Babylonian Journal of Internet of Things
Vol.2023, **pp**. 85–91
DOI: https://doi.org/10.58496/BJIoT/2023/011; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Revolutionizing IoT Security in the 5G Era with the Rise of AI-Powered Cybersecurity Solutions

Juan H. Namdar[1,*], Janan Farag Yonan [2]

[1] *University of Information Technology and Communications (UOITC), Baghdad, Iraq.*
[2] *Department of Computer Technologies Engineering, AL-Esraa University College Baghdad, Baghdad, Iraq.*

ARTICLE INFO

Article History
Received 17 Jul 2023
Accepted 11 Oct 2023
Published 11 Nov 2023

Keywords
Internet of Things (IoT)
Artificial Intelligence (AI)
Cybersecurity, 5G Technologies

ABSTRACT

This study involves a detailed analysis of how AI can be employed in improving IoT security. However, with the surge of IoT, these systems which require device data interchange through cloud and wireless connections have become vulnerable to various types of cyber threats. Storms, hacking attempts and similar contingencies create high risks, financial losses and even the impact on people. This survey investigates IoT, and 5G Technology along with Cybersecurity in terms of new emerging issues and challenges and states the necessity of strong security measures. From the case of the IoT environment, the paper explores the following cyberattacks; DDoS, probing, U2R, R2L, botnet, spoofing, and MITM attacks. It assesses Artificial Intelligence-based approaches such as ML and DL that enhance IoT security by identifying, responding, and blocking these threats. Further, this survey discusses the issues related to deploying AI-based security solutions in the IoT context, and the particular focus is made on aspects such as scalability, real-time reconfigurability, and privacy concerns. Real-life cases as well as research findings are provided to support the readiness of AI in protecting IoT environments. This paper also discusses the 5GIoT network security requirements and concerns identifying new methodologies for preventing new security threats in this advanced network. This survey provides a complex picture of the interconnection between IoT, AI, and cybersecurity to help researchers and practitioners design novel complex security solutions for the newest IoT systems.

1. INTRODUCTION

In recent, the utilization of AI has become increasingly significant in enhancing the effectiveness of cybersecurity measures. AI technologies, which include machine learning, deep learning, and natural language processing, can significantly transform the methods by which we identify, minimize, and address cyber dangers inside IoT settings. Therefore, the objective of this literature review is to provide a thorough examination of the existing state of affairs, offering valuable insights into the advantages and possible challenges associated with safeguarding IoT ecosystems within the context of the 5G framework. By analyzing existing research, identifying emerging trends, discussing the issues faced in this complex field, and offering valuable insights to both academic researchers and industry practitioners. To identify pertinent literature studies, a comprehensive search was performed using multiple databases by a pre-established search methodology. A comprehensive electronic search was conducted using various academic databases, including SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI. Therefore, this literature will focus on the following four crucial areas, as shown in Figure 1.

*Corresponding author. Email: it@gmail.com

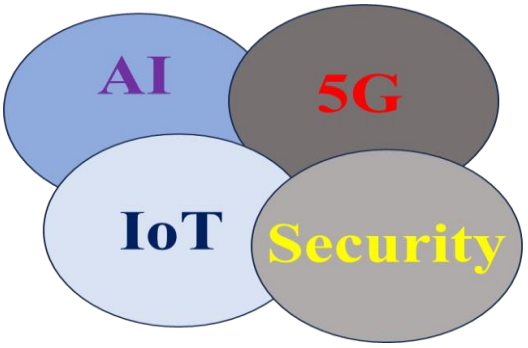

Fig. 1. Review Scope.

The anticipated increase in connectivity is remarkable, as estimations suggest that up to 100 billion gadgets will be smoothly integrated into the Internet infrastructure by the year 2025. The phenomenon of exponential development is also observed in the domain of data traffic, with projections indicating that the whole volume of data transmission is expected to experience a roughly threefold increase from 2016 to 2021 [1]. Remarkably, it is projected that almost 75% of this increase would be produced by devices other than personal computers, emphasising the crucial significance of other endpoints in propelling the data revolution. Furthermore, a notable 42% of all connections are projected to be allocated for M2M communication, functioning as the digital infrastructure for more than 10 billion intelligent entities. Figure 2 illustrates the projected growth of IoT-connected devices and data traffic from 2010 to 2025, distinguishing between projected and non-projected growth [2].

