



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Machine Learning Based Defect-Detection Networks for Intrusion Detection, Using the NSL-KDD dataset: a comparative versus Deep learning Models

Viral Kumar Gupta¹, Dr. Sunil Kumar²

¹Research Scholar; Department of Computer Applications, School of Computer Science & Applications, IFTM University, Moradabad (UP) India, E-mail: viralkumargupta12@gmail.com, Orcid Id: <https://orcid.org/0009-0003-6945-6057>

²Assistant Professor; Department of Computer Applications, School of Computer Science & Applications, IFTM University, Moradabad (UP) India, E-mail: skiftm@gmail.com

ABSTRACT

Modern networks face an expanding and increasingly sophisticated set of security threats driven by the rapid growth of the Internet of Things (IoT), cloud computing, and high-speed communication technologies. Conventional, rule-based security systems struggle to keep pace with attacks that evolve in real time, motivating a shift toward intelligent, data-driven defect detection. This paper synthesizes the literature on Artificial Intelligence (AI), Machine Learning (ML), and Neural Networks (NNs) as applied to network security, tracing the evolution from early supervised classifiers to deep learning and, most recently, Explainable AI (XAI) and Self-Supervised Learning (SSL). It presents the principal categories of network threats, contrasts supervised and unsupervised learning paradigms, reviews the standard evaluation metrics used to judge detection performance, and consolidates twenty years of foundational and contemporary research into a structured comparative table and chart. The review concludes that while supervised methods deliver strong accuracy when labeled data is available, unsupervised and self-supervised approaches offer the scalability and adaptability required for real-world, label-scarce environments, and that interpretability remains an open research gap for AI-driven Defect Detection Networks (DDNs).

Keywords: Network Security; Artificial Intelligence; Machine Learning; Neural Networks; Deep Learning; Intrusion Detection; Defect Detection Networks (DDNs); Anomaly Detection; Explainable AI (XAI); Self-Supervised Learning (SSL).

Introduction

The dependability of any communication system rests on its capacity to protect data and resources as they move across increasingly complex infrastructures. The proliferation of IoT devices, virtualized cloud services, and 5G connectivity has multiplied the number of endpoints and attack surfaces that must be defended, while simultaneously increasing the volume and velocity of network traffic that must be inspected. Traditional signature- and rule-based intrusion detection systems were designed for comparatively static threat landscapes; they falter when confronted with novel or rapidly mutating attacks. This limitation has driven a sustained research effort toward intelligent Defect Detection Networks (DDNs) that use AI, ML, and NN techniques to recognize anomalous behavior automatically, adapt to new patterns, and reduce reliance on manually crafted rules. This paper reviews that body of research, organizing it around three questions: (i) what threats must modern DDNs defend against, (ii) which learning paradigms have been applied and with what trade-offs, and (iii) how is detection performance measured and where do current gaps remain.

In the current era of technology, Internet of Things (IoT) continues to gain traction, due to increasing use being an integral part of everyday life, IoT was initially named in 1999 by British technologist Kevin Ashton. IoT refers to an array of devices that have access to the internet and even can “speak” with each other. Due to this IoT envisioned a world where there was an enormous universe of devices communicating with one another and gathering and processing data such that they could perform tasks independently like Pushing beyond current uses just like process automation, home appliance automation, intelligent cars, smart grids, health care system, decision analytics, educational advancement, industrial development. IoT consists of many elements, such as sensors, some actuators, different software, processors, and other types of technologies employed to link and facilitate devices and systems to exchange data over the Internet. Who would have ever imagined a notion that seemed to be science fiction today is an imminent reality in a rapid phase (Ashton, 2009). According to the Statista report, there is a projection that the number of IoT based devices in the world would increase by 50% from 15.9 billion in 2023 to over 32.1 billion in 2030 (Statista Report, 2024). With all the benefits of IoT, cybercriminals have a wider attack surface because of the vast number of devices that are interconnected, most of which lack strong security controls and lack much processing power (Symantec, 2023). As certain recent studies have shown, more than 60% of IoT attacks target weaknesses like old firmware, weak authentication mechanisms and unsafe network protocols (Al-Hadhrani and Hussain, 2020). Though IoT networks continue to be vulnerable to ransomware, botnets, Distributed Denial of Service (DDoS) attacks, man-in-the-middle

