Model / Algorithm Class	Dataset(s) Used	Accuracy	F1-Score	Qualitative Analysis / Key Findings
RNN / LSTM	CIC-IDS2017, UNSW-NB15, NSL-KDD	99% [1], 93% [2], 97.7% [1]	High (>0.90) [3]	Excellent for capturing temporal dependencies in network flows. Maintains an internal state or "memory" to learn patterns based on the order and timing of events. A cornerstone of modern NIDS architecture.
CNN	CIC-IDS2017, UNSW-NB15, NSL-KDD	96.5% (Overall) [4], **58.8% (Unknown)** [4], 82.8% - 99.8% [5, 6, 7], >99% [8, 9]	0.9160 (Overall) [4], **0.3218 (Unknown)** [4], ~0.81 [7], ~0.99 [10]	Extracts hierarchical "spatial" features from network data. Highly effective for known attack patterns but brittle against novelty; performance collapses on zero-day exploits not seen during training.

Hybrid CNN-LSTM	NSL-KDD, UNSW-NB15, CIC-IDS2017	99.7% - 99.89% [11, 10, 12], 98.95% [12], 95.21% [13]	~0.99 [10]	Fuses the spatial feature extraction of CNNs with the temporal sequence modeling of RNNs. Consistently achieves state-of-the-art results, creating a more comprehensive and resilient detection capability.
Transformer / Attention	UNSW-NB15, 3 Benchmark Datasets	98.26% [14], >99% (Balanced) [15]	95.80% [14]	Masters long-range dependencies using self-attention, overcoming limitations of sequential models. **Key Challenge:** Can exhibit a higher false alarm rate, leading to potential "alert fatigue" in a SOC environment.

Graph Neural Networks (GNN)	CIC-IDS2017, UNSW-NB15, Multi-Dataset	99.96% [16], 99.99% [16]	99.91% [16], 99.98% [16], 0.947 [16]	Models the network's topological structure, making it unparalleled for detecting coordinated, distributed attacks (e.g., botnets). **Major Hurdles:** Faces significant operational challenges in scalability, real-time training latency, and interpretability.
Autoencoders	HIKARI-2021	94% [17]	0.89 [17]	Unsupervised model trained only on "normal" data to detect anomalies via high reconstruction error. Achieves very high recall (99%) but low precision (81%), indicating a high number of false positives.

One-Class SVM (OCSVM)	CIC-IDS2017	83.56% (Overall) [4], **79.19% (Unknown)** [4]	0.5520 (Overall) [4], **0.7575 (Unknown)** [4]	Unsupervised model that learns a boundary around normal data. While overall accuracy is lower, it delivers the **best performance by a wide margin on unknown attacks**, making it a necessary safety net for zero-day threats.
Contrastive Learning	CIC-IDS2017, UNSW-NB15	99.66% [18], 91.27% [18]	99.12% [18], 92.30% [18]	Advanced self-supervised method that learns robust feature representations from unlabeled data. Directly addresses data imbalance and improves detection of rare attacks, reducing dependency on manual labeling.

Generative Adversarial Networks (GANs)	N/A (Not a direct detection model)	N/A	N/A	**Dual Role:** 1) Data augmentation to generate synthetic data for rare attack classes. 2) Adversarial robustness testing to proactively find and fix model vulnerabilities. Essential for a robust MLOps pipeline.
Ensemble Tree Models (XGBoost, Random Forest)	CIC-IDS2017, UNSW-NB15, NSL-KDD	99.91% [19], 98.63% - 99.67% [20, 21]	97.80% - 98.83% [20, 21]	Consistently delivers state-of-the-art performance on tabular data, rivaling deep learning models. **Key Advantage:** High interpretability, providing feature importance scores that explain *why* an alert was triggered. A strong, production-grade candidate.

1.