Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
[77]	2019	Y	BoT-IoT	Artificial Neural Network (ANN)

FS Techniques: Not Used

Balancing Techniques: Synthetic Minority Over-sampling Technique (SMOTE)

Performance Measure: True Positive Rate (TPR), False Positive Rate (FPR), Precision, Recall, F1-Score

Main Idea: Introduced an ML-based detection system specifically designed for IoT environments to effectively identify Distributed Denial of Service (DDoS) attacks facilitated by IoT malware, such as Mirai.

Contributions: Utilizes an ANN and addresses data imbalance in IoT security datasets by employing the SMOTE.

Conclusion: Demonstrates promising results in detecting DDoS attacks, emphasizing the need for specialized approaches to IoT security.

Limitations: Primarily designed to handle DDoS attacks and may not be as effective against other types of security threats prevalent in IoT environments.

[90]	2019	Y	Custom, NSL-KDD, UNSW-NB15	Deep Belief Network (DBN)

FS Techniques: Not Used

Balancing Techniques: Modified Density Peak Clustering (MDPCA)

Performance Measure: Accuracy, Precision, recall, FPR, Detection Rate (DR)

Main Idea: Proposed a hybrid intrusion detection system using MDPCA and DBN for efficient attack detection in network systems. MDPCA helps segment the training data into manageable clusters, reducing data imbalance, while DBNs extract high-level features for improved classification accuracy.

Contributions: Enhanced density peak clustering algorithm to better handle complex and nonlinear separable network traffic data. Utilizes MDPCA to segment network data into subsets, reducing data imbalance and enhancing minority class detection.

Conclusion: Achieves higher accuracy and demonstrates potential in addressing limitations of traditional ML in network security.

Limitations: Struggles with the detection of low-frequency attack types like U2R and R2L due to their underrepresentation in training datasets.

[12]	2019	Y	UNSW-NB15	Random Forest (RF)

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, Precision, recall, FPR, DR

Main Idea: Introduced the Anomaly Detection IoT (AD-IoT) system, an intelligent anomaly detection framework designed to enhance cybersecurity in smart cities. It focuses on detecting compromised IoT devices within distributed fog networks using the RF algorithm.

Contributions: Proposes the AD-IoT system for detecting IoT cyberattacks in smart city networks, utilizing fog nodes rather than traditional cloud centers for data processing, enhancing responsiveness and scalability of attack detection. Implements and evaluates the system with a modern dataset, demonstrating high accuracy in identifying compromised devices.

Conclusion: Proven highly effective in experimental setups, achieving a classification accuracy of 99.34% with a very low false positive rate, validating its potential for real-world applications.

Limitations: Does not discuss the scalability of the AD-IoT system beyond the test scenarios or its effectiveness in more heterogeneous or larger-scale network environments that may exist in actual smart cities.

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
[16]	2019	Y	Custom	Naïve Bayes (NB), Bayesian Networks (BN), Decision Tree (DT), Logistic Regression (LR), Support Vector Machines (SVM), RF, Multi-Layer Perceptron (MLP)

FS Techniques: Manual

Balancing Techniques: Spread Subsampling and Class Balancing filters

Performance Measure: Precision, recall, F1 score

Main Idea: Introduced a novel three-layer IDS specifically designed for IoT networks within smart homes, capable of classifying device types, detecting malicious packets, and identifying specific attack types using a supervised learning approach.

Contributions: A smart home testbed with commercially available IoT devices used to validate the system against various attack scenarios, including Denial of Service (DoS), MITM/Spoofing, Reconnaissance, Replay attacks, and complex multi-stage attack scenarios.

Conclusion: Demonstrates high effectiveness in distinguishing between normal and malicious activities across IoT devices, achieving high F-measure scores in all three of its core functions. Addresses the limitations of current security measures in IoT environments by providing an automated, intelligent, and specific attack detection solution.

Limitations: Limited to a controlled testbed environment, which may not fully replicate the complexities and unexpected behaviors found in diverse real-world IoT implementations.

[22]	2019	Y	Not Clearly Defined	SVM, RF, LR, DT

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy

Main Idea: Addressed the significant security vulnerabilities within the IoT, particularly focusing on DDoS attacks perpetrated through compromised IoT devices. The article presents a new approach to detect DDoS traffic efficiently within a local network router environment, demonstrating high detection accuracy in experimental settings.

Contributions: Tests the effectiveness of this framework under controlled experimental conditions, achieving high accuracy rates.

Conclusion: Outlines a successful experimental approach to detect DDoS attacks, highlighting the potential for further development in network anomaly detection systems to safeguard against vulnerabilities in IoT devices.

Limitations: Primary evaluation metric used is accuracy, which might not be adequate for datasets that have a class imbalance, potentially skewing the effectiveness of the detection framework. It does not provide sufficient information about the dataset used, which is crucial for replicating the study, limiting its applicability and credibility.

[28]	2019	Y	DS2OS	LR, SVM, DT, RF, ANN

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, precision, recall, F1 score, Area Under the ROC Curve (AUC)

Main Idea: Evaluated the effectiveness of various ML algorithms—LR, SVM, DT, RF, and ANN—in detecting attacks and anomalies within IoT systems.

Contributions: Compares several ML models to determine the best for predicting attacks and anomalies in IoT infrastructures.

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Conclusion: Identifies RF as the most effective algorithm for detecting various IoT network attacks due to its superior performance across multiple evaluation metrics.				
Limitations: Models were only tested in a virtual environment, raising questions about their effectiveness in real-world settings and with real-time data.				
[32]	2019	Y	Own Data	SVM
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: Accuracy				
Main Idea: Introduced an SVM-based anomaly detection model specifically tailored for identifying unauthorized activities within the IoT networks.				
Contributions: The anomaly detection model was trained and tested using real IoT network traffic, which included deliberate network-layer attacks, thereby enhancing the model's relevance and applicability to real-world scenarios.				
Conclusion: Demonstrates high efficacy of the SVM-based anomaly detection system, achieving up to 100% detection accuracy within the same network topology it was trained on. However, accuracy dropped to 81% when applied to different network topologies, highlighting the challenges in generalizing the detection capabilities across varying network configurations.				
Limitations: Shows reduced effectiveness when deployed in unfamiliar network topologies, indicating a need for further refinement to enhance its adaptability across diverse IoT environments.				
[58]	2019	Y	KDDCup99	Restricted Boltzmann Machine (RBM) Based Clustering
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, DR, FNR, TPR				
Main Idea: Presented a comprehensive analysis of ML and DL solutions for IDS in Wireless Sensor Networks (WSNs), introducing a new DL-based IDS methodology called RBM-based Clustered IDS (RBC-IDS) designed to monitor critical infrastructures.				
Contributions: Comparative analysis of RBC-IDS with a previously developed adaptive ML-based IDS, focusing on detection time, accuracy, and detection rates.				
Conclusion: Confirms that while RBC-IDS matches the performance of adaptive ML-based IDS in terms of accuracy of 99.12% and DR of 99.91%, it incurs longer detection times. It underlines the effectiveness of DL approaches in IDS for WSNs but highlights the need for optimization to reduce response times.				
Limitations: Longer detection time of RBC-IDS compared to adaptive ML-based systems, which could be a drawback for real-time intrusion detection requirements in critical infrastructure monitoring.				
[63]	2020	Y	NSL-KDD	Auto Encoder (AE)
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: Sensitivity, Specificity, Precision, DR, False Alarm Rate (FAR), Accuracy				
Main Idea: Introduced a novel IDS leveraging AE combined with adaptive self-taught transfer learning.				
Contributions: Utilization of a pre-trained network for regression-related tasks to initialize feature extraction, which is novel in the context of IDS.				
Conclusion: Presents a DL-based IDS that significantly outperforms traditional methods by employing a combination of self-taught learning and feature enhancement. Enhanced feature sets lead to better generalization and stability of the model, providing a robust solution against various network intrusions.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Limitations: Adaptation of the model relies heavily on the initial pre-training for regression tasks, which may not always perfectly align with the intrusion detection tasks, potentially affecting the universality and adaptability of the model.				
[67]	2019	Y	Aegean WiFi Intrusion Dataset (AWID)	Deep Neural Network (DNN)
FS Techniques: Used but not clearly discussed **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced a deep autoencoded dense neural network designed to enhance intrusion detection within 5G and IoT networks, utilizing advanced neural networks to distinguish between normal activities and various network threats such as flooding, denial of service attacks, and other malicious intrusions. **Contributions:** Application of a deep autoencoded dense neural network for intrusion detection in 5G and IoT environments. **Conclusion:** Demonstrated high efficiency with an accuracy of 99.9%, marking it as a robust tool against diverse network threats in modern interconnected environments. **Limitations:** Operates offline on high-performance computers, which may limit its real-time application capabilities.				
[70]	2019	Y	CICIDS2017	MLP, Convolutional Neural Network (CNN), Long Short-term Memory (LSTM), CNN+LSTM.
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall **Main Idea:** Introduced DL models to enhance cybersecurity within IoT networks, focusing on combating DDoS attacks using a hybrid CNN-LSTM model. **Contributions:** Identification of open research challenges in utilizing DL for IoT cybersecurity. **Conclusion:** Outperformed standard ML algorithms, with the highest recorded accuracy of 97.16%. **Limitations:** Requires balancing the dataset through data duplication, which might not be ideal. Increased computational need. Limited to DDoS attack detection.				
[95]	2019	Y	ISCX 2012 IDS dataset	1D-CNN+LSTM
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Precision, Recall, F1 Score **Main Idea:** Introduced DeepVCM, a hybrid DL model with 1D CNN and LSTM-based end-to-end intrusion detection method tailored for Vehicular Ad-hoc Networks (VANETs). **Contributions:** Introduction of DeepVCM, a novel DL-based intrusion detection system specifically designed for VANETs that utilizes raw traffic data, bypassing the need for feature extraction. **Conclusion:** Evaluation on both a public dataset and a simulated real-life VANET dataset demonstrates superior performance in detecting malware with lower resource requirements compared to existing methods. **Limitations:** While the study highlights the advantages of using raw traffic data for intrusion detection, it does not address potential challenges such as increased computational demand and the handling of highly variable traffic conditions in real-world VANET scenarios.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
[98]	2019	Y	NSL-KDD	DBN

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, FAR, DR, Precision, Recall

Main Idea: Introduced a self-adaptive intrusion detection model that combines an improved Genetic Algorithm (GA) with a DBN to optimize network structure for different attack types, ensuring high detection rates with reduced complexity.

