Nguyen et al. (2012) developed an adaptive intrusion detection system (A-IDS) using an ensemble of Naive Bayes, Bayes Network, Decision Stump, and RBF Network. Their system achieved 90.52% accuracy on the CSIC-2010 dataset, outperforming majority voting and boostingmethods. However, scalability remains a challenge for larger datasets. This study demonstratesthe advantages of adaptive ensemble techniques in anomaly detection.

Kozik et al. (2014) proposed a decision-tree-based algorithm for cyberattack detection in webapplications, utilizing simulated HTTP requests. C4.5 outperformed other classifiers like NaiveBayes and PART in detecting attacks. Though effective, the study is limited by its use of simulated data, indicating the need for testing on real-world datasets.

Parhizkar and Abadi (2015) applied a one-class SVM for web traffic anomaly detection on theCSIC-2010v2 and CSIC2012 datasets. While they achieved reasonable performance in terms of TPR, FPR, and F1-score, the model struggled with HTTP-specific feature extraction. This highlights the efficacy of one-class SVM but emphasizes the need for broader feature coverage.

Zhang et al. (2018) employed deep neural networks (DNNs) for network intrusion detection using the CICIDS-2017 dataset. Their approach significantly improved detection accuracy, but required substantial computational resources. This study showcases deep learning's potential inreal-time anomaly detection, though resource management remains a challenge.

Ali Moradi Vartouni et al. (2018) combined a Stacked Auto-Encoder (SAE) and Isolation Forest for web application firewall implementation on the CSIC 2010 dataset. Feature extraction improved detection accuracy, although high-dimensional feature sets posed difficulties. This study underscores the effectiveness of feature extraction in deep learning models for anomaly detection.

Pubudu et al. (2022) proposed a stacked ensemble classifier using tree-based models for malicious traffic detection in IoT networks. The ensemble achieved high accuracy (98.5% binary, 98.4% multiclass) on UNSW-NB15 and IoTID20 datasets, but was computationally expensive. The study emphasizes the balance between accuracy and computational cost in ensemble learning.

João B.D. Cabrera et al. (2007) examined distributed intrusion detection in Mobile Ad-Hoc Networks (MANETs) using ensemble methods and clustering algorithms. Improved detection rates were achieved through a node-cluster-manager hierarchy, though the system remained vulnerable to communication losses in MANET environments.

Rajagopal et al. (2020) developed a stacking ensemble model for network intrusion detection, using datasets UNSW NB-15 and UGR'16. Their model achieved 97% accuracy on real-time Printed using Save ChatGPT as PDF, powered by PDFCrowd HTML to PDF API. ½ datasets, outperforming individual classifiers like Logistic Regression, KNN, and Random Forest. However, it struggled with emulated datasets, demonstrating the need for robust models across data types.

Meenal Jain & Gagandeep Kaur (2021) proposed a hybrid ensemble model integrating Random Forest, Logistic Regression, and SVM for anomaly detection in IoV traffic. Using the NSL-KDD, CIDDS-2017, and Testbed datasets, their system achieved up to 98% accuracy. However, handling concept drift and maintaining low computational costs remained challenges in distributed environments.

Imran et al. (2021) combined autoML and Kalman filters to enhance anomaly detection in IoV using UNSW-NB15 and CICIDS2017 datasets. Their ensemble model achieved 98.801% and 97.02% accuracy respectively. The study demonstrates the potential of combining machine learning and prediction models, though computational efficiency needs further optimization.