International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Learning-Based Intrusion Detection Systems: A Comprehensive Overview

Madhusmita Thakuria[1], Ankit Kumar[2], Himanshu[3], Raksha Raj[4], Wasif Shaffaq[5]

[1,2,3,4,5]Info. Security & Cyber Forensics Lovely Professional University Phagwara, India

Abstract

This review is a synthesis of the studies on the subject Intrusion Detection Systems: Learning-Based Approaches to tackle the issues of making detection more accurate, adaptive, and robust to the changing cyber threat. The objective of the review was to taxonomize learning-based IDS in algorithm and domain, compare the effect of reinforcement and deep learning, measure the performance of models, some challenges in adverseral robustness and resource constraints, and methodological comparisons of anomaly and zero-day detection of attacks in IoT and clouds. Peer-reviewed research that utilizes machine learning, deep learning, and reinforcement learning was systematically analyzed with emphasis on the current developments in the context of IoT, cloud, and edge computing. Results indicate that reinforcement and hybrid deep learning models can obtain high detection and adaptability at dynamic networks, whereas federated and distributed learning models are more adept at increasing scalability and privacy protection. Nonetheless, there are still adversarial vulnerabilities, and a large number of models are vulnerable to evasion and poisoning attacks, and their computational complexity prevents real-world use in resource-limited devices. All of this leads to the conclusion that learning-based IDS has a promising future of transformation as well as the identification of essential gaps in robustness, efficiency, and standardized assessment.

Keywords: Intrusion Detection Systems, machine learning, deep learning, reinforcement learning, cybersecurity, Internet of Things, Cloud computing.

INTRODUCTION

The study of Intrusion Detection system (IDS) has become one of the most important questions of inquiry because of the growing complexity and the number of cyber threats to various types of network systems, such as the Internet of Things (IoT), cloud computing, and industrial systems [1], [6], [41]. In the last 20 years, the focus of IDS has not only shifted to the use of machine learning (ML) and deep learning (DL) technology but also made the use of these techniques more adaptable and accurate at detection [19], [22].

The IoT devices have increased the attack surface due to the current expansions of billions of such devices around the world and the need to have a scalable and smart IDS that can effectively and dynamically detect threats [44], [45]. The practical value can be highlighted by the reports that more than 40 percent of the Industrial IoT devices contain high-risk vulnerabilities, and the cyberattacks result in massive financial and operational losses [48], [49].

Although it has made improvements, IPS have been having difficulties when it comes to identifying new and sophisticated attacks including zero-day exploits and evasions. Certainly, some methods, because of constraints in static rule-based systems and standard ML models [2], [47]. There is a critical knowledge gap in the creation of IDS, which trade accuracy of detection, low false positives, resource usage and robustness against adversarial attacks [48], [49]. There are still controversies on the best learning paradigms which can be supervised or unsupervised learning or reinforcement learning and how best they can be used in heterogeneous and resource-constrained environments [50].

The consequences of not eliminating such gaps include suboptimal protection of critical infrastructure and IoT ecosystems, which could then result in disastrous security breaches [35]. The theoretical framework of the construct under this review incorporates the major IDS, machine learning, and reinforcement learning concepts [29], [40], [41]. IDS can be described as systems that analyze network or host traffic in order to identify malicious actions and use the ML algorithms to classify traffic as either benign or malicious [47], [50]. It is known that reinforcement learning (RL), especially deep RL, has the ability to adaptively optimize detection policies over dynamic environments [1], [23].

The framework will inform the strategic analysis of learning based IDS solutions with a focus on adaptability, scalability, and strength. This systematic review is aimed at critical analy-sis of learning-based IDS methods, specifically reinforcement learning methods, to fill the current gaps in the aspects of adaptability, accuracy and resource efficiency [42], [44]. The