Contributions: Presentation of an intrusion detection model that adaptively optimizes its neural network structure using GA.

Conclusion: Effectively tailors its network structure to various attack types using GA iterations, achieving high detection accuracy and streamlined training processes. This approach enhances performance in IoT intrusion detection and holds potential for broader classification and recognition task applications.

Limitations: The study utilizes the NSL-KDD dataset to demonstrate the performance of the proposed methods. However, it is important to note that NSL-KDD is not specifically designed for IoT environments. This may limit the direct applicability of the results to IoT-specific security challenges.

[84]	2020	Y	CIDDS-001, UNSWNB15, NSL-KDD	RF, AB, Gradient Boosting Machine (GBM), Extreme Gradient Boosting (XGB), ETC, Classification and Regression Tree (CART), MLP

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, Sensitivity, Specificity, FPR, AUC

Main Idea: Explored the use of ML classifiers for protecting IoT systems against DoS attacks. It assesses the performance of various classifiers on prominent IoT datasets and implements them on IoT-specific hardware to evaluate their practical response times.

Contributions: Statistical assessment of classifiers using Friedman and Nemenyi tests to identify significant performance differences among them. Implementation and performance testing of these classifiers on Raspberry Pi hardware to understand their response times in a real IoT environment.

Conclusion: Provides a comprehensive analysis of several ML classifiers, demonstrating that XGB offers the highest accuracy of 98.77%, where EGB offers the least response time of 1.4×10^{-6} sec. Suggests their suitability for developing IDS tailored to IoT environments, specifically for combating DoS attacks.

Limitations: Limited itself to detecting only the DoS attacks.

[10]	2020	Y	NSL-KDD	Recurrent Neural Network (RNN)

FS Techniques: Yes

Balancing Techniques: Yes

Performance Measure: Accuracy, DR, Precision, Kappa, Matthews Correlation Coefficient (MCC), F1-Score

Main Idea: Introduced an advanced IDS tailored for Fog computing security, crucial for IoT environments. The system employs a multi-layered RNN to detect various cyber-attacks effectively.

Contributions: Development of a Fog computing-based intrusion detection model using deep RNNs, designed to address specific cyber threats prevalent in IoT settings. Data balancing achieved by Majorityclass Undersampling and Minority class Oversampling.

Conclusion: Achieves high accuracy of 91.69% to real-time data, demonstrating the potential to enhance the security landscape of IoT and Fog computing significantly.

