Model Research

Model/ Algorithm	Dataset(s) Used	Performance Factors	Accuracy	Robustness
Random Forest	CICIDS2017, NSL-KDD, UNSW-NB15	Handles high-dimens-ional features, feature importance ranking	92–99	High
Autoencoder	CICIDS2017, UNSW-NB15	Unsupervised anomaly detection learning normal traffic patterns	85–93	Moderate depending on-training data
LSTM	CICIDS2017, NSL-KDD	Sequential data, detects time-based anomalies	90–96	Moderate-high due to res-tence to pattems
Gradient Boosting (XGBoost/ LightGBM)	CICIDS2017, NSL-KDD, UNSW-NB15	Handles imbalanced classes, robust to overfitting	94–99	Low Moderate-high-m-sates harder
SVM	CICIDS2017, NSL-KDD	Effective for high-dimensional linear/ non-linear separation	88–95	Moderate-high resistance to nolsy features
CNN	CICIDS2017, UNSW-NB15	Extracts packet-level spatial features	90–96	Low-Moderate bust nace possible-
Deep Belief Network (DBN)	CICIDS2017, KDD99	Advanced feature extraction, layered unsupervised learning	87–94	Low interpreting deep layers
K-Nearest Nelghbors (KNN)	CICIDS2017, NSL-KDD	Classifies network traffic based on pro-ximity in multidimen-	85–92	Low-Moderate interpretable
Isolation Forest	CICIDS2017, UNSW-NB15	Anomaly detection efficiently isolating outilers in network	85–94	High effective for rare anomalies
Reinforcem-Learning (DQN, PPO)	CICIDS2017, UNSW-NB15	Automates threat mitigation, learning optimal policies	88–95	Moderate outlier scores