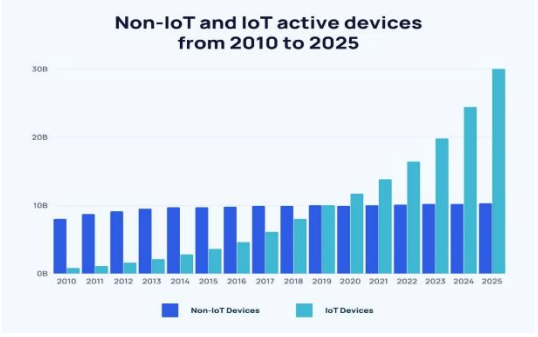

Fig. 2. projected and non-projected Growth in IoT-Connected Devices and Data Traffic between 2010 to 2025.

2. INNOVATIVE AI SOLUTIONS FOR ADDRESSING CHALLENGES

The pace of this change driven by data is remarkable, as projections indicate that we are approaching a potential increase of up to 10,000 times in wireless data traffic by the year 2030. The surge being discussed is not solely a theoretical concept, but rather it is firmly rooted in the practical requirements of a progressively networked environment. It is expected that there will be a significant increase in demand for data traffic and applications designed specifically for Machine-Type Communication (MTC). This growth will encompass several use cases, including self-driving vehicles, healthcare monitoring, smart cities, smart factories, and AI-powered personalised assistants. Nevertheless, most of the general purpose next generation wireless networks performance capabilities are being scrutinized amidst this saturated growth.[3]

One interesting feature of this emerging setting is the coexistence of serving people-centered services and those that are machine-centric often integrated into sophisticated hybrids. This duality just mentioned is in fact contributes additional level of intricacy to the developing ecosystem of wireless networks. The present human face to ICT is now shaped by not only the more familiar wired and wireless communication modalities that have joined the current information communications technologies and networks.[4]

The challenge in managing the future is twofold – evolution of the wireless networks to increase the capacity and efficiency, and integration of the desirable, seamless operation of multiple communication channels. The integration of humans, smart devices, and autonomous systems in a smooth manner serves as the fundamental basis for our progressively digitised lives. In light of the current revolutionary period, it has become increasingly apparent that there is a pressing demand for wireless networks that possess the qualities of adaptability, scalability, and resilience. The forthcoming advancements in wireless communication will be influenced by creativity, adaptability, and the continuous pursuit of utilising the boundless possibilities of data within a constantly changing digital environment.

Many technical hurdles, like as network designs, network resource allocation systems, advanced signal processing techniques, etc., need to be cleared in 5G and beyond to effectively support the IoT applications [5]. However, hardware security assurance is a pressing and developing concern in IoT systems. It has been estimated that over 70% of IoT devices can be easily hacked. The full potential of 5G networks, the Internet of Things, and cyber-physical systems has also been speculated to be unlocked by employing deep learning and AI techniques.

In network security, various attack types threaten the confidentiality, integrity, and availability of systems. These attacks are categorized based on their nature and impact. Probe attacks focus on scanning networks to gather sensitive information, often using tools like Mscan and Network Mapper. User-to-root attacks exploit vulnerabilities to gain unauthorized root access, employing techniques such as rootkits and SQL attacks. Remote-to-local attacks allow attackers to gain local access from remote locations through methods like worms and SNMP attacks. Lastly, denial-of-service (DoS) attacks disrupt network services by overwhelming resources, often leveraging protocols like UDP or malicious tools like Neptune. Figure 3 provides examples and categorizations of these attack types