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Limitations: Although the proposed model demonstrates high overall accuracy, it exhibits a lower DR of 64.93% for R2L attacks. This underperformance can be partly attributed to the significant imbalance in the NSL-KDD dataset used, which may not adequately represent this attack type to train the model effectively.				
[48]	2020	Y	DS2OS	Random Neural Network (RaNN)
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Introduced a novel lightweight RaNN-based model to predict various cybersecurity attacks on Industrial Internet of Things (IIoT) systems. By employing ML techniques, the model aims to detect diverse threats such as DoS, malicious operations, and data probing, achieving significant improvements in detection accuracy and speed over traditional methods. **Contributions:** The paper proposes a RaNN-based model specifically tailored for IIoT environments capable of high-accuracy threat prediction. **Conclusion:** The RaNN model not only outperforms existing ML models in terms of accuracy and speed, achieving an accuracy of 99.20% and a prediction time of 34.51 milliseconds but also demonstrates potential for real-time application in IIoT systems. **Limitations:** The model is tested on a single non-IoT dataset (DS2OS), which may not fully represent the diverse range of IIoT environments. Additionally, the comparative analysis was conducted against other research that utilized different datasets, potentially affecting the applicability and generalizability of the results.				
[50]	2020	Y	NSL KDD	Multi-CNN
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score, FAR **Main Idea:** Introduced a novel DL-based intrusion detection approach utilizing a multi-CNN fusion method. **Contributions:** The paper proposes a unique method for transforming one-dimensional feature data into a more analyzable format (grayscale graphs), enhancing the suitability of this data for CNN. **Conclusion:** The proposed multi-CNN fusion model demonstrates superior performance with a high accuracy rate of 81.33% and low complexity compared to other DL methods. **Limitations:** Although the proposed model achieves high overall accuracy, it exhibits a lower detection rate (DR) of 35.15% for R2L attacks and 23.50% for U2R attacks. This underperformance can be partly attributed to the significant imbalance in the NSL-KDD dataset used.				
[69]	2020	Y	CISIDS2017	CNN-LSTM
FS Techniques: Jumping Gene adapted Non-dominated Sorting Algorithm **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Presented an advanced IDS using hybrid DL designed to enhance cybersecurity within IoT networks, focusing specifically on detecting DDoS attacks. **Contributions:** The proposed IDS leverages a jumping gene adapted Non-dominated Sorting Genetic Algorithm (NSGA)-II algorithm for efficient data dimension reduction, coupled with CNN-LSTM for high-accuracy classification of cyber-attacks. **Conclusion:** Introduces a robust framework capable of identifying DDoS attacks with high accuracy (99.03%) and efficiency, evidenced by a significant reduction in training time.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Limitations: The current focus is primarily on DDoS attacks; extending this approach to other types of attacks may require additional modifications and testing.				
[75]	2020	Y	Bot-IoT	NB, BN, DT, RF, Random Tree (RT)
FS Techniques: Yes **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recal, TPR **Main Idea:** Addressed the challenge of selecting the most effective ML algorithm for identifying cyber-attacks in IoT networks within smart city contexts. **Contributions:** Utilization of a bijective soft set approach for the selection of the most effective ML classifier among multiple algorithms. **Conclusion:** The comparative analysis of various machine learning algorithms revealed that DT, RT, and RF outperformed other ML techniques in terms of efficiency and accuracy in IDS. These algorithms demonstrated superior capability in handling the complexities and variations present in IDS data, making them more effective for practical security applications in IoT environments. **Limitations:** -				
[78]	2020	Y	Custom	Deep Convolutional Neural Network (DCNN)
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** FNR, ER, Precision, Recall,F1-Score **Main Idea:** Presented a novel IDS tailored for in-vehicle networks, specifically targeting the Controller Area Network (CAN) bus. The proposed IDS utilizes a DCNN optimized from the Inception-ResNet architecture to effectively learn traffic patterns and detect malicious activities without manual feature engineering. **Contributions:** Creation of a fully labeled, publicly available in-vehicle network attack dataset using real vehicle data, enhancing the scope for further research in this field. **Conclusion:** Successfully develops a DCNN-based IDS that adapts the Inception-ResNet architecture to fit the specific data traffic patterns of the CAN bus, utilizing a novel 'frame builder' module to process CAN message IDs directly. This allows the system to effectively learn and identify deviations in network traffic indicative of various message injection attacks. **Limitations:** The complexity of the Inception-ResNet model, even when reduced, may still pose challenges in terms of computational demands and scalability across different vehicle systems.				
[31]	2021	Y	ICSX IDS 2012, CIC-IDS-2017	Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH)
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Precision, Recall, F1-score **Main Idea:** Introduced a novel ML-based approach tailored to address the unique challenges of anomaly detection within the IoT networks, which are constrained by limited energy and computing resources. **Contributions:** Developed a lightweight ML algorithm using Probabilistic Hierarchical Intrusion Correlation and Detection (PHICAD) using BIRCH specifically designed for resource-constrained environments typical of IoT networks, addressing the need for efficient anomaly detection without compromising the network's functionality. Implemented an architecture that adheres to the layering principle commonly found in computer communications, which ensures flexibility and enhances security by isolating different network layers.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Conclusion: Concludes that traditional ML approaches for network security need significant adaptation to be viable for IoT networks, which face unique challenges such as limited power and computational capacity. By developing tailored lightweight ML algorithms and adopting a layered architectural approach, this study provides a framework that enhances anomaly detection in IoT networks and improves the explainability of the detected anomalies. **Limitations:** While the model showed strong performance in detecting Scanning, DoS, and DDoS attacks, it struggled to effectively identify other types of attacks, indicating a need for further model refinement. Additionally, when comparing F1-Scores, the model's performance was inferior to that of k-Nearest Neighbours (kNN), DT, and RF, suggesting these algorithms may be more adept at balancing precision and recall in diverse attack scenarios.				
[44]	2021	Y	UNSW-NB15	kNN, Stochastic Gradian Decent (SGD), RF, LR, NB
FS Techniques: Filter: Chi-Square **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, MSE, Precision, Recall, F1-score, TPR, and FPR **Main Idea:** Explored the effectiveness of various ML classifiers for network intrusion detection, specifically using the UNSW-NB15 dataset. **Contributions:** Applied multiple ML classifiers (kNN, SGD, RF, LR, NB) to the UNSW-NB15 dataset to evaluate their performance in network intrusion detection. Implemented Chi-Square feature selection to refine the dataset, reducing feature dimensionality and potentially improving classifier performance. **Conclusion:** Concludes that among the tested classifiers, RF performs best with 99.57% accuracy and 100% F1-Score. The Chi-Square feature selection streamlines the dataset and slightly enhances the performance of classifiers, particularly RF. **Limitations:** The study focuses on binary classification, and extending this work to multi-class classification could provide a more comprehensive assessment of intrusion detection capabilities.				
[45]	2021	Y	NSL-KDD, DS2OS, BoT-IoT	RF, kNN, XGB
FS Techniques: Filter1: Correlation Based; Filter2: Gain Ratio (GR); Wrapper: RF-based **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, DR, F1-Score **Main Idea:** Presented an intelligent cyber attack detection system for IoT networks utilizing a novel hybrid feature reduction approach. **Contributions:** Combined feature ranking techniques—correlation coefficient, random forest mean decrease accuracy, and gain ratio—to refine the feature set. **Conclusion:** Proposed framework significantly improves cyber attack detection in IoT networks by employing a novel hybrid feature selection approach and leveraging advanced ML techniques, especially XGB. **Limitations:** The complexity of the hybrid feature selection process might introduce computational overhead, affecting the scalability of the system in larger, real-time environments.				
[65]	2021	Y	AWID	ANN
FS Techniques: Wrappers: SVM, DT, NB **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, DR, FAR, MCC **Main Idea:** Introduced a centralized IDS that leverages DL for feature abstraction and multiple ML techniques for effective feature selection to enhance the detection of malicious activities in IoT environments.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Used an unsupervised autoencoder for deep feature abstraction to generate additional features, enhancing the system's ability to identify anomalies. Applied multiple wrapper-based feature selection techniques (SVM, DT, and NB) to refine the feature set for optimal classification. **Conclusion:** Proposed IDS effectively identifies malicious activities within IoT environments, achieving a high detection accuracy of up to 99.95% on the AWID. **Limitations:** The approach utilized the top features selected by the three feature selection methods. Comparative analysis indicates that the detection rate using this feature set is lower than the feature set selected through the SVM wrapper. This finding suggests that further exploration is needed to enhance feature selection and improve detection accuracy.				
[81]	2021	Y	KDD99, NSLKDD, BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, MQTTset, IoT-23	Conditional Generative Adversarial Network (CGAN)
FS Techniques: Not Used **Balancing Techniques:** Yes **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Introduced a novel framework for anomaly detection in IoT networks using CGAN, particularly focusing on overcoming data imbalances. By employing one-class CGANs (OCGAN) for learning minority classes and binary-class CGANs (BCGAN) for data augmentation, the study enhances the robustness of anomaly detection models in binary and multiclass settings. **Contributions:** Demonstrated the effectiveness of cGAN-based models in detecting anomalies across various IoT networks using multiple datasets, achieving superior performance metrics compared to traditional methods. **Conclusion:** CGANs approach effectively addresses the challenge of imbalanced datasets in IoT anomaly detection, with ocGAN focusing on dataset balancing and bcGAN on data augmentation. **Limitations:** It is implicit that the proposed models would demand considerable computational power, especially when handling multiple large-scale datasets as indicated.				
[6]	2022	Y	IoTID20, NSL-KDD	Bagging, DT, kNN,MLP
FS Techniques: Filters: Union of Information Gain (IG) & GR and Intersection of IG & GR **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Introduced a novel feature selection and extraction method for IDS in IoT networks, utilizing entropy-based approaches and mathematical set theory. **Contributions:** Introduced a hybrid feature selection approach combining IG and GR with set theory operations (intersection and union) to optimize the feature set for ML classification. **Conclusion:** The proposed feature selection and extraction framework significantly enhances the performance of IDS by effectively reducing the feature space and improving classification accuracy to 99.70%. **Limitations:** The dependency on entropy-based methods and set theory may not capture all types of dependencies or interactions between features, potentially overlooking some subtle but critical patterns relevant for detecting sophisticated cyber threats.				
[8]	2022	Y	NSL-KDD++, UNSWNB15 , CIDCC-2017	Cascade Forward Neural Network (CFNN)
FS Techniques: Not Used **Balancing Techniques:** Not Used				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Performance Measure: Accuracy, Precision, Recall,F1-Score, Receiver Operating Characteristic Curve (ROC) **Main Idea:** Introduced a novel IDS for IoT networks, utilizing a Political Optimizer (PO) with a CFNN model, termed PO-CFNN. **Contributions:** Implemented a three-stage process including data preprocessing, intrusion classification using CFNN, and parameter optimization using the PO algorithm to improve the accuracy and efficiency of the IDS. **Conclusion:** The PO-CFNN model provides an effective solution for detecting and classifying intrusions in IoT networks. Through a systematic approach involving data preprocessing, advanced neural network classification, and optimization of model parameters, the system demonstrates enhanced performance compared to conventional IDS solutions. **Limitations:** All the datasets utilized for performance analysis of the proposed method are general IDS datasets, not specifically tailored for IoT environments. This could potentially affect the applicability and accuracy of the findings within actual IoT security contexts.				
[2]	2022	Y	CICIDS-2017 and NSL-KDS	Redefined Long Short-term Memory (RLSTM)