(MitM) attacks, and many more types of cyberattacks. The heterogeneity resulted due to merging various nodes in IoT is vulnerable to a serious security breach. Making the resource-constrained IoT nodes strongly secure is the greatest challenge since such nodes are most vulnerable to cyberattacks as they have constrained resources. Such nodes' vulnerable by nature is easily accessed by malwares that compromise the integrity of the whole network. Intrusion detection systems are primitive but potent security devices for making IoT-embedded environments secure (Islam et al., 2021). Conventional security appliances like firewalls, access control, and encryption are insufficient to protect them. They do not work and are inefficient on large networks having numerous devices, with each device being a vulnerability point. The IoT network can be better secured by the inclusion of the intrusion IDS, the second defense against security attacks (Adewole and Torra, 2023). The distinctiveness of intrusion detection systems is that it is capable of determining whether the source of this data packet is a legitimate user or an attacker. They are excellent at passively sniffing traffic and listening, looking, and sensing live data packets. In most cases, intrusion detection systems are network-based or host-based depending on the physical point of deployment within the system. Early detection of malicious activity via monitoring of network traffic is crucial to, intrusion detection technologies must be enhanced and developed in a hurry owing to the increase of advanced cyber anomalies. Most notable intrusion detection challenge is detecting advanced cyberattacks amidst typical network traffic.

Thus, development and massive market for IoT technology has been created that generated its economic value, and drew many people - from scientists to inventors, entrepreneurs to businesspeople, and even hackers. IoT even spawned other schemes of investment on technological innovation on businesses. Innovators and inventors keep evolving and selling fresh IoT applications that further increase convenience and efficiency for a vast majority of activities. The widespread use, however, has also invited vulnerabilities in IoT networks on several occasions in security breaches, which are also employed by hackers in finding IoT device vulnerability weaknesses. IoT platform has proven to be a lucrative cyberattack target due to businesses emerging at lightning speed through IoT as well as financial incentives. It has also led to the serious escalation of security threats caused by IoT because of rising numbers of connected devices and their integration into critical infrastructures. Open-ended vulnerabilities have been exploited by attackers when crafting complex cyberattacks, poor encryption, and poor authentication as they sought to execute successful attacks. This ever-growing demand calls for strong and improved security controls, real-time threat detection, and continuous innovation in intrusion detection technologies to defend IoT ecosystems. Machine learning (ML) has also emerged as a viable solution to address the issue of intrusion detection in IoT networks because it can identify deviations and anomalous patterns in the network traffic (Telnix, 2024).

ML-based intrusion detection system in IoT devices have been revised in prominent literature. Ensemble-based techniques, in this context, have become very popular since they can advance the execution and reliability of IDS. (Abbas et al., 2022), for instance, recommended an ensemble IDS model that incorporates a lot of ML techniques such as Naive Bayes (NB), DT, and logistic regression (LR). The execution of the model in detecting malicious network traffic and it was established when it was tested against the CICIDS2017 intrusion detection dataset and achieved 88.96% accuracy for multi-class sorting and 88.92% accuracy for binary classification. Likewise, (Awotunde et al., 2023) suggested ensemble approaches using modern state-of-the-art machine learning algorithms like AdaBoost, Random Forest, Bagging, XGBoost, and Extra Trees. Their method utilized the ToN-IoT dataset, which contains telemetry data of seven IoT devices: refrigerator, thermostat, modbus, motion light, GPS tracker garage door, and weather sensors. Their ensemble models utilized heterogeneous sources of data to improve detection accuracy and generalizability across a vast range of IoT environments. Due to the intrusion detection issue in IoT networks, ML has also been proposed as a useful solution because it can detect anomalies and unusual network traffic behavior. Some of the relevant research works in the literature have considered ML-based intrusion detection in IoT networks. Ensemble-based techniques are particularly of interest in this regard because they can assist in making IDS more effective and efficient. Subsequently, a superior prediction-performing AdaBoost ensemble algorithm was then trained on feature-cleaned features. Two of the largest IDS datasets, NSL-KDD and BoT-IoT, have been utilized by their paper in an attempt to legitimize the model as well as show its success at maximizing IDS efficiency. They report an increase in applications of ML-empowered ensemble methods for IoT network hardening that offers adaptive and scalable defensive measures against evasive cyber-attacks.