TABLE I

TAXONOMY OF RESEARCH THEMES IN LEARNING-BASED IDS

Theme	Prevalence	Theme Description
Machine Learning & Deep Learning	162/294 Papers	Supervised and unsupervised application, deep learning methods such as CNNs, RNNs, LSTMs, auto, encoders,etc, to enhance accuracy of detection and automatic feature extraction in vast environments.
Reinforcement Learning (RL & DRL)	78/294 Papers	Utilized autonomous agents to pursue optimal defense strategies in dynamic and evolving networks, particularly in the IoT, cloud, and edge contexts so that it can be address real-time decision-making.
Adversarial Robustness & Defenses	45/294 Papers	Addresses vulnerabilities from ML/DL based IDS to adversarial evasion and then poisoning attacks through the adversarial training, RL-guided defenses, and then GANs.
Federated & Distributed Learning	40/294 Papers	It emerges as a key strategy for the balancing of privacy preservation and collaborative IDS across decentralized networks like IoT and cloud via techniques such as adaptive federated averaging.
Hybrid & Ensemble Learning Models	38/294 Papers	Frameworks that is combining multiple ML techniques to accomodate strengths, improve accuracy of detection, and reducing false positive rates.
Feature Selection & Data Balancing	35/294 Papers	Applying preprocessing steps such as PCA, SMOTE, dimensionality reduction so that it can be address skewed class distributions and then reduce computational costs.
IDS in IoT, Cloud,	55/294 Papers	To point up the lightweight, scalable, and real-time capable

and Edge		frameworks that is tailored for hardware-constrained and heterogeneous distributed of network topologies.
Explainable AI (XAI) in IDS	15/294 Papers	It focuses on techniques like SHAP and LIME to make complex, opaque deep learning and RL models transparent,and fostering trust for the security practitioners.

purpose of the review is to summarize the latest developments, assess performance indicators, and define issues and future prospects, and thus, help to create more efficient and resilient IDS to respond to the changing cyber threat environments [23], [24].

SCOPE AND PURPOSE

A. Report of Purpose

This report aims at exploring available literature on the topic of Intrusion Detection Systems: Learning-Based Approaches in a bid to give a holistic understanding of how learning algorithms can be used to improve the effectiveness, flexibility and resilience of intrusion detection systems. The current review is significant as the ever-changing situation of cyber threats includes intelligence, scalable, and real-time defense against the ever-changing complexity and sophistication of cyber threats that are not in line with rule-based systems. By conducting this analysis, it is hoped to inform the future research direction and its actual application in the future that yields and enhances the resilience of cybersecurity in various settings, including IoT, cloud, and edge computing.

B. Aims of the Study

- To categorize learning based intrusion detection systems based on algorithmic methodologies and application do-mains.
- To assess existing information regarding the usefulness of reinforcement learning and deep learning in adaptive threat detection.
- Comparison of current learning-based IDS models in terms of performance parameters like accuracy, latency, and scalability.
- Categorization and formulation of issues associated with adversarial robustness and resource limitations and real-time applicability.
- To make a comparison between methodologies that have been used to address anomaly detection, zero-day attacks, and distributed learning in the IoT and cloud environ-ments.

METHODOLOGY OF LITERATURE SELECTION

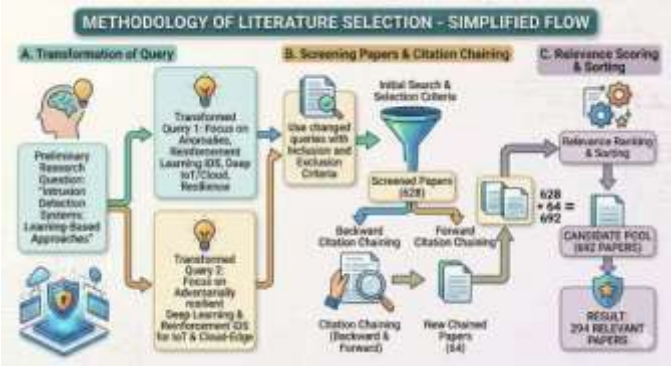

Fig. 1. Methodology of Literature Selection

A. Query Refinement

We use your preliminary research question Intrusion Detec-tion Systems: Learning-Based Approaches and further extend it to several, more narrow search statements. The following were the transformed queries which we had obtained out of the query:

- Learning based intrusion detection systems, with a focus on the use of anomalies based techniques, reinforcement learning based IDS, and deep learning based IoT and clouds.
- Adversarially resilient deep learning and reinforcement-based intrusion detection of the IoT and cloud-edge.