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Presented an RLSTM DL model specifically tailored for detecting DoS attacks in IoT networks. **Contributions:** Implemented preprocessing techniques such as encoding, dimensionality reduction, and normalization to improve the data quality for the IDS. **Conclusion:** Introduces a robust IDS based on RLSTM that significantly improves the detection of DoS attacks in IoT networks and achieved 99.22% accuracy. **Limitations:** Only worked on detecting DoS attacks. Also, while the model shows high accuracy on specific non-IoT datasets, its performance on newer or more varied IoT datasets remains to be tested.				
[19]	2022	Y	BoT-IoT	CNN, LSTM, Gated Recurrent Unit (GRU)
FS Techniques: Yes **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Investigated various DL methods for intrusion detection within IoT systems, implementing and comparing models like CNNs, LSTMs, and GRUs. **Contributions:** Developed intrusion detection solutions using advanced DL techniques, specifically CNNs, LSTMs, and GRUs, tailored for IoT security. Evaluated the proposed models using a standard IoT intrusion detection dataset to establish their effectiveness and superiority over existing methods. **Conclusion:** Presents a robust approach to IoT security using DL models that are rigorously tested against a standard dataset. **Limitations:** DL models, particularly those used in this study, often require significant computational resources, which might not be feasible for all IoT devices, especially those with stringent power and processing limitations.				
[23]	2022	Y	KDDCup-99, NSL-KDD, CICIDS- 2017, BoT-IoT	CNN
FS Techniques: Filter: Reptile Search Algorithm (RSA) **Balancing Techniques:** Not Used				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Performance Measure: Accuracy, precision, Recall,F1-Score **Main Idea:** Introduced a novel IDS framework for IoT environments, utilizing a combination of DL for feature extraction and a metaheuristic optimization method for feature selection. **Contributions:** Developed a CNN model as a core feature extractor aimed at handling IoT-specific datasets effectively. Introduced an innovative feature selection mechanism using the RSA, which optimizes the feature set by mimicking the hunting behavior of crocodiles, enhancing the overall efficiency of the IDS. **Conclusion:** The RSA demonstrated superior feature selection capabilities through extensive testing, contributing to high classification accuracies across various datasets. **Limitations:** While the RSA shows promising results in feature selection, its convergence speed needs enhancement to support real-time intrusion detection requirements better.				
[24]	2022	Y	IoTID20, CIC-IDS-2017, BOT-IoT	SVM, kNN, Linear Discriminant Analysis (LDA), Quadratic Discriminant Analysis (QDA), MLP, DT, LSTM, AE
FS Techniques: Filter: Correlation based **Balancing Techniques:** Random Under Sampling for Majority Class & SMOTE for Minority Class **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Introduced MidSiot, a collaborative IDS for IoT networks, addressing cybersecurity threats across diverse IoT devices. **Contributions:** Developed a collaborative IDS architecture and MidSiot that operates through a three-stage process: classifying IoT device types, differentiating between benign and malicious traffic and identifying specific attack types, utilizing computational resources from the internet and local gateways. **Conclusion:** The MidSiot system offers a robust solution for protecting IoT networks against a range of cyberattacks, demonstrating an average detection accuracy of 99.68%. By deploying a distributed IDS that categorizes device types, traffic, and attack vectors, MidSiot efficiently manages the diverse and resource-constrained nature of IoT environments. **Limitations:** -				
[25]	2022	Y	CIC-IDS-2018 , BoT-IoT	Bidirectional Long Short-Term Memory (BiLSTM)-GRU
FS Techniques: Yes **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Presented the development of a hybrid DL model called BGH for effective intrusion detection in IoT networks. **Contributions:** The BGH model was developed by combining BiLSTM and GRU architectures to enhance the detection of IoT network intrusions. Utilized comprehensive feature extraction techniques, including advanced methods like XGB, DT, and PCA, to improve classification performance. **Conclusion:** The BGH model represents a significant advancement in IoT security, effectively combining multiple DL frameworks to enhance intrusion detection accuracy and efficiency. **Limitations:** -				
[49]	2022	Y	UNSW-NB15 and CI-CIDS2017	CNN (Leightweight)
FS Techniques: Not Used				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Balancing Techniques: Generative Adversarial Network (GAN)				
Performance Measure: Accuracy, Precision, Recall,F1-Score				
Main Idea: Introduced IMIDS, a convolutional neural network-based intelligent intrusion detection system designed to protect IoT devices from cyber threats. IMIDS utilizes a lightweight CNN model to classify various cyber-attacks.				
Contributions: Introduced an attack data generator leveraging a conditional GAN to produce additional training data, significantly enhancing the model's learning and detection capabilities.				
Conclusion: IMIDS represents a significant advancement in IoT security, effectively combining DL and synthetic data generation to address the critical challenge of cyber threat detection in IoT environments.				
Limitations: The reliance on synthetic data for training may introduce biases or overfitting, particularly if the generative models do not accurately represent the diversity of real-world attack vectors.				
[57]	2022	Y	CIC-IDS2017	DNN
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: TPR, FPR, Accuracy				
Main Idea: Introduced Realguard, a deep neural network-based Network-based IDS (NIDS) designed for local IoT gateways. Realguard can detect various cyber attacks in real time while operating within the computational constraints of devices like Raspberry Pi.				
Contributions: Developed Realguard, a lightweight, DNN-based intrusion detection system tailored for IoT gateways, addressing the gap in local security measures for these devices.				
Conclusion: Realguard offers a significant advancement in local network security for IoT environments by combining a lightweight architecture with robust DL techniques to detect a range of cyber threats on resource-limited gateways efficiently.				
Limitations: Frequent retraining requirements could lead to substantial computational and network resource consumption, which could hinder continuous real-time updates and scalability. Also, the proposed model excelled in only detecting DoS, DDoS, & Botnet attacks compared to existing approaches.				
[59]	2022	Y	NSL-KDD	Stacked-Deep Polynomial Network (SDPN)
FS Techniques: Filter: Spider Monkey Optimization (SMO)				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall,F1-Score				
Main Idea: Introduced a new DL-based IDS (DL-IDS) designed for IoT environments, addressing the increasing security challenges due to the rapid expansion in connected IoT devices.				
Contributions: Implemented the SMO algorithm to select optimal features from datasets, enhancing the learning capability and accuracy of the DL-IDS. Utilized SDPN that classifies data into normal or anomalous states, effectively identifying several types of attacks, including DoS, U2R, probe, and R2L.				
Conclusion: Concludes that the proposed DL-IDS is highly effective in detecting severe anomalies in IoT networks. It leverages advanced ML techniques to enhance feature selection and data classification, demonstrating significant improvements in accuracy to 99.02%.				
Limitations: The use of the NSL-KDD dataset, while popular, may not fully represent current IoT-specific threats due to its age and the types of attacks it encompasses, potentially limiting the generalizability of the model to contemporary IoT environments.				
[64]	2022	Y	NSL-KDD	SVM, LR, RF
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Discussed the application of IoT and ML to revolutionize agriculture through smart irrigation and precision farming. It highlights the use of the NSL-KDD dataset to develop an intrusion detection framework to ensure the security of IoT networks in agriculture. **Contributions:** Conducted a comparative analysis of ML algorithms (SVM, LR, RF) based on performance metrics like Accuracy, Precision, and Recall, highlighting the strengths and limitations of each method within the context of IoT security in agriculture. **Conclusion:** Concludes that smart irrigation and precision farming, enabled by IoT and ML, can significantly address water scarcity issues and enhance agricultural productivity. **Limitations:** The study focuses primarily on a single outdated general IDS dataset (NSL-KDD), which may not encompass all types of cybersecurity threats relevant to agricultural IoT networks.				
[66]	2022	Y	ToN-IoT	RF, XGB, Light Gradient Boosting Machine (LGBM), CatBoost
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score,AUC **Main Idea:** Presented an in-depth examination of ensemble decision tree techniques, specifically bagging and boosting, to develop an efficient IDS for IoT networks using the TON-IoT datasets. **Contributions:** Explored various DT ensemble techniques for classifying IoT system network traffic. Conducted a comprehensive comparison of ensemble learning techniques for multiclass classification and threat detection in IoT environments, focusing on optimizing model performance in speed and accuracy. **Conclusion:** Concludes that ensemble-based ML models, particularly LGB, are effective in handling the complex and voluminous data associated with IoT, demonstrating high efficiency in speed and average ROC_AUC score of 98.97%. **Limitations:** While LGB showed promising results, it sometimes compromised on accuracy compared to other algorithms like RF, which could limit its application in scenarios where maximum accuracy is critical.				
[41]	2022	Y	UNSW-NB15	XGB, CatBoost, kNN, SVM, QDA, NB
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision,F1-Score, Mathew correlation coefficient (MCC) **Main Idea:** Introduced an ML-based IDS (ML-IDS) designed to enhance security in IoT networks by applying supervised ML algorithms. It focuses on preprocessing, dimensionality reduction, and classification using several ML models evaluated on the UNSW-NB15 dataset. **Contributions:** Implemented Principal Component Analysis (PCA) for effective dimensionality reduction, enhancing the IDS's efficiency. Developed and assessed multiple ML models tailored for IoT networks, demonstrating high accuracy and competitive performance against existing IDS solutions. **Conclusion:** Developed a robust ML-IDS that successfully identifies network intrusions in IoT environments with minimal resource usage. The IDS performed exceptionally well on the UNSW-NB15 dataset. **Limitations:** The study's reliance on a single outdated dataset (UNSW-NB15) may limit the generalizability of the results across diverse IoT scenarios.				
[82]	2022	Y	IoTID20	DCNN
FS Techniques: Filter: Extra Tree Classifier **Balancing Techniques:** Not Used				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Performance Measure: Accuracy, precision, Recall,F1-Score **Main Idea:** Introduced a deep-convolutional-neural-network (DCNN)-based IDS aimed at enhancing the detection of malicious activities in IoT networks, focusing on improved performance and reduced computational demands suitable for low-power IoT devices. **Contributions:** Conducted a comparative analysis of the proposed DCNN with existing DL and ML models using the IoTID20 dataset, showcasing its superiority in terms of accuracy, precision, recall, and F1-score. **Conclusion:** Presents a DCNN model that not only meets the performance criteria with high accuracy but also addresses the computational efficiency necessary for IoT devices, proving its effectiveness through comprehensive testing against traditional and contemporary models. **Limitations:** While the model reduces computational demands, the scalability and adaptability of the system to newer or evolving cyber threats have not been thoroughly explored, which could limit its long-term applicability in diverse IoT environments.				
[85]	2022	Y	NF-UQ-NIDS (BoT-IoT+ToN-IoT+CICIDS2018+UNSW-NB15)	DNN
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Proposed a DNN-based IDS tailored for IoT networks to detect various types of cyberattacks in real-time. The system is trained on a newly developed Netflow-based benchmark dataset to identify malicious packets effectively. **Contributions:** Developed a DL model incorporating batch normalization and dropout layers to handle normalization and reduce overfitting. Evaluated the proposed model on the NF-UQ-NIDS combined dataset, which integrates data from BoT-IoT, ToN-IoT, CICIDS2018, and UNSW-NB15, covering 20 types of IoT networking attacks. **Conclusion:** Effectively identifies diverse network attacks in IoT environments, showcasing superior performance compared to existing systems. **Limitations:** While the NF-UQ-NIDS dataset encompasses a broad range of attacks, its composition from multiple sources might introduce inconsistencies or biases that could affect the generalizability of the model across different IoT environments.				
[13]	2023	Y	N-BaIoT	Regularized extreme learning machine (RELM)
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,F1-Score **Main Idea:** Introduced the Mayfly Optimization (MFO)-RELM model, a new cybersecurity threat detection and classification system designed for the IoT environment, leveraging a combination of MFO and RELM. **Contributions:** Applied the MFO algorithm to optimize the parameters of the RELM model, enhancing its performance in classifying cybersecurity threats. **Conclusion:** The MFO-RELM model offers a robust solution for cybersecurity threat detection in IoT environments by combining effective data preprocessing, advanced ML, and optimization techniques. The proposed model demonstrated 99.50% accuracy. **Limitations:** -				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
[20]	2022	Y	CICIDS2017, KDDCup 99, UNSWNB15	CNN

