, and IoT device activity. By analyzing these elements and identifying potential security issues, decision trees aid in making well-informed decisions about security measures. Decision trees include nodes representing decision points and branches representing possible outcomes. Evaluating a specific characteristic or circumstance yields distinct branches at each decision point. Based on observed data, decision trees can classify network traffic or IoT devices as legitimate or malicious by retracing their path through the tree. In addition, by employing predefined rules or learned patterns, they can identify out-of-the-ordinary behavior, facilitating the early detection of potential attacks or security breaches [31].

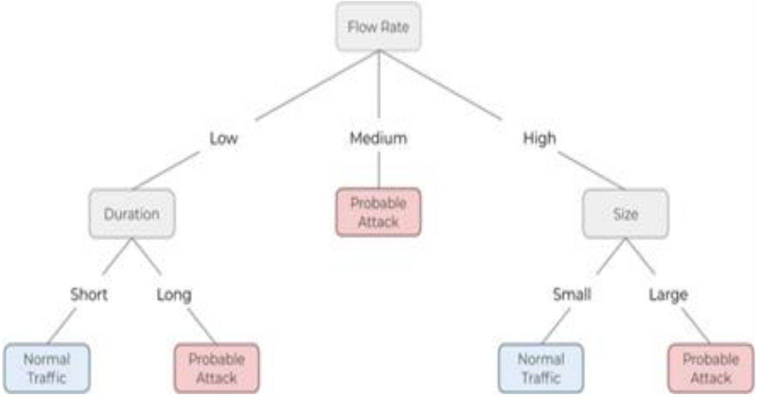

Fig. 2: An example of a decision tree for classifying network traffic.

C. Equ K-Nearest Neighbors (KNN)

K-Nearest Neighbors is a machine-learning technique that categorizes data components in a feature space according to their proximity to other points. Regarding IoT security, KNN has a variety of uses, such as anomaly detection, intrusion detection, and user authentication. By examining the traits and behaviors of nearby data points, KNN can efficiently spot suspicious or malicious activity within an IoT system. The KNN algorithm determines how far a specific data point is from its k nearest neighbors. Most of the data point's neighbors decide what class the data point belongs to. For IoT security, KNN can recognize suspicious access attempts, spot abnormal network traffic patterns, and authenticate users based on behavioral patterns. Due to its versatility and simplicity, KNN is a valuable tool for real-time IoT security monitoring [32].

D. Support Vector Machines (SVM):

Support Effective machine learning categorization methods include vector machines. SVMs find the best hyperplanes to divide different data point groups. SVMs are used in many IoT security domains, such as malware detection, network intrusion detection, and anomaly detection. By creating the best decision limits, SVMs assist in the discovery and mitigation of security risks in IoT systems. SVMs look for the hyperplane that maintains the largest margin of separation while maximizing separating data points of different classes. SVMs can be trained on labeled datasets in IoT security to categorize network traffic as legitimate or malicious, find specific types of malware, and spot unusual behaviors. SVMs are suited for assessing intricate IoT security scenarios because they offer thorough classification capabilities and the capacity to handle high-dimensional data [33].

E. Artificial Neural Networks (ANN):

As a tribute to the human brain, artificial neural networks are adaptable models capable of recognizing intricate patterns and connections. Multiple aspects of IoT security rely on ANNs, including user authentication, malware detection, and intrusion detection. Utilizing their capacity to record complex relationships, ANNs enhance detecting and preventing cyber risks within IoT systems. Layers of interconnected nodes or neurons compose ANNs. As information travels through the network, each neuron performs calculations and transmits the results to the next layer. During training, connection weights must be modified to optimize the performance of ANNs. ANNs can acquire typical IoT security behavior patterns and identify deviations that indicate potential threats. By analyzing network traffic, device interactions, and user activity [34], they can recognize anomalies, classify malware, and authenticate individuals based on their unique patterns.

IV. Impact of Artificial Intelligence on Cybersecurity within the Internet of Things

Artificial intelligence (AI) has had a profound and revolutionary effect on Internet of Things (IoT) cybersecurity, fundamentally changing the approach to protecting IoT infrastructure. The ever-evolving cyber threats that target IoT networks and devices have made AI a powerful tool in the fight against them [35]. One of the significant benefits of AI in IoT cybersecurity is the technology's ability to analyze large amounts of data in real time and discover patterns indicative of malicious behavior or irregularities [36]. Due to the vast number of interconnected gadgets, manual monitoring and threat detection are no longer practical in an IoT setting. Autonomous threat identification is now achievable thanks to AI-driven solutions, which allow for rapid reactions to prospective security breaches and shorter response times [37]. The ability of artificial intelligence (AI) to recognize and actively counter emerging cyber threats is greatly enhanced by machine learning algorithms, which enable AI to learn from past events and adapt to new hazards continuously.