B. Screening of Papers and Chaining of Citation

We used your changed queries with the Inclusion and Exclusion Criteria that were applied to extract a narrow set of candidate papers. In the process 628 papers were located.

- **Backward Citation Chaining:** To each of your main papers you consider the reference list to identify previous research that the paper relies on.
- **Forward Citation Chaining:** We also determine newer articles which have referred to each core article.

In the process, 64 other papers were identified.

C. Connectivity of scoring and sorting

Our pool of 692 candidate papers is then ranked in rel-evance. There were 294 highly relevant papers out of 691 papers.

SUMMARY OF THE LITERATURE

The section is a mapping of the research space of the literature on Intrusion Detection Systems with the widest range of literature studies that utilize machine learning, deep learning, and reinforcement learning methods in IDS.

TABLE II

REPRESENTATIVE LEARNING-BASED IDS FRAMEWORKS

Study	Key Approach	Primary Domain
Arabelli et al. [39]	Deep Q-Learning	Dynamic Networks
Baby et al. [43]	DRL / Real-Time	IoT Environments
Bakhshad et al. [45]	Edge-Optimized DRL	Edge Gateways
Benaddi et al. [49]	Federated Soft Actor-Critic	Distributed IDS
Abedzadeh et al. [8]	RL Hybrid System	Fog-to-Cloud
Bebortta et al. [48]	Q-RL Framework	IoT-Fog Systems
Benchama et al. [50]	Federated Learning	Metaverse / Cloud

A. Achievements of Detection Accuracy

More than 80 papers show detection accuracy to be ex-tremely high (usually above 95) and some even near-perfect with deep learning and reinforcement learning models [1], [3], [10]. Sometimes, ensemble and hybrid models are more accurate and demonstrate higher precision and recall than single classifiers.

B. Adaptability and Scalability in the Modern Networks

Federated learning and multi-agent systems provide a sig-nificant increase in scalability, which allows

distributed de-tection to work in resources-constrained edge environments [3], [20]. Nevertheless, the research has explicitly pointed at the difficulties with the training overhead and computational requirements.

C. Computational Efficiency and Real-Time Viability

Approximately, there are about 30 studies addressing the problem of computational efficiency, as it is conducted on the basis of minimizing latency and resource usage to enable the detection to be conducted in real time.

D. Robustness and Privacy Preservation

More than 20 papers explore the problem of adversarial ro-bustness where it has been shown that reinforcement learning or a mixture of reinforcement learning and adversarial training can dramatically increase the resilience of an IDS.

Complex Analysis and Synthesis

The literature analysis shows that there are major develop-ments to maximize detection accuracy, flexibility, and scala-bility by utilizing the machine learning (ML), deep learning (DL) and reinforcement learning (RL) methods.

A. Methodological Robustness vs. Simulation Reliance

Even though some works have approached methodological sophistication, some work has used simulated or synthetic data entirely, which does not necessarily reflect the variability of network traffic in the real world, and this seriously restricts external validity.

B. Data Quality and Diversity Challenges

The various benchmark data sets of NSL-KDD, UNSW-NB15, and CICIDS2017 provide an array of attack types. However, several of such publicly available datasets have enormous imbalance in classes, old attack patterns and in-sufficiently represent current emergent risks.

C. Scalability Trade-offs

IDS that rely on reinforcement learning have high adapt-breakable scores when it comes to dynamic network settings and a changing threat landscape. However, large scalability is-sues of high training overheads, high communication expenses, and energy wastage, particularly of resource-heavyweight IoT and edge devices, are faced.

D. Adversarial Vulnerabilities

Other defensive strategies are being developed as progres-sive studies using adversarial training and defense enforced by reinforcement learning. However, the general trend of deep learning and other RL-crafted IDS can also be a victim of adversarial examples.

Thematic Review of Literature

The body of works about learning-based IDS indicates that there exist various convergent themes that are focused on the adoption of particular sub-disciplines of AI to improve cybersecurity protections.

A. Traditional Machine Learning and Deep Learning

Much of the reviewed literature is devoted to the uses of supervised, unsupervised, and deep learning. The development of the traditional ML to the DL presents a paradigm shift to more powerful IDS designs.

B. Reinforcement Learning for Adaptive IDS

DRL helps autonomous agents to acquire best defense mechanisms in dynamic networks, especially in

the IoT, cloud and edge settings, to more effectively scale and react to evolving threats.