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, Precision, Recall,F1-Score

Main Idea: Introduced DFE, a highly efficient and lightweight DL-based NIDS designed specifically for IoT devices with limited processing capabilities.

Contributions: Developed the DFE model, utilizing deep feature extraction by permuting input data into 3D space to reduce the complexity and computational requirements of the neural network.

Conclusion: The DFE model presents a significant advancement in NIDS for IoT environments by achieving high detection accuracy with markedly lower computational demands. This efficiency makes DFE ideal for implementing resource-limited IoT devices, providing robust real-time intrusion detection.

Limitations: While DFE shows overall high classification accuracy, it exhibits some weaknesses in detecting Bot attacks.

[27]	2022	Y	UNSW-BOT-IoT and UNSW15	ANN

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, Precision, Recall, F1-Score, FPR

Main Idea: Presented MUSE, a novel deep hierarchical stacked neural network system designed to detect malicious activities in healthcare networks, particularly addressing the challenges posed by IoT, edge, and core cloud technologies.

Contributions:MUSE employs smaller models at the edge clouds for initial training, which are then aggregated into a larger, partly pre-trained model at the core cloud, significantly reducing training time and epochs needed.

Conclusion: The MUSE system effectively addresses the complex security needs of next-generation healthcare networks by leveraging a unique method of layer merging and aggregation from trained edge models to a core cloud model.

Limitations: -

[40]	2022	Y	CICIDS2018, UNSWNB15	LR, LDA, NB, DT, RF, SVM, GBM

FS Techniques: Filter: Hybrid of Mutual Information (MI) & IG

Balancing Techniques: Not Specified

Performance Measure: Accuracy, Precision, Recall, F1-Score, ROC

Main Idea: Introduced a novel lightweight IDS for IoT devices, featuring an innovative feature selection algorithm, MI2G (MI-IG). The algorithm selects features based on their statistical dependence and entropy reduction.

Contributions: Conducted a detailed experimental analysis validating the effectiveness of the MI2G algorithm in reducing computational costs and improving accuracy across various classifiers.

Conclusion: Utilizing the MI2G feature selection algorithm effectively addresses the challenges of deploying IDS in resource-constrained IoT environments.

Limitations: The MI2G algorithm, although effective, might not capture all relevant features in extremely noisy or complex datasets, potentially affecting the system's ability to detect subtle or sophisticated attacks.

[73]	2022	Y	IoTID20, UNSW-NB15	RF

FS Techniques: Filter: Improved Dynamic Sticky Binary Particle Swarm Optimization (IDSBPSO)

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Employed	Algorithms
Balancing Techniques: Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** IDSBPSO, a novel feature selection method designed to enhance the efficiency and accuracy of IDS in IoT networks. **Contributions:** IDSBPSO incorporates a dynamic bit-masking strategy to iteratively reduce the search space, allowing for more efficient feature optimization. Introduced dynamic parameters to balance exploration and exploitation, improving the algorithm's performance in feature selection. **Conclusion:** The IDSBPSO algorithm successfully enhances the performance of IoT network IDS by reducing the search space and computational demands, making it suitable for resource-constrained environments. **Limitations:** While IDSBPSO reduces computational time, it still demands considerable resources, suggesting a need for further optimization to make it more applicable to energy-constrained IoT devices.					
[7]	2022	Y	CAR-HACKING DATASET	CNN, CNN-LSTM	
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Precision, Recall, F1-Score **Main Idea:** Presented a high-performance security system designed to protect autonomous vehicle networks from cyber threats using DL models. The system focuses on detecting message attacks in the CAN bus. **Contributions:** Introduced an artificial intelligence-based intrusion detection system tailored for CAN buses in autonomous vehicles, employing CNN and hybrid CNN-LSTM models to enhance the detection and classification of cyber threats. **Conclusion:** Significantly improves the security of autonomous vehicle networks by effectively identifying and classifying cyber threats. **Limitations:** Further research is needed to explore the scalability of the proposed system across different automotive manufacturers and models, ensuring its effectiveness in diverse automotive environments.					
[1]	2023	Y	NSL KDD	SVM, NB,CGAN	
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-score, AUC, TPR, FPR **Main Idea:** Introduced a novel Three-Level IDS using GANs (3LIDS-CGAN) tailored for IoT environments. **Contributions:** Developed a three-tiered IDS architecture, utilizing a firewall for initial packet filtering, a combination of SVM and golden eagle optimization for the first-level intrusion detection, and event-based semantic mapping in the second level for improved anomaly detection. Implemented CGAN in the third-level IDS to accurately identify adversary packets that mimic normal behavior, significantly reducing false positives. **Conclusion:** The proposed 3LIDS-CGAN model demonstrates an advanced capability for securing IoT environments by efficiently identifying and classifying different types of intrusions. **Limitations:** -					
[26]	2022	Y	ToN-IoT	kNN, XGB, DT, RF	
FS Techniques: Filter: Chi-Square **Balancing Techniques:** SMOTE **Performance Measure:** Accuracy, Precision, Recall, F1-score, FPR					

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Proposed a novel distributed ML-based IDS for IoT networks, utilizing the ToN-IoT dataset to address the latest security threats in IoT environments effectively. **Contributions:** Emphasized advanced feature selection and class balancing techniques to enhance the detection accuracy of various cyberattacks across multiple layers of IoT infrastructure. **Conclusion:** Demonstrates its effectiveness in accurately detecting and classifying malicious activities in IoT networks using a contemporary and comprehensive dataset. Combining Chi-Square-based feature selection, SMOTE for class balancing, and advanced ML algorithms like XGB ensures robust security measures for IoT systems. **Limitations:** -				
[4]	2023	Y	NSL KDD2015, CI-CIDS2017	Modified Elman Spike Neural Network (MESNN)
FS Techniques: Wrapper : FSA **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced an innovative Automated Threat Detection using the FSA with Optimal DL (ATD-FSAODL) technique tailored for Cyber-physical Systems (CPS) environments. **Contributions:** Developed the ATD-FSAODL technique employing the FSA for optimal feature subset selection, reducing data dimensionality and emphasizing critical information for threat detection. Utilized an MESNN tailored to meet specific threat detection needs of CPS environments, ensuring high accuracy in real-time scenarios. Implemented the Slime Mold Algorithm (SMA) for meticulous hyperparameter tuning of the MESNN, optimizing the model to achieve maximum performance in detecting and classifying threats. **Conclusion:** The ATD-FSAODL approach demonstrates exceptional performance across benchmark databases, achieving high accuracy, precision, recall, F1-score, and MCC. **Limitations:** The complexity and resource demands of the ATD-FSAODL may limit the practical deployment of it in resource-constrained settings within CPS.				
[55]	2023	Y	ToN-IoT, UNSWNB15, Bot-IoT	LR, DT, RF, NB, kNN, SVM
FS Techniques: Gini Impurity-Based Weighted Forest (GIWRF) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, DR, F1-Score, AUC **Main Idea:** Explored the efficacy of ML models and feature extraction techniques such as PCA and GIWRF in enhancing the performance of network intrusion detection systems (NIDS) for IoT networks. **Contributions:** Evaluated six ML models (LR, DT, NB, RF, kNN, SVM) combined with PCA and GIWRF feature extraction methods to determine their effectiveness in detecting intrusions across multiple NIDS datasets. **Conclusion:** Demonstrates that while certain combinations like RF with GIWRF achieve high accuracy on specific datasets, no single approach excels universally. **Limitations:** The variability in performance across different datasets indicates a lack of a universally effective combination of ML models and feature extraction techniques, suggesting a gap in current research towards developing truly generalizable NIDS solutions.				
[11]	2023	Y	N-BaIoT	CNN-Quasi RNN
FS Techniques: Wrapper: Modified Firefly Optimization (FFO) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score, AUC				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Introduced a novel Hybrid Metaheuristics with ML-based Botnet Detection (HMMLB-BND) method for cloud-aided IoT environments, employing advanced feature selection and hybrid neural network models to enhance the detection and classification of botnet attacks. **Contributions:** Developed the HMMLB-BND technique incorporating a modified FFO algorithm for feature selection, a hybrid CNN-Quasi RNN model for classification, and Chaotic Butterfly Optimization Algorithm (CBOA) for hyperparameter tuning. Implementing MFFO for feature selection improves exploration capabilities and avoids local optima, enhancing the system's detection accuracy. **Conclusion:** The HMMLB-BND method demonstrates superior performance in detecting botnet activities within cloud-based IoT systems compared to existing methods. **Limitations:** While the HMMLB-BND method shows promising results, its computational demand and the complexity of integrating hybrid algorithms may limit its practical deployment in resource-constrained environments.				
[14]	2023	Y	BOT-IoT	Convolutional Variational Auto Encoders (CVAE)
FS Techniques: Wrapper: Chaotic Binary Pelican Optimization Algorithm (CBPOA) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced the Botnet Detection using the CBPOA with DL (BNT-CBPOADL) technique, designed to effectively detect and categorize botnet attacks in IoT environments using advanced feature selection and DL strategies. **Contributions:** The BNT-CBPOADL algorithm integrating Z-score normalization, CBPOA-based feature selection, CVAE classification, and Arithmetical optimization Algorithm (AOA)-based hyperparameter tuning to enhance botnet detection accuracy. **Conclusion:** The BNT-CBPOADL method has demonstrated exceptional performance in detecting botnets within IoT platforms, proving superior to existing methods with an accuracy of 99.50%. **Limitations:** While the BNT-CBPOADL method shows high accuracy, the complexity of its implementation may pose challenges in real-world applications, particularly in terms of computational demands and integration with existing IoT infrastructures.				
[17]	2023	Y	CICIDS2017, KDDCup 99	LR, DT, RF, NB, ,GRU, RNN, LSTM, BiLSTM
FS Techniques: Not Used **Balancing Techniques:** SMOTE **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced an IoT-empowered smart cybersecurity framework called the Internet of Drones (IoDs), utilizing ML and DL techniques to enhance security measures in drone networks, addressing vulnerabilities and effectively detecting cyber-attacks. **Contributions:** Developed a cybersecurity framework for drone-based networks integrating DL models, specifically BiLSTM and LSTM, to identify and mitigate security threats efficiently. Implemented SMOTE to balance the datasets to ensure robust model training and effective classification of attack patterns. **Conclusion:** The proposed IoD framework leverages advanced ML techniques to provide a secure environment for IoT-enabled drones, demonstrating superior performance in cyber-attack detection compared to traditional models. **Limitations:** The complexity of integrating and maintaining such advanced models in real-world drone operations poses practical challenges. Also, the datasets used were general IDS datasets that may not represent the challenges faced in drone networks.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
[34]	2023	Y	NSLKDD, KDDCUp99,	LR,FFNN, 1DCNN, AE, Vanilla RNN, LSTM, GRU

FS Techniques: Not Used

Balancing Techniques: SMOTE

Performance Measure: Accuracy, Precision, Recall, F1-Score, AUC

Main Idea: Proposed a Federated Learning-based anomaly detection framework for smart grids, training ML models directly on smart meters to enhance privacy and reduce data security risks associated with central server-based systems.