AI also increases IoT security by bolstering access control and authentication procedures. Artificial intelligence systems can analyze patterns of human behavior and device interactions to detect anomalous behavior or attempted intrusion. AI systems can now protect critical IoT resources from illegal access because of their capacity to tell legitimate users apart from potential attackers. AI has also had a significant effect on IoT cybersecurity in anomaly detection [38]. Using AI, detecting anomalies in IoT devices and network behavior that could instantly indicate intrusion is possible. As a result, security teams can respond rapidly to assaults in progress, mitigating their effects and preventing data breaches. In addition, AI-driven predictive analytics are crucial in risk management and vulnerability assessment [39]. By constantly monitoring and analyzing IoT devices for potential weaknesses, AI can proactively recommend tightening security measures and patch vulnerabilities before attackers may use them. Keep in mind that there are new challenges due to the advancement of AI in IoT cybersecurity. Adversarial AI refers to the growing danger posed by attackers who use AI algorithms to bypass security safeguards. As artificial intelligence develops, so are the methods utilized by cybercriminals. Therefore, the constant investigation into AI-driven cybersecurity solutions is necessary to stay ahead of evolving threats.

The literature on the impact of artificial intelligence (AI) on cybersecurity in the Internet of Things (IoT) is rich with studies that look at novel approaches to addressing the growing threats to online safety. In [40], the authors demonstrate the importance of AI-driven anomaly detection in IoT security by demonstrating the efficiency and effectiveness of deep learning models in identifying suspicious behavior. AI-powered predictive analytics is crucial in vulnerability assessment for IoT systems, as suggested by the authors of [41], who offer a hybrid machine learning and data mining technique to finding security gaps. While [42] examines the challenges adversarial AI algorithms confront in IoT cybersecurity and propose ways to prevent future exploitation, the former paper focuses on the former topic. While [43] provides a comprehensive analysis of AI-based IoT intrusion detection, [44] delves deeply into the use of machine learning techniques to keep IoT systems safe. In [45], we see an example of how AI can enhance security with the presentation of IoT Sentinel, an automated device-type recognition system for IoT security enforcement. In [46], the authors present an overview of machine learning security for the Internet of Things and discuss recent developments and trends. While [47] investigates machine learning for IoT data analysis, [48] looks into how AI may be used to keep IoT secure. In addition, [49] discusses how blockchain and machine learning may work together to make the Internet of Things safer and more private. The literature provides insight into various AI-powered approaches and their potential applications in safeguarding IoT ecosystems from cyber threats. It highlights AI's crucial role in strengthening IoT cybersecurity overall.

AI-driven solutions for securing IoT devices are becoming increasingly important, as evidenced by a literature review. Several research has investigated the possibility of using AI methods like machine learning and deep learning to improve IoT security measures like anomaly detection, vulnerability assessment, and intrusion detection. Problems with adversarial artificial intelligence and securing IoT data processing have also been the focus of studies. Despite the promising findings, these studies have limitations, such as the need for extensive data, a shortage of empirical research, and a need for more practical application. As the IoT environment evolves, overcoming these challenges and exploring innovative AI-based techniques to build a safe and robust IoT ecosystem becomes increasingly critical. The table summarizes the findings, the methods used in each investigation, and the limitations of each approach. By reviewing these works, we may better understand the field's current state and the pros and cons of employing artificial intelligence to strengthen IoT protection.