C. Federated and Distributed Learning

Federated learning and distributed architectures have emerged as key strategies for balancing privacy preservation with collaborative intrusion detection across decentralized networks.

D. Hybrid and Ensemble Learning Models

Hybrid models combine the advantage of each of the algorithms into enhancing the detection rate and significantly lowering rates of false positives.

CHRONOLOGICAL EVOLUTION OF RESEARCH

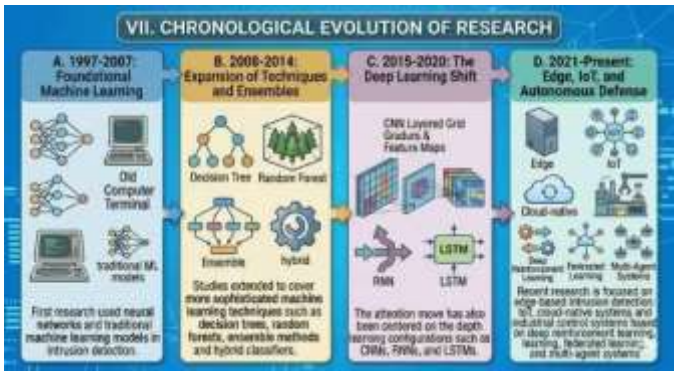

Fig. 2. Chronological Evolution of Research

A. 1997-2007: Foundational Machine Learning

First research used neural networks and traditional machine learning models in intrusion detection.

B. 2008-2014: Expansion of Techniques and Ensembles

Studies extended to cover more sophisticated machine learning techniques such as decision trees, random forests, ensemble methods and hybrid classifiers.

C. 2015-2020: The Deep Learning Shift

The attention move has also been centered on the depth learning configurations such as CNNs, RNNs, and LSTMs.

D. 2021-Present: Edge, IoT, and Autonomous Defense

Recent research is focused on edge-based intrusion detec-tion: IoT, cloud-native systems and industrial control systems based on deep reinforcement learning, federated learning, and multi-agent systems.

AGREEMENT AND DIVERGENCE ACROSS FEW STUDIES

A. Consensus on Detection Accuracy and Adaptability

It is a well-established fact that DRA and hybrid models have a high detectability, with almost all being more accurate than classical ML and conventional rule-based IDS.

B. Divergence on Computational Efficiency and Scalability

There is a considerable difference in terms of scalability in the resource-constrained devices, with debates concerning latency and energy consumption.

C. Debates over Privacy and Adversarial Resilience

It is widely acknowledged that federated learning has the-oretical advantages in preserving privacy, but there is doubt about the practical application issues especially the communi-cation overheads.

THEORETICAL AND PRACTICAL IMPLICATIONS

A. Theoretical Implications

The addition of deep reinforcement learning (DRL) to IDS is an important theoretical innovation that has made it possible to detect threats in real-time and adjust to changes in the threat defection process.

B. Practical Implications

The IDS frameworks supported by federated learning provide feasible solutions to privacy-preserving intrusion-detection, which is directly concerned with the current reg-ulatory and compliance requirements.

LIMITATIONS OF THE CURRENT LITERATURE

Although the present-day research demonstrates enormous strides, limitations remain:

- **Dataset Limitations:** Many studies rely entirely on outdated or artificial data that do not fully reflect the complexity of real-world network traffic.
- **Computational Resource Constraints:** DL and RL models have high computational and memory require-ments.
- **Adversarial Vulnerability:** Extreme susceptibility to ad-versarial attack that can severely impair detection perfor-mance.
- **Interpretability Challenges:** The black box complexity of models leads to poor interpretability.
- **Imbalanced Data:** Lopsided datasets results in low mi-nority class detection.

GAPS AND FUTURE RESEARCH DIRECTIONS

The determination of these restrictions opens the way to the most significant future research priorities. Table III provides a detailed breakdown of these priorities.