Contributions: Developed novel ML models for smart grid anomaly detection and created a federated learning testbed using Raspberry Pi devices to perform on-device training without data sharing. Conducted in-depth experimental analysis using real hardware to assess the resource efficiency of FL models in smart meter contexts.

Conclusion: Federated Learning enhances privacy and reduces latency in anomaly detection within smart grids by decentralizing the data processing to the smart meters themselves. This approach shows promise in maintaining high performance while significantly reducing the vulnerability to privacy breaches and network dependency.

Limitations: -

[46]	2024	Y	IOTID20,IOT23	Different Ensemble Learners

FS Techniques: Filter: Correlation

Balancing Techniques: Not Used

Performance Measure: Accuracy, Precision, Recall, F1-Score, Expected Maximum Reward, Harmonic Low Score, Composite Key Score

Main Idea: Developed a cognitive cybersecurity methodology that enhances human analytical capabilities by reconciling conflicting vulnerability reports and preprocessing advanced embedded indicators using ML, significantly improving the reliability of cybersecurity data sets.

Contributions: Introduced a cognitive cybersecurity methodology that addresses diversification and asymmetric information challenges in vulnerability reporting. Utilized ensemble methods combining LSTM, NBSVM, LR, and MLP to improve the accuracy and reliability of cybersecurity vulnerability detection.

Conclusion: The proposed cognitive cybersecurity approach effectively synchronizes and enhances data from diverse internet security sources, allowing for more accurate vulnerability assessment and classification.

Limitations: The variability in the performance of different ML models suggests that further optimization and testing are needed to achieve consistent and universally high accuracy across all cybersecurity datasets.

[52]	2023	Y	BOT-IoT, TON-IoT	LR, SVM,MLP

FS Techniques: Not Used

Balancing Techniques: Not Used

Performance Measure: Accuracy, AUC

Main Idea: Introduced a novel intrusion detection approach for IoT environments utilizing the Stream Classification Algorithm Guided by Clustering (SCARGC) to address extreme verification latency (EVL) challenges.

Contributions: Developed an ML-based detection model integrated with an EVL method, SCARGC, to handle nonstationary environments and concept drift in IoT security.