TABLE I. AI IN IOT CYBERSECURITY: A COMPREHENSIVE LITERATURE REVIEW

Paper Title	Key Findings	Methods Used	Drawbacks
[40]	Demonstrated the effectiveness of AI-driven anomaly detection in IoT security using deep learning for identifying potential threats.	Deep Learning	Limited evaluation of real-world IoT systems.
Liu et [41]	Proposed an AI-powered vulnerability assessment approach for IoT systems using machine learning and data mining for security analysis.	Machine Learning, Data Mining	The need for extensive data for accurate vulnerability assessment.
[42]	Explored adversarial AI in IoT cybersecurity and suggested countermeasures to mitigate potential threats.	Adversarial AI, Security Countermeasures	Limited focus on real-world implementation and scalability.
[43]	Conducted a survey of machine learning techniques for securing IoT systems, offering insights into various approaches.	Literature Review	Lack of empirical evaluation of the surveyed techniques.
[44]	Conducted a systematic review of AI-based intrusion detection in IoT, highlighting the latest developments and challenges.	Systematic Review	Limited coverage of recent research in a rapidly evolving field.
[45]	Presented IoT Sentinel, an automated device-type identification system using AI for enhancing security measures in IoT.	AI-based Device-Type Identification System	Limited evaluation of a wide range of diverse IoT devices.
[46]	Provided a survey of machine learning security for IoT, discussing the application of various ML techniques in IoT cybersecurity.	Literature Review	The evolving nature of cybersecurity may make some findings outdated.
[47]	Explored secure IoT using AI, emphasizing the potential of AI in enhancing security and privacy protection for IoT systems.	AI for Security Enhancement	Limited analysis of the potential risks associated with AI implementation in IoT security.
[48]	Conducted a survey of machine learning for IoT data analysis, showcasing the role of ML in processing and analyzing IoT data.	Literature Review	Lack of in-depth exploration of specific challenges faced in ML-driven IoT data analysis.
[49]	Discussed AI and blockchain technologies' integration for IoT security and privacy protection, offering insights into their potential.	AI, Blockchain	Limited practical implementation of the proposed integration in real-world IoT systems.

V. CONCLUSION AND DISCUSSION

The topic focuses on the numerous security problems and attack vectors related to IoT devices. It highlights IoT device vulnerabilities such as weak passwords, obsolete firmware, and insecure default installations. The debate emphasizes implementing robust authentication procedures, regular updates and patches, network segmentation, encryption, and user awareness to reduce these dangers. It emphasizes the importance of proactive security measures, such as identifying and fixing vulnerabilities in IoT devices, safeguarding network connections, and adopting physical security measures. Collaboration between AI researchers, IoT device manufacturers, and cybersecurity specialists is required to resist AI-driven threats and safeguard IoT networks effectively. As a result, the discussion highlights the dynamic nature of IoT security vulnerabilities and underscores the importance of comprehensive security solutions to safeguard IoT devices and networks. It emphasizes the necessity of proactive defensive techniques and stakeholder participation in addressing emerging IoT security threats. In conclusion, safeguarding IoT devices is critical in the face of changing threats. This study thoroughly examined many security factors, such as vulnerabilities, attacks, and mitigation measures. It emphasized the importance of proactive defenses, collaborative efforts, and robust security procedures in dealing with AI-driven attacks, network-based assaults, physical attacks, and IoT botnets. Collaboration among stakeholders is critical in establishing improved protection mechanisms and safeguarding IoT devices. A complete solution encompassing device-level security, network defenses, and stakeholder collaboration is required to protect IoT devices and ensure a secure and trustworthy ecosystem. Continuous research and innovation are critical for avoiding emerging threats and tackling increasing security concerns in the IoT arena.