The Internet of Things is expanding at an astounding rate, with an estimated 40 billion connected devices by 2030 (Awotunde et al., 2023). Due to their intrinsic security flaws, IoT devices are extremely susceptible to attack, and their proliferation is creating difficult security problems. The most notable are: repeated attacks according to (NETGEAR, 2024), home network devices subject to roughly ten typical cyberattacks every day, sector weaknesses more than 0.7 times as many industrial firms experienced cyberattacks on IoT devices (Kaspersky, 2023). In terms of data breaches in 2023, healthcare analytics breaches primarily caused by compromised IoT devices affected 25% of Americans (Asimily, 2024). Unencrypted Data (Asimily, 2023) reports that 98% of Internet of Things traffic is unencrypted, making it possible to target data. Conventional intrusion detection systems (IDS) are not appropriate for secure IoT environments. Because it is rule-based, it produces a high false positive rate and is ineffective against novel attacks, particularly in dynamic and resource-constrained environments.

Therefore, an IDS that is machine learning based and adaptive is required in order to recognize and react to

emerging threats in IoT networks. With the exponential growth of IoTs to an estimated 40 billion devices by 2030, convenience came at a cost in the form of increased security vulnerabilities (Awotunde et al., 2023). Standard attacks like DDoS and data breaches take advantage of exposure because 98% of IoT traffic is not encrypted (Hazman et al., 2024) and the majority of devices run outdated software (Al-Hadhrami and Hussain, 2020). Due to resource and scalability limitations, the Internet of Things poses a threat to traditional intrusion detection systems (IDS) (Al-Hadhrami and Hussain, 2020). Rather, through dynamic anomaly detection, machine learning offers a practical solution (Hazman et al., 2024).

Security Challenges In Modern Network Environments:

Network security threats can be grouped into a small number of recurring categories, each requiring a different detection strategy. Table 1 summarizes the principal threat types discussed in the literature together with their underlying mechanism and typical impact.

Table1. Principal categories of network security threats and their operational impact

Threat Category	Core Mechanism	Primary Impact on Network
Malware (virus, worm, trojan)	Malicious code execution and file corruption	Service disruption, data corruption
Phishing	Social engineering via deceptive emails/links	Credential theft, unauthorized access
DoS / DDoS	Traffic flooding to exhaust resources	Denial of service to legitimate users
Unauthorized Access	Bypassing authentication controls	Exposure of restricted systems
Data Breach	Exploiting weak security controls	Loss or theft of sensitive information
Man-in-the-Middle (MITM)	Covert interception of communication	Data tampering, loss of confidentiality
Insider Threats	Misuse of legitimate internal access	Intentional or accidental data exposure
Advanced Persistent Threats (APT)	Prolonged, stealthy intrusion campaigns	Long-term surveillance and data exfiltration

Beyond categorizing individual attacks, the literature frames network intrusions in terms of three fundamental actions that any secure architecture must resist: interruption, in which services are rendered unavailable; interception, in which confidential data is accessed without authorization; and modification, in which transmitted information is altered in transit. These three actions constitute the underlying threat model against which AI-driven defect detection systems are evaluated, since an effective DDN must be able to recognize the behavioral signatures associated with each.