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Conclusion: The SCARGC framework effectively enhances the resilience and adaptability of IoT intrusion detection systems, showing promise in managing the dynamic nature of cyber threats within IoT networks.				
Limitations: The effectiveness of the SCARGC model in broader and more diverse IoT environments remains to be thoroughly tested. Adapting DL models to the EVL framework, which could offer more sophisticated detection capabilities, has not yet been implemented.				
[53]	2023	Y	BOT-IOT	Adaboost, NB, kNN, QDA, DT, RF, MLP
FS Techniques: Embedded: RFR				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall,F1-Score				
Main Idea: Explored the effectiveness of ML algorithms in enhancing cybersecurity for IoT networks, specifically against Network-related DoS attacks.				
Contributions: Applied multiple ML algorithms to detect IoT network attacks promptly, using the Bot-IoT dataset for performance evaluation. Feature selection was performed using an embedded approach with the RFR to optimize the effectiveness of the ML models.				
Conclusion: Demonstrates that ML algorithms can significantly enhance the detection of cyber attacks within IoT networks, employing the Bot-IoT dataset and CIC Flow-Meter for feature extraction and evaluation. The Random Forest Regressor is crucial in identifying the most relevant features for ML cybersecurity applications.				
Limitations: The study lacks a comparative analysis with proper results, potentially limiting the assessment of the proposed ML methodology's efficacy relative to other approaches.				
[60]	2023	Y	IOTID20	RF,DT,kNN,MLP
FS Techniques: Filter: MI				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score, AUC				
Main Idea: Introduced an ML-driven methodology for detecting and classifying cyber-attacks in IoT networks, emphasizing the system's defense against adversarial ML attacks like JSMA, FGSM, and DeepFool, and exploring the efficacy of adversarial training.				
Contributions: Incorporated multiclass classification for identifying cyber-attacks using ML algorithms, tested on the IoTID20 dataset. Implemented feature selection using a Filter based on MI greater than a threshold to enhance classifier effectiveness.				
Conclusion: The proposed ML framework successfully classifies IoT network threats with high accuracy and demonstrates enhanced resilience to adversarial attacks through adversarial training, offering a robust defense without degrading performance on legitimate data.				
Limitations: The computational intensity of adversarial training may limit its application in resource-constrained IoT settings.				
[74]	2023	Y	UNSW BoT IoT	Adaboost, DT, RF, ANN, LSTM, AE
FS Techniques: Filter: Correlation				
Balancing Techniques: SMOTE				
Performance Measure: Accuracy, Precision, Recall, F1-Score				
Main Idea: Developed an ML-based anomaly detection system for smart homes, using the UNSW BoT IoT dataset to evaluate performance across multiple classifiers.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Implemented an anomaly detection framework that analyzes IoT device traffic in smart homes using six different ML algorithms. Developed a high-performing anomaly detection model that utilizes a machine-learning classification approach, enhanced by feature selection methods such as Filter: Correlation Based and balancing by SMOTE, significantly improving detection capabilities. **Conclusion:** The proposed ML framework offers robust protection for IoT devices in smart homes, achieving high accuracy in anomaly detection across various attack categories. The use of advanced feature selection and balancing techniques contributes to the model's effectiveness, providing a secure environment and safeguarding user privacy and safety. **Limitations:** The computational efficiency of the proposed models, especially in resource-constrained smart home environments, needs further evaluation to ensure they are practical for widespread deployment.				
[76]	2023	Y	TON-IoT	Ensemble of 3 CNNs
FS Techniques: Not Used **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, Sensitivity, Specificity, F1-Score **Main Idea:** Presented an innovative ensemble DL-based IDS enhanced with explainable Artificial intelligence (AI) techniques for the IIoT networks. **Contributions:** Introduced a robust ensemble DL architecture that not only enhances intrusion detection accuracy in IIoT systems but also boosts interpretability, helping cybersecurity professionals understand and trust the system's decisions. **Conclusion:** By integrating three CNN models and an Extreme Learning Machine (ELM) model, alongside SHAP and LIME for explainability, the IDS effectively distinguishes between normal and anomalous behaviors while improving the transparency of its decision-making process. **Limitations:** The sophisticated architecture involving multiple CNN models and ensemble methods may require significant computational resources, which could be a constraint in some IIoT environments.				
[83]	2023	Y	BOT-IoT, TON-IoT	An Ensemble Model
FS Techniques: Yes **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Sensitivity, F1-Score **Main Idea:** Explored the application of ML to enhance network security in IoT systems, presenting a hybrid ML model that effectively detects anomalies. **Contributions:** Introduced a novel hybrid ML model that strategically combines RF, XGB, kNN, and DT algorithms with assigned weights to optimize anomaly detection in IoT environments. **Conclusion:** The proposed hybrid ML model demonstrates superior performance in detecting misbehaviors in IoT systems, showcasing its potential as a robust solution for securing increasingly interconnected and vulnerable IoT networks. **Limitations:** While the hybrid model shows promising results, the complexity of managing multiple algorithms might impact the model's efficiency and speed, particularly in real-time scenarios where quick response is crucial. Although designed for resource-constrained environments, the actual resource consumption of the hybrid model needs thorough evaluation to ensure it does not exceed the typical capacities of IoT devices.				
[94]	2023	Y	N-BAIOT, Kitsune, WUSTL	Resource Efficient DNN (REDNN), Resource Efficient Federated DNN (REFDNN)
FS Techniques: Not Used **Balancing Techniques:** Not Used				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Performance Measure: Accuracy, Precision, Recall, F1-Score **Main Idea:** Addressed the challenges of training DNNs for IoT security by introducing the REDNN and REFDNN methodology, which incorporates regularization and simulated micro-batching to enhance performance in resource-constrained environments. **Contributions:** Applied federated learning to train DNNs across distributed IoT devices, ensuring data privacy while reducing memory and processing requirements. **Conclusion:** The REDNN and REFDNN models significantly improve the efficiency and effectiveness of IoT security systems. They have been validated across multiple datasets, showing notable resource conservation and high accuracy in detecting cyberattacks. **Limitations:** While the proposed optimization method incorporating regularization and simulated micro-batching aims to enhance model performance, its effectiveness can vary significantly across different network architectures and data characteristics. This variability may limit the generalizability of the method, particularly in complex or highly dynamic IoT environments where data distributions and network behaviors can significantly differ from those in controlled experimental settings.				
[5]	2024	Y	CIC-IDS2017	LSTM
FS Techniques: Filter: Chi-Square **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced a sophisticated LSTM-based IDS integrated with a Dynamic Access Control (DAC) algorithm specifically designed for IoT environments. **Contributions:** Leveraged novel features like the DAC algorithm in the IDS to enhance security by preventing repeated intrusions from the same source and optimizing detection rates to minimize false positives, thus reducing service interruptions. **Conclusion:** Achieves high accuracy in detecting and defending against intrusions, maintaining a balance between security and user experience with fast response times and low FAR. **Limitations:** The model was tested using the non-IoT specific CIC-IDS2017 dataset, and the computational resources required may be substantial, particularly when implementing complex models like LSTM. This could pose challenges in resource-constrained IoT environments.				
[29]	2024	Y	BoT-IoT, Edge-IIoT, NSL-KDD	LSTM
FS Techniques: Filter: IG; Wrapper: GA **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall,FNR, FPR **Main Idea:** Introduced IDS-SIoDL, an advanced IDS tailored for IoT-based smart cities, which integrates LSTM and feature engineering techniques to address IoT interface attacks in real-time efficiently. **Contributions:** IDS-SIoDL model incorporates DL with feature engineering techniques (AE, MI, GA) to improve intrusion detection. **Conclusion:** Successfully demonstrates the effectiveness of the IDS-SIoDL system in identifying and mitigating threats in IoT networks, with exceptional performance of 99.71% accuracy and 4 ms validation time. **Limitations:** The reliance on TPUs for training and classification could limit deployment options, particularly in settings where such resources are not readily available or cost-effective.				
[36]	2024	Y	NSL-KDD	SVM
FS Techniques: Wrapper: FFO **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score, AUC Score				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Advanced IoT and WSN security by developing a novel FA-ML technique that combines ML with the FFO for enhanced intrusion detection.				
Contributions: The FA-ML technique integrates the FFO for feature selection with SVM optimized by GWO.				
Conclusion: The FA-ML technique for robust security in WSN-IoT environments outperformed other ML approaches with 99.34% accuracy and 99.67% F1-Score.				
Limitations: Although the NSL-KDD dataset is a standard benchmark in intrusion detection research, it is dated and may not include the latest attack types or the complex behavior of modern cyber threats in IoT and WSN environments. The dataset's age and the static nature of its scenarios limit the ability to assess the effectiveness of the FA-ML technique against current and emerging threats.				
[92]	2024	Y	CICIoT2023, TON-IoT	CNN, LSTM
FS Techniques: Filter: Correlation				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score				
Main Idea: Presented a hybrid DL algorithm combining CNN and LSTM, optimized for detecting DDoS attacks within IoT environments.				
Contributions: Introduced a novel hybrid algorithm by combining 1D-CNN with LSTM for both binary and multi-class classification of the attacks.				
Conclusion: Successfully develops and validates a high-performance IDS that uses advanced DL to detect DDoS attacks, achieving near-perfect accuracy of 99.97%.				
Limitations: Does not capture the full spectrum of other types of cyber threats that could impact diverse IoT networks. The computational resources required for training and testing the hybrid model, especially on-device deployment in IoT contexts.				
[47]	2024	Y	Edge-IIoTset	Deep Transfer Learning (DTL) with GA using Multiple pre-trained CNNs
FS Techniques: Yes				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score, Kappa				
Main Idea: Introduced an advanced IDS for the IIoT using DTL and a tri-layer architecture combining CNN, GA, and bootstrap aggregation.				
Contributions: Contributed a novel IDS framework that utilizes a combination of state-of-the-art pre-trained CNN architectures and genetic algorithms for hyperparameter optimization, along with an ensemble technique for integrating the best models.				
Conclusion: The proposed IDS framework demonstrates exceptional efficacy in detecting multiple types of cyberattacks in IIoT networks, achieving perfect attack detection rates.				
Limitations: The use of multiple advanced CNN architectures and GA for hyperparameter tuning might result in significant computational overhead limiting the practical deployment in IoT environments. Also, the pre-trained models, like VGG16, VGG19, and Inception, were designed for tasks other than intrusion detection, such as image recognition or classification.				
[79]	2024	Y	NSL KDD	Adaboost
FS Techniques: Filter: Particle Swarm Optimization (PSO)				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Sensitivity, Specificity, Precision, Recall				
Main Idea: Introduced an ML-based IDS (ML-IDS) combining PSO and AdaBoost algorithms for effective malware detection in health app platforms.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Innovatively applied the synergy of PSO for feature selection and AdaBoost for classification, demonstrating high performance in detecting various attack types within health-related IoT environments.				
Conclusion: Shows that the ensemble learner AdaBoost gave a better performance with an accuracy of 98.50% when compared to other traditional ML algorithms.				
Limitations: The study utilizes the NSL KDD dataset from 2009, which, while commonly used, may not fully represent the current and specific threats encountered in medical IoT environments.				
[56]	2024	Y	CICIDS2017	CNN, LSTM
FS Techniques: Not Used				
Balancing Techniques: Not Used				
Performance Measure: Categorical Cross Entropy, Accuracy				
Main Idea: Introduced an advanced IDS for IoT networks, using DL techniques to analyze the CICIDS2017 dataset for detecting various attacks.				
Contributions: Contributed a DL model utilizing a 1D Convolution layer and LSTM architecture, capable of recognizing spatial and temporal patterns in data, which significantly outperforms traditional ML models in detecting various types of cyberattacks on IoT networks.				
Conclusion: The proposed hybrid architecture has given higher performance with an accuracy of 99.70% when compared to other DL models.				
Limitations: The study's reliance on the CICIDS2017 dataset, which is not specifically tailored for IoT environments and may not reflect the most current threat landscape, presents a significant gap.				
[43]	2024	Y	Edge-IIoT	CNN, LSTM, GRU
FS Techniques: Filter:Chi-square				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score, Log Loss				
Main Idea: Introduced an innovative IDS for IoT-based electric vehicle charging stations using a hybrid DL architecture.				
Contributions: Contributed a novel hybrid architecture that integrates CNN, LSTM, and GRU for high-efficiency intrusion detection in IoT environments, validated with real-world datasets and exhibiting scalability and practical applicability.				
Conclusion: This architecture shows superior performance over other traditional and hybrid DL models with an accuracy of 97%.				