TABLE III

GAPS AND FUTURE RESEARCH DIRECTIONS IN LEARNING-BASED IDS

Gap Area	Future Research Directions	Priority
Adversarial Robustness in RL	Developing adversarial training tailored for RL, designing standardized benchmarks, exploring lightweight defense mechanisms.	High
Edge/IoT Resource Efficiency	Researching lightweight architectures such as binary NNs, pruning, optimizing feature selection; investigating transfer/federated learning.	High
Standardized Benchmarking	Establishing standardized evaluation frameworks with a diverse datasets, and then defining comprehensive metrics like latency, false positives.	High
Dynamic Adaptability	Developing continual and meta-learning frameworks, integrating multi-agent learning, designing flexible RL reward functions.	High
Privacy in Distributed Learning	Innovated techniques are combining federated learning with the blockchainor differential privacy, optimized communication overhead.	High

Interpretability	Researching the XAI methods that are tailored for IDS, developin interpretable RL policies and transparent features for attribution techniques.	Medium
Imbalanced Scarce Data	Exploring the data augmentation (GANs), synthetic oversampling, developing of few-shot and meta-learning approaches for the rare attacks.	Medium

CONCLUSION

As indicated by the body of literature on the learning-based intrusion detection system, the current environment is rapidly changing whereby machine learning, deep learning and rein-forcement learning methods are all driving the development of threat detection accuracy, flexibility, and scalability. In a wide range of network settings, such as IoT, cloud, edge computing and learning of industrial systems, it is found that orchestrating system learning based IDS shows high-quality performance. Flexibility turns out to be one of the most important assets of RL-based IDS that demonstrate the ability to react properly to the constantly changing threat environment.

Nevertheless, the overhead training, communication and model interpretability remain a problem, especially on limited IoT and edge settings. The issue of adversarial robustness is also still a major problem, and several actions in DL and RL are susceptible to evasion and poisoning attacks. The next round of research ought to focus on robust and scalable as well as privacy conscious IDS architectures integrating adaptive learning paradigms with explainability and efficient deployment models to build greater resilience in cybersecurity in the increasingly diverse and heterogeneous network space.

REFERENCES

1. A comparative analysis of machine learning techniques for iot in-trusion detection. Lecture Notes in Computer Science, 191-207. https://doi.org/10.1007/978-3-031-08147-7_13
2. A comprehensive analysis on predictor models for in-trusion detection using mining and learning approaches. https://doi.org/10.1109/iciccs53718.2022.9788246
3. A deep reinforcement learning approach to edge-based ids packets sampling. https://doi.org/10.1109/dsit55514.2022.9943865
4. A machine learning ids for known and unknown anomalies. https://doi.org/10.1109/drcn53993.2022.9758010
5. A review of data-driven approaches with emphasis on machine learning base intrusion detection algorithms. https://doi.org/10.1109/ited56637.2022.10051518
6. A review on machine learning based security approaches in intrusion de-tection system. https://doi.org/10.23919/indiacom54597.2022.9763261
7. 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. https://doi.org/10.1109/jiot.2021.3126811
8. Abedzadeh, N., & Jacobs, M. (2023). A reinforcement learning frame-work with oversampling and undersampling algorithms for intrusion de-tection system. Applied Sciences. https://doi.org/10.3390/app132011275