Foundations of AI, Machine Learning, and Neural Networks:

Artificial Intelligence- Artificial Intelligence refers broadly to computational systems capable of performing tasks that would normally require human cognition, including perception, reasoning, and decision-making. Within network security, AI provides the conceptual umbrella under which specific learning techniques are deployed to monitor, classify, and respond to traffic patterns without constant human supervision.

Machine Learning Paradigms- Machine Learning, this subfield of AI, lets systems get better at a task by learning from experience rather than by explicit programming. When you look at it in network security, an ML model usually views each network flow as a feature vector, so it's basically a description made up of attributes like packet size, connection length, protocol type, and the source address. From there it learns a mapping from that feature space toward some output set, say benign traffic versus specific attack labels like Denial of Service, Probe, Remote-to-Local, or even User-to-Root. In the papers, two main ways keep showing up, kind of like the

standard playbook.

● **supervised learning:** here the model is trained using labeled samples, and it learns how feature vectors link to known results. It's pretty handy for things like spam detection or intrusion classification, especially when labeled datasets exist and you can actually rely on them.

● **Unsupervised Learning:** in this case the model gets no labels at all, and instead it tries to discover underlying patterns , like grouping similar points together , or spotting strange ones. This is useful for dimensionality reduction, noise filtering, and flagging attack behavior that it has never seen before, in other words new or previously unseen attack patterns. Then there is reinforcement learning, where an agent improves by trial-and-error while it receives feedback from its environment. People are increasingly exploring it for self-correcting, real-time network defenses, but honestly it still feels less mature in this area compared to supervised and unsupervised approaches.

Neural Networks and Deep Learning- Neural Networks extend machine learning by stacking computation across layers of linked nodes, where the signals get changed through weighted links and a non-linear activation function, or so it goes. In the past the sigmoid function was the big thing, but nowadays the Rectified Linear Unit, usually written ReLU , is the go-to for deep learning since it eases the vanishing-gradient issue and tends to speed up training. After that straightforward feed-forward setup, a bunch of more specialized architectures showed up: Convolutional Neural Networks (CNNs) are especially good for spotting spatial patterns, and they've been used with things like network telemetry plus log data. Meanwhile, Recurrent Neural Networks, or RNNs, work well when the data is sequential, like time-series traffic. In all these setups, learning is still driven by back propagation, meaning the gap between what the model predicts and what actually happens is then used to update weights and biases, step by step, until the prediction error is brought down as much as possible. Also, the amount of data along with the network depth has been crucial for performance improvements, though at some point the gains feel less dramatic and the compute expense climbs fast as the model grows.

Evaluation Framework for Defect Detection:

Assessing a network intrusion detection model requires a consistent vocabulary for classification outcomes. The confusion matrix which crosses-tabulates actual versus predicted classes provides the basis for the most widely used evaluation metrics in this literature, summarized in Table 2.

Table 2. Confusion matrix and outcomes

Outcome	Definition	Role in Evaluation
True Positive (TP)	Malicious instance correctly identified as malicious	Reflects detection capability
True Negative (TN)	Benign instance correctly identified as benign	Reflects specificity
False Positive (FP)	Benign instance incorrectly flagged as malicious	Indicates false-alarm rate
False Negative (FN)	Malicious instance incorrectly classified as benign	Indicates missed threats
Detection Rate / Recall	$TP / (TP + FN)$	Primary indicator of intrusion-detection effectiveness

Since True Positive Rate, Recall, and Detection Rate are used kind of interchangeably across many studies, this review just treats them as equal, when we compare the reported results, following what is pretty common in the network intrusion detection literature.

Review of Related Work:

Table 3 consolidates the foundational and contemporary studies discussed in this review, tracing the field's progression from statistical and rule-based reasoning toward adaptive, data-driven, and ultimately explainable detection systems.

Table 3. Chronological synthesis of key contributions to AI/ML-based network defect detection.