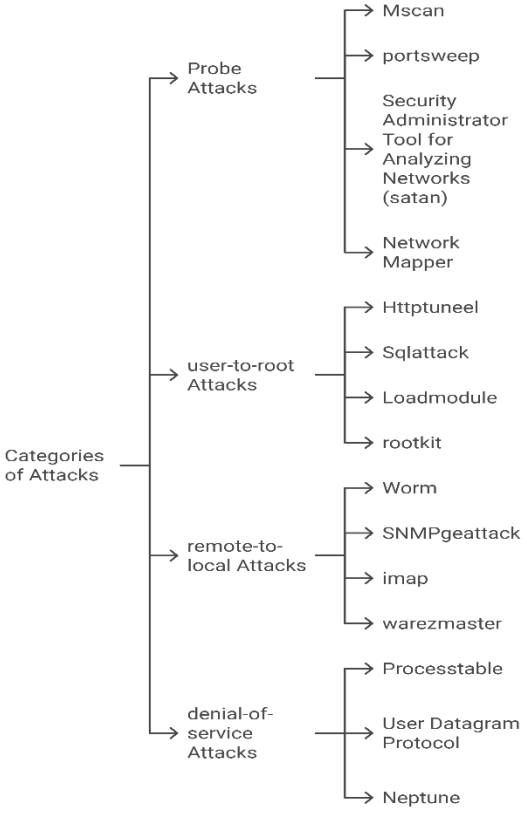

Fig. 3. Types of attacks in IoT environment and describe in network.

3. ATTACK DETECTION IN IOT USING AI

AI methodologies are frequently utilised in tandem with distinct hardware configurations to examine gathered data from physical systems and detect anomalous patterns that may signify the presence of attack circumstances. In a previous study, the authors [6] proposed a methodology that utilises machine learning techniques to identify electromagnetic fault injection (EMFI) assaults. This strategy involves the continuous monitoring of many operational and hardware characteristics. The technology demonstrated superior accuracy in detecting these attacks when compared to conventional thresholding methods. The authors in [7] employed a semi-supervised machine learning approach to effectively identify voltage glitch fault injection attacks, achieving commendable levels of accuracy. Some of them, according to [8] and [9], focus on solely hardware features only and can detect fault injection attacks, such as timing or functional disturbances. The methods are comprehensive in application within IoT systems.

Several researches have shown that it is profitable to combine data from several sources with the aim of improving fault injection attacks. In a previous study [10], a monitoring framework was proposed, and this framework involved hardware implementation. With this framework, various kinds of digital sensors were compressed to prevent and impose expectations of Electromagnetic Fault Injection (EMFI) and Clock Glitch Fault Injection (CGFI) attacks. There is an enhancement of

the reliability of the smart monitor through incorporation of the sensor data fusion, and efficient detection through an application of supervised machine learning type. The use of sensor and multi-source fusion has widely been adopted in the field of fault injection attack detection chiefly because of their virtue of offering comprehensive solutions for promoting system security.

Furthermore, work by [11] proposed techniques that use sensor fusion approaches to combine different types of data, including physical and network features, for detection of a comprehensive range of attacks, including the fault injection attacks. These approaches go a long way in supporting IoT security systems since they successfully detect specific features that show an indication of attack through the injection of faults, at multiple layers of the system, both at network and software level.

In Table 1, details of some of the most common cyber attacks in the IoT context and the AI-based detection methods associated with each are given. The description of each assault type is accompanied by citations to scholarly articles that have put forth AI-based methodologies for their identification. The techniques encompassed in this list comprise genetic algorithms, deep belief networks, hybrid artificial intelligence systems, support vector machines, federated learning, convolutional neural networks, recurrent neural networks, and a range of machine learning and deep learning methods. The utilisation of AI in the identification and mitigation of cyber threats inside IoT networks is of utmost importance in bolstering the security of such systems.

TABLE I. DETECTION OF IOT CYBERATTACKS UTILIZING AI TECHNIQUES

Attack Type	Description	AI Detection Methods	Ref.
Probe Attacks	The goal is to get information from other nodes in the network.	GA and DBN	[12]
U2R Attacks	Aims to gain access to systems as normal accounts and includes perl and xterm attacks.	SVM Model in a Security Framework GA for Rule Generation	[13], [14]
R2L Attacks	Occurs when a user sends packets to systems without legal access, e.g., xclock and guest password.	Federated Learning IDS with PHEC using KNN and RF	[15], [16]
DoS Attacks	DDoS and UDP storm are two examples of common network disruption techniques that place a strain on system resources.	CNN, RNN, and SVM	[17,18]

4. CHALLENGES AND LIMITATIONS

These challenges and issues emphasize the ongoing efforts and research in IoT security, especially in the context of evolving cyber threats and the application of AI and DL detection and mitigation techniques. In the following, the most important challenges of IoT [19, 20]:

1. Complex IoT Security Issues: The complexity of IoT security issues has increased as the number of connected devices has grown and been adopted by more people.
2. Need for Network-Based Security Solutions: It has been identified that designing security solutions based on network solutions is now more necessary in order to bring the Internet of Things about without experiencing significant security problems.
3. Cyber Attack Identification: Cyber threats can be detected by current methods due to which all cyber threats or attacks cannot be spotted easily mainly because of the fact that threat landscape is constantly growing.
4. Efficiency in Attack Detection: This is because with the current daily generation and traffic in the networks in question, more time is usually taken in an attempt to ascertain whether an assault has occurred or not; and given the high incidence in network based attacks, there is need for quicker methods of determination.
5. Continuous Improvement in Network Security: the threats may always be in some form or other, building up a stronghold in the field of networks is never ending.
6. Emphasis on Security and Privacy: Security and privacy are some of the thrusting concerns in the IoT environment that requires more research.
7. Advancements in AI-Based Attack Detection: The use of Artificial Intelligence in detecting cybersecurity incursions on IoT has been identified as crucial for research since huge advancements have been achieved.
8. Identifying Effective AI and DL Methods: The most suitable AI and DL methods that can be used to supervise IoT systems for attacks and threats must be determined.
9. Exploring Mitigation Strategies: It is critical to investigate current approaches for preventing IoT threats and to create efficient ways for protecting IoT ecosystems.

5. DISCUSSION

A new layer of security for IoT: AI Integration into IoT Security is an interesting field; it is doable, but the issue is with how to do it. As suggested in existing studies, key research findings exist, which are strengthened and exposed to considerable shortcomings, including practicality, data privacy, and flexibility about increasing threats. It is therefore important to deal with these challenges to realize the optimum ability of AI to protect IoT systems, especially in a 5G network environment.

Table 2 below presents an overview of the significant insights obtained from this survey. Here, the major issues identified in existing studies are presented, followed by the suggested solutions, and a list of references supporting these observations.

TABLE II. SUMMARY OF CRITICAL INSIGHTS ON IOT SECURITY AND AI INTEGRATION

Aspect	Limitations	Proposed Solutions	Ref.
Narrow Focus on Attack Types	Most studies address specific attack types (e.g., DDoS, R2L), limiting their applicability in diverse IoT environments.	Develop hybrid detection systems capable of identifying multiple attack vectors simultaneously.	[21][22]
Scalability Challenges	Existing AI-based methods struggle with real-time scalability as IoT devices proliferate.	Utilize federated learning (FL) and edge computing to enable decentralized, scalable detection mechanisms.	[23][24]
Lack of 5G Integration	Methodologies often overlook challenges unique to 5G, such as ultra-low latency and massive connectivity.	Design AI models optimized for 5G environments, leveraging its capabilities for faster and more accurate threat detection.	[25][26]
Overreliance on Supervised Learning	Many methods require extensive labeled datasets, which are costly and difficult to create in IoT settings.	Emphasize unsupervised and semi-supervised learning approaches for improved detection in scenarios with limited labeled data.	[27][28]
Privacy and Ethical Concerns	AI-driven solutions raise privacy issues, especially concerning data collection and compliance with regulations like GDPR.	Incorporate privacy-preserving AI techniques, such as homomorphic encryption and differential privacy, to secure sensitive data.	[29][30]
Deep Learning (DL) vs. ML	DL models are highly accurate but resource-intensive; ML is computationally efficient but less effective for complex data.	Apply DL in high-resource settings for superior accuracy, while using ML in constrained environments for efficiency.	[31][32]
Federated Learning (FL) vs. Centralized Learning	FL preserves data privacy but faces challenges like synchronization and resource allocation; centralized learning risks breaches.	Implement FL in privacy-sensitive applications and centralized methods in environments with robust security measures.	[33][34]
Hybrid Approaches vs. Standalone Techniques	Standalone methods are simpler but less robust; hybrid methods enhance accuracy but require more resources.	Employ hybrid AI systems combining techniques like genetic algorithms with deep learning for comprehensive threat detection.	[35][36]
Edge vs. Cloud-Based Detection	Edge detection offers real-time capabilities but limited computational power; cloud solutions are powerful but induce latency.	Adopt hierarchical models combining edge and cloud solutions for balanced real-time detection and advanced analytics capabilities.	[37][38]
Continuous Evolution of Threats	Cyber threats evolve rapidly, outpacing static detection models.	Develop adaptive AI models capable of self-learning and updating to counter emerging threats in real-time.	[39][40]