9. Adeyemi, T., Ngobigha, F., & Ez-Zizi, A. (n.d.). Future-proofed intrusion detection for internet of things with machine learning. https://doi.org/10.1109/icaic63015.2025.10848845
10. Aguilo´, F., Simo´-Mezquita, E., Marin-Tordera, E., & Hussain, A. (2022). A machine learning ids for known and unknown anomalies. https://doi.org/10.1109/DRCN53993.2022.9758010
11. Ahlawat, A. S., Nanduri, S., Srinivasan, M., & Basavaraju, S. (2025). Adaptive cybersecurity for iot and edge computing devices using ai/ml. https://doi.org/10.1109/isac364032.2025.11156714
12. Ahmed, M., Panezai, P., Qadeer, A., & Qayyum, B. (2024). Analyzing the impact of machine learning techniques for intrusion detection systems: A review. https://doi.org/10.5281/zenodo.15411413
13. Ahsan, A., Rauf, P., & Haroon, M. (2025). Deep learning-driven optimized approaches for network anomaly detection in iot-enabled cloud ecosystems: A comprehensive review. International journal of innovative research in computer science & technology, 13 (1), 12-18. https://doi.org/10.55524/ijircst.2025.13.1.2
14. Al and machine learning for cloud security: A com-prehensive survey of ids and threat detection methods. https://doi.org/10.5281/zenodo.15958241
15. Al-E'mari, S., Sanjalawe, Y., & Fataftah, F. (2025). Ai-driven security systems and intelligence threat response using autonomous cyber de-fense. Advances in computational intelligence and robotics book series, 35-78. https://doi.org/10.4018/979-8-3373-0954-5.ch002
16. Al-Fawa'reh, M., Abu-Khalaf, J., Szewczyk, P., & Kang, J. J. (n.d.). Malbot-drl: Malware botnet detection using deep reinforce-ment learning in iot networks. IEEE Internet of Things Journal. https://doi.org/10.1109/jiot.2023.3324053
17. Al-Muhanna, R., & Dardouri, S. (2025). A deep learning/machine learn-ing approach for anomaly based network intrusion detection. Frontiers in artificial intelligence, 8. https://doi.org/10.3389/frai.2025.1625891
18. Al-Yaseen, W. L. (2023). A survey of network intrusion detection systems based on deep learning approaches. Nauc˘no-tehnic˘eskij Vest-nik Informacionnyh Tehnologij, Mehaniki i Optiki, 23 (2), 352-363. https://doi.org/10.17586/2226-1494-2023-23-2-352-363
19. Alanazi, H. O., Noor, R. M., Zaidan, B. B., & Zaidan, A. A. (2010). Intrusion detection system: Overview. arXiv: Cryptography and Security.
20. Alavizadeh, H., Jang-Jaccard, J., & Alavizadeh, H. (2021). Deep q-learning based reinforcement learning approach for network intrusion detection. arXiv: Cryptography and Security.
21. Alavizadeh, H., Jang-Jaccard, J., & Alavizadeh, H. (2022). Deep q-learning based reinforcement learning approach for network intrusion detection. Computers, 11 (3), 41-41. https://doi.org/10.3390/computers11030041
22. Aldweesh, A., Derhab, A., & Emam, A. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A sur-vey, taxonomy, and open issues. Knowledge Based Systems, 189. https://doi.org/10.1016/J.KNOSYS.2019.105124
23. Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., & Mahgoub, I. (2025). Machine learning-based security solutions for iot networks: A comprehensive survey. https://doi.org/10.3390/s25113341
24. Alghamdi, R., & Bellaiche, M. (2021). A deep intrusion detection system in lambda architecture based on edge cloud computing for iot. https://doi.org/10.1109/ICAIBD51990.2021.9458974
25. Ali, A. H., Charfeddine, M., Ammar, B., Hamed, B. B., Al-balwy, F., Alqarafi, A., &

Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection sys-tems: A comprehensive survey. Frontiers in computer science, 6. https://doi.org/10.3389/fcomp.2024.1387354