Author(s) / Year	Focus Area	Contribution to Network Defect Detection
Alpaydin (2010)	Foundations of ML	Argued for adaptive learning algorithms over static rule-based systems in dynamic network environments
Russell & Norvig (2016)	AI paradigm shift	Traced the move from symbolic reasoning to learning-based intelligence, framing modern fault-detection design
Mitchell (1997)	Supervised learning	Established decision trees and SVMs as core tools for labeled-data anomaly classification
Breiman (2001)	Ensemble learning	Introduced Random Forests, improving noise tolerance and scalability for high-dimensional network data
Vapnik (1998)	Support Vector Machines	Enabled non-linear decision boundaries for detecting subtle network failures
Pearl (1988)	Probabilistic reasoning	Proposed Bayesian networks as a graphical basis for anomaly detection under uncertainty
Bishop (2006)	Unsupervised learning	Advanced clustering and Gaussian mixture models for detecting rare, unlabeled network events
Yegnanarayana	Neural signal processing	Linked neural modeling to pattern-based anomaly detection in traffic signals
Sastry	Reinforcement learning	Explored adaptive, self-correcting network learning in real time
LeCun, Bengio & Hinton (2015)	Deep learning	Showed deep networks can capture non-linear relationships for automated anomaly detection
Goodfellow, Bengio & Courville (2016)	Generative models	Applied autoencoders to reconstruct normal patterns and flag deviations as defects
Dubey (2018)	CNN applications	Demonstrated convolutional architectures for pattern recognition in network telemetry/log data
Satapathy (2020)	Model optimization	Tuned deep architectures for efficient large-scale, real-time anomaly detection
Kelleher (2019)	Feature engineering	Emphasized preprocessing for noisy, high-dimensional network datasets
Zhang et al. (2016)	Comparative evaluation	Benchmarked decision trees, SVMs, and neural networks for intrusion detection accuracy
Lloyd et al. (2016)	Continuous learning	Highlighted retraining needs as network behaviour evolves over time
Wang et al. (2017)	Early-warning systems	Used predictive ML to flag faults before full failures occur
Recent works (2020-2024)	XAI & Self-Supervised Learning	Combine interpretability (XAI) with label-free learning (SSL) to close transparency and data-scarcity gaps

Comparative Analysis of Learning Paradigms:

Synthesizing the findings summarized in Table 3, the three dominant paradigms supervised learning, unsupervised learning, and deep neural networks exhibit distinct strengths across four practical dimensions relevant to network defect detection: dependency on labeled data, scalability to large and high-dimensional traffic datasets, interpretability of the resulting model, and adaptability to real-time, evolving conditions. Figure

1 presents a qualitative comparison derived from the patterns observed across the reviewed literature.