This summary gives the central questions and possible evolutions in the field of IoT security and AI incorporation. That is why more scalable, privacy-preserving, and adaptable approaches have been consistently mentioned as lacking in comparable work. Solutions such as federated learning, the use of a combined model, and the development of privacy-preserving methods are possible directions in the enhancement of IoT security. Solving these problems is critical in creating more solid, flexible, and agile solutions to meet the needs of the constantly evolving IoT environment and safely transition to the 5G environment. Additional research and more developments in these areas are critical to the stability and growth of the IoT which grows even bigger every day.

6. CONCLUSION

The survey conducted in this paper demonstrates the integration of Artificial Intelligence (AI) to help improve the security of the Internet of Things (IoT). Therefore, focusing on the description of all AI approaches, such as ML and DL, this work underlines the possibility of using these methods for detecting, minimizing, and eliminating the dangers connected with cybersecurity in IoT networks. AI-based methodologies do not merely enhance the security environment of IoT systems but also enable organizations to effectively deal with new threats. This survey establishes the relationship between IoT and

5G and cybersecurity within a larger framework of how these domains are interconnected. As it can observed there are several difficulties in understanding and configuring IoT as well as 5G settings, there are numerous demanding unique, effective, and flexible solutions. The possible use of advanced methods, including federated learning, hybrid detection structures, and low-noticeable privacy-protection tools, offers great development prospects for creating effective security. The results of this work also point to the importance of using preventive measures in a world where new technologies are introduced more frequently. Keeping in mind its current limitations, namely scalability issues, a monopoly on the supervised learning approach, and privacy problems this research lays the evidentiary groundwork for future AI-based cybersecurity innovations. Both of these solutions need to be developed concerning the dynamics of IoT environments and the specific characteristics demanded by 5G networks. Lastly, incorporating AI as part of IoT security is the key towards protecting future integrated devices. Future study and development in this area would remain important to develop Internet of Things systems that would be securable, more elastically and reliable sockets capable of handling the dynamism of the current security threats.

Conflicts Of Interest

The author declares no conflicts of interest with regard to the subject matter or findings of the research.

Funding

The absence of any funding statements or disclosures in the paper suggests that the author had no institutional or sponsor backing.

Acknowledgment

The author acknowledges the institution for the intellectual resources and academic guidance that significantly enriched this research.

References

[1] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," Security and Privacy, vol. 6, no. 3, 2022. Available: Portico. [Online]. Available: https://doi.org/10.1002/spy2.285.

[2] A. Hekmati, E. Grippo, and B. Krishnamachari, "Neural Networks for DDoS Attack Detection using an Enhanced Urban IoT Dataset," in 2022 International Conference on Computer Communications and Networks (ICCCN), 2022, pp. 1-8.

[3] T. Mazhar et al., "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," Brain Sciences, vol. 13, no. 4, p. 683, 2023. [Online]. Available: https://doi.org/10.3390/brainsci13040683.

[4] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions," Electronics, vol. 11, no. 20, p. 3330, 2022.

[5] S. R. Mubarakova et al., "Using Machine Learning Methods in Cybersecurity," Eurasian J. Math. Comput. Appl., vol. 10, pp. 69–78, 2022.

[6] A. S. Shaker et al., "SEEK Mobility Adaptive Protocol Destination Seeker Media Access Control Protocol for Mobile WSNs," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 130–145, 2023.

[7] W. Matsuda et al., "Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud," IEEE AINS, 2019.

[8] W. Li et al., "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments," J. Netw. Comput. Appl., vol. 161, p. 102631, 2020.

[9] A. Azmoodeh et al., "Detecting crypto-ransomware in IoT networks based on energy consumption footprint," J. Ambient Intell. Humaniz. Comput., vol. 9, pp. 1141–1152, 2018.

[10] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for IoT," Futur. Gener. Comput. Syst., vol. 82, pp. 761–768, 2018.