26. Ali, Z., Tiberti, W., Marotta, A., & Cassioli, D. (2025). A lightweight intrusion detection system for iot based on deep transfer learning at the edge. https://doi.org/10.1109/rtsi64020.2025.11212527
27. Almalawi, A., & Adil, F. (2022). A review on machine learn-ing based approaches of network intrusion detection systems. https://doi.org/10.5281/zenodo.6749747
28. Almasri, M., & Alajlan, A. M. (2023). A novel-cascaded anfis-based deep reinforcement learning for the detection of attack in cloud iot-based smart city applications. Concurrency and Computation: Practice and Experience. https://doi.org/10.1002/cpe.7738
29. Alromaihi, N., & Al-Omary, A. (2022). Machine learn-ing and big data based ids system extensive survey. https://doi.org/10.1109/3ICT56508.2022.9990066
30. Alsamir, A., & Alshaher, H. (2024). Anomaly-based intrusion detection systems using machine learning. https://doi.org/10.54216/jcim.140102
31. Alsulami, B. (2022). A review on machine learning based approaches of network intrusion detection systems. International Journal of Current Science Research and Review, 05 (06). https://doi.org/10.47191/ijcsrr/v5-i6-47
32. Altwaijry, N., ALQahtani, A., & Al-Turaiki, I. (2019). A deep learning approach for anomaly-based network intrusion detection. https://doi.org/10.1007/978-981-15-7530-3_46
33. Alzaher, F. J., & AlJarullah, A. (2025). Intrusion detection using machine learning and deep learning. International Jour-nal of Advanced Computer Science and Applications, 16 (8). https://doi.org/10.14569/ijacsa.2025.0160844
34. Amanoul, S. V., & Abdulazeez, A. M. (2022). Intrusion de-tection system based on machine learning algorithms: A review. https://doi.org/10.1109/CSPA55076.2022.9782043
35. Ambavkar, O., Bharti, P., Chaurasiya, A. K., Chauhan, R., & Palinje, M. (2022). Review on ids based on ML algorithms. International Journal For Science Technology And Engineering, 10 (11), 169-174. https://doi.org/10.22214/ijraset.2022.47284
36. Analysis of anomalous behavior in network systems using deep reinforcement learning with cnn architecture. https://doi.org/10.48550/arxiv.2211.16304
37. Anand, L. (2025). Reinforcement learning-based intrusion prevention in m2m systems. https://doi.org/10.31224/4880
38. Applying deep reinforcement learning for detection of internet-of- things cyber attacks. https://doi.org/10.1109/ccwc57344.2023.10099349
39. Arabelli, R., Boddepalli, E., Yadav, R. B. S., Kanwer, B., Wicak-sono, Y. K., & Dhanraj, J. A. (2024). Intrusion detection and preven-tion systems for wireless iot networks: Machine learning approaches. https://doi.org/10.1109/ic3i61595.2024.10828859
40. Arqane, A., Boutkhoum, O., Boukhriss, H., & Moutaouakkil, A. E. (2021). A review of intrusion detection systems: Datasets and machine learning methods. https://doi.org/10.1145/3454127.3456576
41. Aziz, A. S. A., Hassanien, A. E., Hanaf, S. E., & Tolba, M. F. (2013). Multi-layer hybrid machine learning techniques for anomalies detection and classification approach. https://doi.org/10.1109/HIS.2013.6920485
42. B.C, B. S., & P, J. J. (2018). Survey on intrusion detection system using machine - learning

approaches. International Jour-nal of Engineering and Computer Science, 7 (05), 23901-23907. https://doi.org/10.18535/IJECS/V715.05

43. Baby, R., Pooranian, Z., Shojafar, M., & Tafazolli, R. (2023). A heterogenous iot attack detection through deep reinforcement learning: A dynamic ML approach. https://doi.org/10.1109/icc45041.2023.10278685
44. badawy, W. (2025). Ai-powered cybersecurity: A technical review of in-trusion detection models, tools, and metrics. https://doi.org/10.1109/itc-egypt66095.2025.11186688
45. Bakhshad, S., Ponnusamy, V., Annur, R., Waqas, M., Alasmary, H., & Tu, S. (2022). Deep reinforcement learning based intrusion detection system with feature selections method and optimal hyper-parameter in iot environment. https://doi.org/10.1109/cits55221.2022.9832976
46. Bala, N., Singal, S., & Bedi, D. S. (2025). A comparative analysis of machine learning algorithms for intrusion detection systems: Unveiling

47. the prowess of predictive models in cybersecurity. Social Science Research Network. https://doi.org/10.2139/ssrn.5089152
48. Balyan, A. K., Trivedi, N. K., & Sharma, S. K. (2023). A survey on machine learning techniques for detecting, mitigating, and preventing intrusions. https://doi.org/10.1109/ictacs59847.2023.10390316
49. Bebortta, S., Tripathy, S. S., Sharma, V., Behera, J. R., & Nayak, A. (2024). A secure deep q- reinforcement learning framework for network intrusion detection in iot-fog systems. https://doi.org/10.1109/otcon60325.2024.10687378
50. Benaddi, H., Jouhari, M., Ibrahimi, K., Ben-Othman, J., & Amhoud, (2022). Anomaly detection in industrial iot using distributional reinforcement learning and generative adversarial networks. Sensors, 22 (21), 8085-8085. https://doi.org/10.3390/s22218085
51. Benchama, A., Bensoltane, R., & Zebbara, K. (2024). Network intrusion system detection using machine and deep learning models: A compara-tive study. https://doi.org/10.1007/978-3-031-48465-0_36