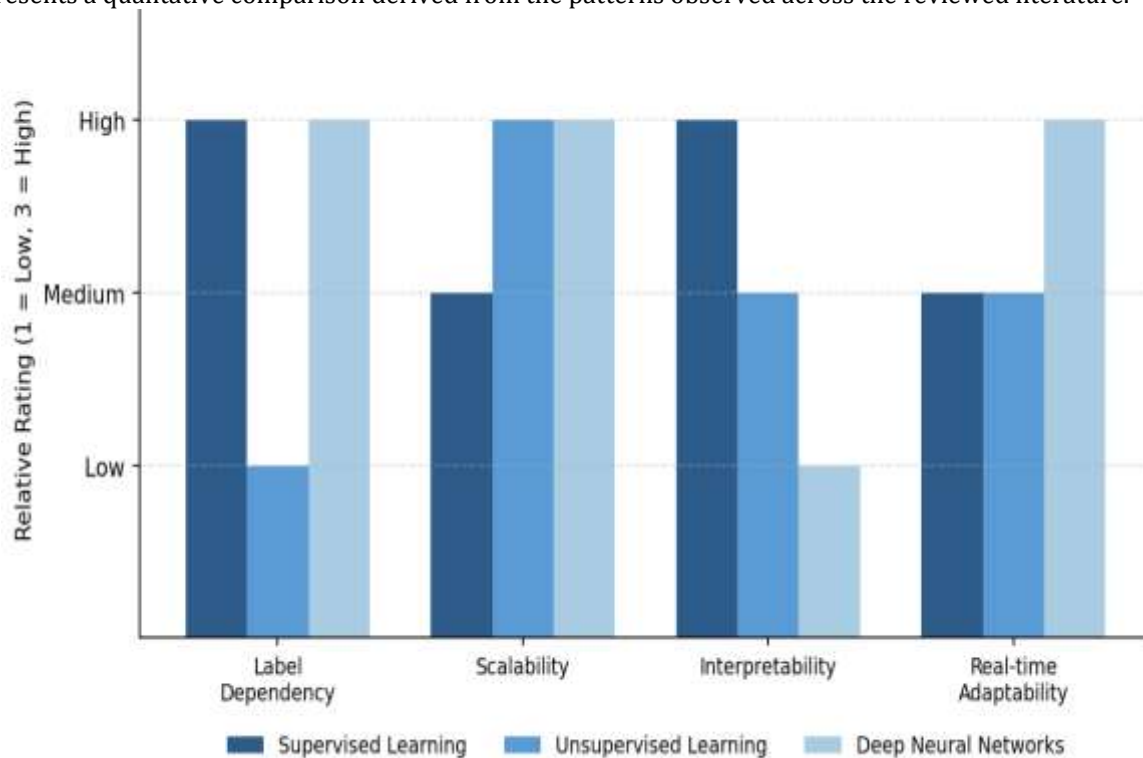


Figure1. Conceptual comparison of supervised learning, unsupervised learning

As Figure 1 illustrates, supervised methods and deep neural networks kind of score highly on label dependency, (meaning they rely a lot on labeled data) but they also show a pretty sharp split in interpretability. Classical supervised models like decision trees are still relatively transparent, whereas deep networks end up trading interpretability for extra representational power. Unsupervised learning, on the other hand, minimizes its need for labels and tends to scale well, so it becomes attractive when attack labels are scarce or when the attacks are basically previously unseen, even if the results are usually more difficult to map straight onto particular threat categories. Deep neural networks also stand out for real time adaptability and scalability once they've been trained, but because interpretability is comparatively low, people have been turning toward Explainable AI, so network administrators can audit the decisions rather than just accept them.

Research gaps and observations

The reviewed literature converges on a few observations, like it stays the same thread throughout. First off, there's a clear move away from static, rule-based security mechanisms toward adaptive, learning-based systems, and this feels now pretty settled due to the fact that fixed rules just don't keep up with threats that keep changing. Second, supervised learning is still showing strong accuracy wherever people actually have labeled datasets, but in real network environments those labels are often missing or not available at all, so interest stays strong in unsupervised and self-supervised alternatives. Third, deep learning architectures especially CNNs and RNNs have turned into something like the core choice for handling large-scale, high-dimensional, time-dependent network data. Fourth, and this part shows up more and more in work from 2020 onward, is the paired focus on Explainable AI together with Self-Supervised Learning: the first one tries to close the transparency gap left by deep models, while the second one tries to deal with the ongoing lack of labeled network data. Scalability, transparency, and real-time deployment remain the three open challenges that are most often mentioned across the papers, and they basically shape the niche where future AI-driven Defect Detection Networks should be placed.

Conclusion

This review kind of traced the intellectual lineage of AI-driven network defect detection, from Alpaydin's early case for adaptive algorithms through the supervised-learning basics laid by Mitchell, Breiman, and Vapnik, to the deep learning upswing of LeCun, Bengio, Hinton, and Goodfellow, and then to today's push on explainability, plus self-supervision. Across that whole arc, the consistent takeaway seems to be that intelligent, data-driven methods beat static rule-based systems in accuracy, adaptability, and even in proactive threat discovery. Still, no one paradigm really "wins" for every need, because supervised learning gives a kind of precision when labels actually exist, unsupervised learning gives scalability when they do not, and deep learning gives representational strength, but it trades off interpretability. So the next generation of Defect Detection Networks is likely to merge these ideas — for example self-supervised or unsupervised pertaining paired with

explainable decision layers — so you end up with detection systems that are accurate enough, scalable enough, and trustworthy for real-time network security operations, not just impressive in a lab.