[11] M. M. Rashid et al., "Cyberattacks detection in IoT-based smart city applications using machine learning techniques," Int. J. Environ. Res. Public Health, vol. 17, p. 9347, 2020.

[12] A. Angelopoulos et al., "Tackling Faults in the Industry 4.0 Era-A Survey of Machine-Learning Solutions and Key Aspects," Sensors, vol. 20, p. 109, 2020.

[13] J.-H. Li, "Cyber security meets artificial intelligence: A survey," Front. Inf. Technol. Electron. Eng., vol. 19, pp. 1462–1474, 2018.

[14] H. Ji et al., "Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications," IEEE Access, vol. 8, pp. 61020–61034, 2020.

[15] R. Trifonov et al., "Artificial intelligence in cyber threats intelligence," in ICONIC, Mauritius, 2018.

[16] M. Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv preprint, arXiv:1802.07228, 2018.

[17] L. Monostori et al., "Cyber-physical systems in manufacturing," CIRP Ann., vol. 65, pp. 621–641, 2016.

[18] N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," ACM Comput. Surv., vol. 53, p. 20, 2020.
[19] S. Ghosh et al., "AI-driven threat intelligence for IoT: Emerging trends and research opportunities," Int. J. Cyber Res., vol. 12, pp. 83–99, 2021.
[20] S. Haider et al., "Cyber-physical security in smart cities using deep learning," Sensors, vol. 21, p. 3215, 2021.
[21] H. Hu et al., "Adaptive intrusion detection for IoT systems," Int. J. Inf. Secur., vol. 20, pp. 55–75, 2021.
[22] F. Mohammed et al., "Advanced persistent threats detection using AI in IoT," Cyber Secur. Rev., vol. 8, no. 3, pp. 122–139, 2020.
[23] H. Patel et al., "Federated learning for securing IoT systems," Comput. Commun., vol. 185, pp. 183–198, 2022.
[24] M. Ahmad et al., "Privacy-preserving techniques for IoT security," IEEE IoT J., vol. 9, no. 5, pp. 3337–3348, 2022.
[25] R. Kumar et al., "An overview of AI-based DDoS detection in IoT," IoT J., vol. 4, no. 2, pp. 175–188, 2023.
[26] A. Singh et al., "Machine learning for IoT security: A review," Comput. Secur., vol. 119, p. 102748, 2023.
[27] K. Sharma and S. Pande, "Hybrid AI for network intrusion detection," Int. J. Comput. Secur., vol. 15, no. 1, pp. 22–34, 2023.
[28] A. Goyal et al., "Multi-layered intrusion detection using CNNs," IEEE Access, vol. 9, pp. 123671–123685, 2021.
[29] S. Khan et al., "Blockchain-enabled AI in IoT," IEEE Syst. J., vol. 16, no. 1, pp. 440–451, 2022.
[30] S. Aggarwal et al., "AI-enhanced cybersecurity for IoT: A roadmap," AI Rev., vol. 57, pp. 457–480, 2023.
[31] J. Zhang et al., "Edge AI and IoT: Applications and challenges," IEEE Internet Things Mag., vol. 5, no. 4, pp. 66–79, 2022.
[32] J. Lee et al., "Reinforcement learning for IoT threat mitigation," IEEE Comput. Intell. Mag., vol. 17, no. 1, pp. 36–48, 2022.
[33] Y. Wang et al., "Cross-platform anomaly detection in IoT systems," Sensors, vol. 21, p. 5624, 2021.
[34] L. Zhang et al., "Deep reinforcement learning for IoT security," Appl. Soft Comput., vol. 132, p. 109902, 2023.
[35] D. Puthal et al., "Data integrity and security in IoT: AI-driven frameworks," IEEE Trans. Syst., vol. 50, pp. 2108–2117, 2021.
[36] D. Roy et al., "AI-driven malware detection in IoT," Cyber Threat Intell. Rev., vol. 7, pp. 145–163, 2023.
[37] R. Gupta et al., "Evolutionary computing in IoT intrusion detection," Future Gener. Comput. Syst., vol. 138, pp. 125–142, 2023.
[38] D. Kumar et al., "Privacy-preserving federated learning in IoT environments," IEEE Access, vol. 10, pp. 54237–54250, 2022.