REFERENCES

1. Abid, M. A., Afaqui, N., Khan, M. A., Akhtar, M. W., Malik, A. W., Munir, A., ... & Shabir, B. (2022). Evolution towards innovative and software-defined Internet of things. AI, 3(1), 100-123.
2. Reddy, K. S., Agarwal, K., & Tyagi, A. K. (2021). Beyond things: A systematic study of the Internet of everything. In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 10th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2019) held in Gunupur, Odisha, India during December 16-18, 2019 10 (pp. 226-242). Springer International Publishing.
3. de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920.
4. Wolf, M., & Serpanos, D. (2020). Safe and secure cyber-physical systems and internet-of-things systems. Cham: Springer.
5. Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of Things for system integrity: A comprehensive survey on security, attacks, and countermeasures for industrial applications. Sensors, 21(11), 3654.
6. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in the Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019, 1-14.
7. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1, 1-14.
8. Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 160, 165-191.
9. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1, 1-14.
10. Ackerson, J. M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. Information, 12(7), 272.
11. Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating artificial intelligence in cyber security for cyber-physical systems. Electronic Research Archive, 31(4), 1876-1896.
12. Wang, S., & Qiao, Z. (2019). Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments. IEEE Access, 7, 88693-88704.
13. Radanliev, P., De Roure, D., Van Kleek, M., Santos, O., & Ani, U. (2021). Artificial intelligence in cyber physical systems. AI & society, 36, 783-796.
14. Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of things and industry 4.0 supply chains. Cybersecurity, 3(1), 1-21.
15. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020(1), 1-18.
16. Vermesan, O., & Friess, P. (2014). Internet of Things applications-from research and innovation to market deployment (p. 364). Taylor & Francis.
17. Wheelus, C., & Zhu, X. (2020). IoT network security: Threats, risks, and a data-driven defense framework. IoT, 1(2), 259-285.
18. Salimitari, M., Chatterjee, M., & Fallah, Y. P. (2020). A survey on consensus methods in blockchain for resource-constrained IoT networks. Internet of Things, 11, 100212.
19. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. International journal of critical infrastructure protection, 25, 36-49.
20. Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2017). Security challenges of the Internet of Things. Beyond the Internet of things: Everything interconnected, 53-82.
21. Duncan, A. J., Creese, S., & Goldsmith, M. (2012, June). Insider attacks in cloud computing. In 2012 IEEE 11th international conference on Trust, security and Privacy in computing and communications (pp. 857-862). IEEE.
22. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of Internet of Things architectures and systems. In 2015 international workshop on secure internet of things (SIoT) (pp. 49-57). IEEE.
23. Mughal, A. A. (2022). Well-Architected Wireless Network Security. Journal of Humanities and Applied Science Research, 5(1), 32-42.
24. Igure, V. M., Laughter, S. A., & Williams, R. D. (2006). Security issues in SCADA networks. computers & security, 25(7), 498-506.
25. Miloslavskaya, N., & Tolstoy, A. (2020). IoTBlockSIEM for information security incident management in the internet of things ecosystem. Cluster Computing, 23, 1911-1925.
26. Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering, 16(9), 379-384.
27. Mughal, A. A. (2019). Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. Applied Research in Artificial Intelligence and Cloud Computing, 2(1), 1-31.
28. KS, D., & Ramakrishna, B. (2013). An artificial neural network based intrusion detection system and classification of attacks. International Journal of Engineering Research and Applications, 3, 1959-1964.
29. Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. Applied Sciences, 12(21), 11039.
30. Park, J. H., Salim, M. M., Jo, J. H., Sicato, J. C. S., Rathore, S., & Park, J. H. (2019). CIoT-Net: a scalable cognitive IoT based smart city network architecture. Human-centric Computing and Information Sciences, 9(1), 1-20.
31. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of things, 1, 1-14.
32. Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system: A review of the literature. Online Information Review, 41(2), 171-184.
33. Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018, April). A survey on anomaly based host intrusion detection system. In Journal

of Physics: Conference Series (Vol. 1000, No. 1, p. 012049). IOP Publishing.

34. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.

35. Aldhyani, T. H., & Alkahtani, H. (2023). Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics, 11(1), 233.

36. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science, 10(5).

37. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., ... & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514.

38. Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y., & Sabrina, F. (2021). Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset. IEEE Access, 9, 140136-140146.

39. Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. Computers & Industrial Engineering, 169, 108206.

40. Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions. IEEE Communications Surveys & Tutorials.

41. Veprytska, O., & Kharchenko, V. (2022, December). AI powered attacks against AI powered protection: classification, scenarios and risk analysis. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

42. Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.

43. Li, Y., Wei, X., Li, Y., Dong, Z., & Shahidehpour, M. (2022). Detection of false data injection attacks in smart grid: A secure federated deep learning approach. IEEE Transactions on Smart Grid, 13(6), 4862-4872.

44. Kim, Y. G., Ahmed, K. J., Lee, M. J., & Tsukamoto, K. (2022, August). A Comprehensive Analysis of Machine Learning-Based Intrusion Detection System for IoT-23 Dataset. In International Conference on Intelligent Networking and Collaborative Systems (pp. 475-486). Cham: Springer International Publishing.

45. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017, June). Iot sentinel: Automated device-type identification for security enforcement in iot. In 2017 IEEE 37th international conference on distributed computing systems (ICDCS) (pp. 2177-2184). IEEE.

46. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. Ieee Access, 8, 23022-23040.

47. Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2018). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings 9 (pp. 30-44). Springer International Publishing.

48. Pise, A. A., Almusaini, K. K., Ahanger, T. A., Farouk, A., Pareek, P. K., & Nuagah, S. J. (2022). Enabling artificial intelligence of things (AIoT) healthcare architectures and listing security issues. Computational Intelligence and Neuroscience, 2022.

49. Tyagi, A. K., Dananjayan, S., Agarwal, D., & Thariq Ahmed, H. F. (2023). Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors, 23(2), 947.