References

1. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780.
2. Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15(1), 1929–1958.
3. Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. In *Proceedings of the International Conference on Learning Representations (ICLR)*.
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
5. Hinton, G. E., Osindero, S., & Teh, Y. W. (2006). A fast learning algorithm for deep belief nets. *Neural Computation*, 18(7), 1527–1554.
6. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*.
7. He, H., Bai, Y., Garcia, E. A., & Li, S. (2008). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In *Proceedings of the IEEE International Joint Conference on Neural Networks (IJCNN)*.
8. Kim, J., Kim, H., Kim, T., & Kim, H. (2019). Hybrid CNN-LSTM network in network intrusion detection. In *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC)*, 942–944.
9. Katkuri, A., et al. A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. GitHub research repository, evaluated on the NSL-KDD dataset with feature selection and model optimization.
10. Jain, R., et al. (2026). Optimizing intrusion detection using a hybrid CNN-LSTM deep learning framework on the NSL-KDD dataset. *Discover Computing*, 29(194).
11. A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system (2024). *Computers & Security*. Evaluates ANN, LSTM, BiLSTM, CNN-LSTM, GRU, and BiGRU with Recursive Feature Elimination on NSL-KDD.
12. IntrusionX: A hybrid convolutional-LSTM deep learning framework with Squirrel Search optimization for network intrusion detection (2025). arXiv:2510.00572.
13. The problem of improving network intrusion detection using a hybrid CNN-LSTM deep learning model: A cyber security perspective (2026). In *Proceedings volume*, Springer Nature.
14. Deep learning for network security: An Attention-CNN-LSTM model for accurate intrusion detection (2025). *Scientific Reports*, evaluated on NSL-KDD and Bot-IoT.
15. A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks (2023). *Ad Hoc Networks / ScienceDirect*, evaluated across Kyoto, CICIDS2017, KDD-Cup99, NSL-KDD, UNSW-NB15, and WSN-DS datasets.
16. Bagui, S., & Li, K. (2021). Resampling imbalanced data for network intrusion detection datasets. *Journal of Big Data*, 8(1), 6.
17. Fu, Y., Du, Y., Cao, Z., Li, Q., & Xiang, W. (2022). A deep learning model for network intrusion detection with imbalanced data. *Electronics*, 11(6), 898.
18. Abdelkhalek, A., & Mashaly, M. (2023). Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning. *The Journal of Supercomputing*, 79(10), 10611–10644.
19. Impact of resampling techniques in deep learning based intrusion detection: A comparative study on NSL-KDD and UNSW-NB15 (2025). *Procedia Computer Science / ScienceDirect*. Evaluates a CNN-BiLSTM model with ADASYN, RUS, TomekLinks, and OSS.
20. Overcoming class imbalance in network intrusion detection: A Gaussian Mixture Model and ADASYN augmented deep learning framework (2024). In *Proceedings of the International Conference on Internet of Things and Machine Learning (IoTML)*. Proposes the C3BANet CNN-BiLSTM model with channel attention.
21. Addressing imbalanced data in network intrusion detection (2024). *International Journal of Advanced Computer Science and Applications (IJACSA)*, 15(2).
22. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
23. An intrusion detection method using Few-Shot Learning (2020). *IEEE Access*. Achieves 92.34% accuracy on KDD-Test+ and 85.75% on KDD-Test-21 using under 1% of NSL-KDD training data.
24. Few-shot network intrusion detection using discriminative representation learning with supervised autoencoder (2022). *Applied Sciences*, 12(5), 2351.
25. A few-shot network intrusion detection method based on mutual centralized learning (2025). *Scientific Reports*.
26. Intrusion detection system for NSL-KDD dataset based on deep learning and recursive feature

- elimination (2021). Evaluates a recurrent neural network for multi-class classification of DoS, Normal, Probe, R2L, and U2R traffic.
27. Advanced cloud intrusion detection framework using graph-based features, transformers, and contrastive learning (2025). PMC / journal article, evaluated on NSL-KDD and CIC-IDS2018.
28. Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives (2018). arXiv:1811.05372. Analyzes minority-class (R2L, U2R) performance limitations on KDD-99 and NSL-KDD.
29. Goh, J., Adepu, S., Junejo, K. N., & Mathur, A. (2016). A dataset to support research in the design of secure water treatment systems (SWaT). In Proceedings of the International Conference on Critical Information Infrastructures Security (CRITIS).
30. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Proceedings of the Military Communications and Information Systems Conference (MilCIS).
31. Ashton, K. (2009). That “internet of things” thing. RFID Journal. Available online at: <https://www.rfidjournal.com/articles/view?4986> (Accessed July 6, 2025)
32. Al-Hadhrani, Y., and Hussain, F. K. (2020). Real time dataset generation framework for intrusion detection systems in IoT. *Futur. Gener. Comput. Syst.* 108, 414–423. doi: 10.1016/j.future.2020.02.051
33. Adewole, K. S., and Torra, V. (2023). “Privacy Protection of synthetic smart grid data Simulated via Generative Adversarial Networks,” in Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT 2023), (Rome: SciTePress), 279–286.
34. Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., et al. (2021). Towards machine learning based intrusion detection in IoT networks. *Comput. Mater. Contin.* 69, 1801–1821. doi: 10.32604/cmc.2021.018466
35. Symantec. (2023). Title of Symantec IoT Security Report. Available online at: <https://www.broadcom.com/products/cyber-security/symantec> (Accessed July 6, 2025).
36. Statista Report. (2024). Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030 [Report]. Available online at: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (Accessed July 6, 2025)
37. Abbas, A., Khan, M. A., Latif, S., Ajaz, M., Shah, A. A., and Ahmad, J. (2022). A new ensemble-based intrusion detection system for internet of things. *Arab. J. Sci. Eng.* 47, 1805–1819. doi: 10.1007/s13369-021-06086-5
38. Awotunde, J. B., Folorunso, S. O., Imoize, A. L., Odunuga, J. O., Lee, C. C., Li, C. T., et al. (2023). An ensemble tree-based model for intrusion detection in industrial internet of things networks. *Appl. Sci.* 13:2479. doi: 10.3390/app13042479
39. Telnyx. (2024). IoT security solutions: Challenges and best practices. Available online at: <https://telnyx.com/resources/iot-security-solutions> (Accessed November 26, 2025).
40. NETGEAR. (2024). Every 24 Hours, home Networks see an Average of 10 Attacks. Is your Network Secure? NETGEAR Hub. Available online at: <https://www.netgear.com/hub/network/2024-iot-threat-report/> (Accessed July 6, 2025)
41. Asimily. (2024). The top Internet of Things (IoT) Cybersecurity Breaches in 2024. Available online at: <https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2024> (Accessed July 6, 2025)
42. Asimily. (2023). IoT Devices are easy Targets for Cyberattacks. Available online at: <https://asimily.com/blog/iot-devices-are-easy-targets-for-cyberattacks> (Accessed July 6, 2025)
43. Asimily. (2024). The top Internet of Things (IoT) Cybersecurity Breaches in 2024. Available online at: <https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2024> (Accessed July 6, 2025)
44. Kaspersky. (2023). Kaspersky Unveils an Overview of IoT-Related Threats in 2023. Kaspersky Press Releases. Available online at: <https://www.kaspersky.com/about/press-releases/kaspersky-unveils-an-overview-of-iot-related-threats-in-2023> (Accessed July 6, 2025).
45. Hazman, C., Guezzaz, A., Benkirane, S., and Azrour, M. (2024). Toward an intrusion detection model for IoT-based smart environments. *Multimed. Tools Appl.* 83, 62159–62180.