Limitations: Features selection was done using Chi-Squared test based filter. The Chi-Square test effectively identifies linear associations between categorical variables and outcomes. However, it may not capture complex, non-linear relationships that could be critical in cybersecurity data. Also, it evaluates features individually for their relationship with the response variable, which might overlook the potential interaction effects between features. Also, the model performed poorly with SQL Injection and XSS attacks.				
[18]	2024	Y	TON-IoT	Stack Classifier of NB, RF, kNN, SVM
FS Techniques: Filter: SelectKBest method using ANOVA F-Score				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score				
Main Idea: Presented a ML-based stack classifier model for IoT intrusion detection, employing feature selection and ensemble modeling to enhance classification metrics and secure IoT networks significantly.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Provided a comprehensive analysis of current intrusion detection methods, identified key limitations and introduced an innovative heterogeneous ML-based stack classifier model that incorporates feature selection and ensemble modeling to enhance IoT network security significantly. **Conclusion:** Ensemble learning approaches perform better than the traditional ones. Additionally, incorporating the K-Best feature selection algorithm and ensemble modeling has significantly enhanced intrusion detection within IoT networks. **Limitations:** The scoring function used by K-Best feature selection is based on the ANOVA F-value and assesses features based solely on their linear relationship with the output variable.				
[61]	2019	N	UNSW-NB15, CICIDS-2017	RF
FS Techniques: Filter: Binary Bat Algorithm (BBA) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, FPR **Main Idea:** Introduced a Hypervisor Level Distributed Network Security (HLDNS) framework designed for cloud computing environments. **Contributions:** Development of the HLDNS framework that monitors virtual machine (VM) network traffic at each server within cloud computing environments for enhanced intrusion detection. Integration of a feature selection mechanism using an extended BBA with two novel fitness functions aimed at improving the detection capabilities of the RF classifier. **Conclusion:** Successfully enhances cloud network security by efficiently monitoring and detecting both known and unknown network intrusions. Using signature-based and anomaly detection techniques, coupled with advanced feature selection, improves the precision and reduces the computational demand of the system. **Limitations:** Effectiveness of the HLDNS framework in detecting attacks that involve encrypted data remains a challenge due to the complexity of analyzing encrypted network traffic.				
[80]	2019	N	NSL-KDD	SVM,ANN
FS Techniques: Wrapper: SVM; 2 Filters: Correlation & Chi-Square **Balancing Techniques:** Not Used **Performance Measure:** Accuracy **Main Idea:** Developed a novel supervised ML system to classify network traffic as malicious or benign, using a combination of supervised learning algorithms and feature selection methods, with a focus on comparing ANN and SVM techniques. **Contributions:** Introduction of an ML model that combines ANN with an advanced wrapper-based feature selection method. This model is contrasted with an SVM technique for classifying network traffic. The feature selection integrates a wrapper using SVM and two filters: Correlation-Based and Chi-Square-Based methods. **Conclusion:** Confirms that the ANN model paired with wrapper feature selection surpasses other models in accurately classifying network traffic, achieving a detection rate of 94.02%. **Limitations:** Despite the improvements, the system primarily detects known attacks effectively, while the detection of zero-day or novel attacks remains challenging due to high false positive rates, indicating a need for further research in this area. Also, it used only accuracy as a performance measure.				
[87]	2019	N	NSL-KDD	DNN
FS Techniques: Filter: Coorelation **Balancing Techniques:** Not Used **Performance Measure:** Accuracy				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Explored the application of feature selection and layer configuration to improve the learning efficiency of DNNs for intrusion detection. **Contributions:** Introduction of a methodology for enhancing the learning time of DNN in intrusion detection systems through targeted feature selection and layer configuration. **Conclusion:** Confirms that appropriate feature selection and neural network layer configuration enhance the performance of IDS by reducing training time and avoiding overfitting. Highlights the balance between reducing computational overhead and maintaining high detection accuracy, providing a promising approach for developing efficient and effective intrusion detection systems. **Limitations:** Primarily addresses learning time, with less emphasis on other critical performance metrics such as detection speed in real-time scenarios and scalability. Also, the accuracy of performance measures is unsuitable for imbalanced datasets like NSL KDD.				
[91]	2019	N	NSL-KDD, UNSW-NB15	DNN
FS Techniques: Not Used **Balancing Techniques:** Improved Conditional Variational Auto Encoder (ICVAE) **Performance Measure:** Accuracy, Precision, Recall, F1-Score, FPR **Main Idea:** Introduced ICVAE-DNN, a novel intrusion detection model for enhanced detection of anomalies in IoT networks. **Contributions:** Introduction of ICVAE for deep feature abstraction and generating synthetic attack samples to address data imbalance and increase sample diversity and DNN for modeling the labeled data. **Conclusion:** Integrated ICVAE for data balancing and feature initialization and DNN for advanced classification. Hence, the model achieves high accuracy and low FPR, proving its effectiveness in detecting various attack types. **Limitations:** Computational complexity of the model, particularly when initializing and training the DNN with enhanced features from ICVAE, may require significant computational resources, which could be a constraint in resource-limited environments.				
[39]	2020	N	UNSW-NB15	SVM, kNN, LR, DT,ANN
FS Techniques: Filter: XGB **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Presented a study on ML-based IDS that focuses on the challenges of high dimensional data and class imbalance in network security. **Contributions:** Implementation of a filter-based feature reduction using XGB to optimize the feature space for ML models. Multiple ML techniques, including SVM, kNN, LR, ANN, and DT, are utilized within the reduced feature space. **Conclusion:** Used the XGB algorithm for feature selection in IDSs, resulting in performance gains across various ML models. Experiments show that reduced feature sets decrease model complexity and enhance accuracy on test data, especially noted in DT's performance improvement from 88.13% to 90.85% in binary classification. **Limitations:** -				
[37]	2020	N	UNSW-NB15, AWID	FFDNN
FS Techniques: Wrapper: Extra Tree **Balancing Techniques:** Not Used **Performance Measure:** Accuracy **Main Idea:** Presented a wireless IDS employing a Deep Long Short-Term Memory (DLSTM) based classifier.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Using the NSL-KDD dataset, the performance of DLSTM is compared with traditional ML and DL methods.				
Conclusion: Successfully demonstrates the effectiveness of the DLSTM model in wireless network intrusion detection, surpassing traditional ML methods in accuracy and other performance metrics.				
Limitations: The computational complexity and resource requirements of the DLSTM model could be a constraint in deployment scenarios with limited computational capabilities. Also, accuracy is only used as a performance measure.				
[96]	2020	N	CICIDS2017	CNN
FS Techniques: Not Used				
Balancing Techniques: SMOTE				
Performance Measure: Accuracy, FAR, DR, Precision, F1-Score				
Main Idea: Proposed a novel intrusion detection model, SGM-CNN, that addresses class imbalance in network intrusion detection by combining statistical balancing methods.				
Contributions: Introduction of the SGM method that uses SMOTE for oversampling minority classes and GMM for cluster-based under-sampling of majority classes to balance the dataset efficiently.				
Conclusion: Effectively handles class imbalance in large-scale intrusion detection datasets and achieves high detection rates. Specifically, the model reached detection rates of 99.74% in binary classification, 96.54% in multi-class classification on the UNSW-NB15 dataset, and 99.85% in a 15-class classification on the CICIDS2017 dataset.				
Limitations: The SGM-CNN model, while effective, might require substantial computational resources, potentially limiting its applicability in resource-constrained environments.				
[38]	2020	N	NSL-KDD	DLSTM
FS Techniques: Filter: IG				
Balancing Techniques: Not Used				
Performance Measure: Accuracy, Precision, Recall, F1-Score				
Main Idea: Introduced a DLSTM-based classifier for wireless IDS, which is evaluated using the NSL-KDD dataset.				
Contributions: Application of a filter-based feature selection algorithm using information gain to optimize data preprocessing for enhancing the model's performance.				
Conclusion: Developed a DLSTM-based IDS that shows significant improvement in detection capabilities compared to existing models. The model achieved an accuracy of 99.51% on validation data and 86.99% on test data, indicating its effectiveness in wireless network intrusion detection.				
Limitations: The NSL-KDD dataset employed for evaluating the methodology is not tailored for wireless network environments, which may affect the generalizability and effectiveness of the proposed model in real-world wireless settings.				
[3]	2020	N	KDD99, UNSW-NB15	Back Propagation Neural network (BPNN)
FS Techniques: Wrapper: Discrete Variant of the Cuttlefish Algorithm (D-CFA)				
Balancing Techniques: Not Used				
Performance Measure: Accuracy				
Main Idea: Focused on a detailed analysis of IDS datasets, specifically KDD99 and UNSW-NB15, employing three distinct methods: Rough-Set Theory, BPNN, and D-CFA. It aims to evaluate the relevance of dataset features in enhancing classification accuracy and performance within intrusion detection systems.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Implementation of Rough-Set Theory to determine the dependency ratio between features and classes, aiding in understanding feature significance. Application of a D-CFA for feature selection across multiple runs, identifying consistently important features. **Conclusion:** Identifies key features within the KDD99 and UNSW-NB15 datasets that significantly contribute to classification performance, suggesting the potential to create more efficient and lightweight IDS models. **Limitations:** The analysis relies solely on accuracy for evaluation, which may not fully represent the model's effectiveness, especially in dealing with imbalanced data or rare attack types.				
[33]	2020	N	NSL-KDD, UNSW NB-15	CNN, BiLSTM
FS Techniques: Not Used **Balancing Techniques:** One-Sided Selection for Majority Class & SMOTE for Minority Class **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced a novel IDS that tackles the challenge of data imbalance in network security through a hybrid sampling approach and a deep hierarchical network. **Contributions:** The model employs a combination of CNN and BiLSTM to extract spatial and temporal features from network data, enhancing the detection capabilities for complex intrusion activities. Introducing a hybrid sampling method that combines OSS and SMOTE to address the imbalance in the dataset, reducing majority class noise and enhancing minority class representation. **Conclusion:** Effectively addresses the challenges posed by imbalanced datasets in network security environments. The system demonstrates enhanced performance metrics such as accuracy, precision, and recall by constructing a balanced dataset and utilizing a sophisticated deep-learning architecture. **Limitations:** The complexity of the deep hierarchical network could introduce computational overhead, potentially affecting the system's scalability and real-time detection capabilities.				
[35]	2020	N	CSE-CIC-IDS2018	kNN, RF, GB, Adaboost, DT, LDA
FS Techniques: Not Used **Balancing Techniques:** SMOTE **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Addressed the inefficiencies in current IDS caused by outdated and imbalanced datasets. Conducted a comparative analysis of six different ML algorithms—kNN, RF, GB, Adaboost, DT, and LDA—combined with an up-to-date and balanced dataset (CSE-CIC-IDS2018). **Contributions:** Application of SMOTE to balance the dataset, thus reducing the imbalance ratio and enhancing the detection capability for minority attack types. **Conclusion:** Demonstrates that using a combination of updated datasets and ML algorithms, specifically with the application of SMOTE for balancing, significantly enhances the performance of IDS. AdaBoos gave an accuracy of 99.70% with the balanced dataset. **Limitations:** The paper primarily focuses on traditional ML models. The exploration of DL models is suggested as future work.				
[42]	2020	N	NSL-KDD, UNSW NB-15, CIC-IDS2017.	DT, RF, NB Tree
FS Techniques: Wrapper: NSGA with LR **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, FAR, DR				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Introduced a multi-objective feature selection approach using NSGA-II and LR to optimize feature selection in NIDS, aiming to enhance classification performance and reduce computational demands by focusing on the most informative features. **Contributions:** The paper proposes a novel feature selection method integrating NSGA-II with logistic regression, evaluated through two schemes—binomial and multinomial logistic regression, across three datasets. **Conclusion:** Shows that binary-class datasets yield better accuracy compared to multi-class datasets using the proposed feature selection method. Successfully reduces computational complexity by selecting the most informative features, showing promise over traditional methods. **Limitations:** The approach may not effectively detect all types of attacks, as indicated by lower performance in identifying certain attack types due to the limited number of instances or missing critical information.				
[54]	2020	N	Own Data	NB, RF, kNN, SVM,ANN
FS Techniques: Filter: MI Based Greedy Approach **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Discussed the development of a robust IDS to identify DDoS attacks using various ML techniques. **Contributions:** Created a new dataset comprising packet data captured during direct attacks on server targets. This dataset includes 25 features across five classes, designed to represent modern attack scenarios not covered in previous datasets. The study focuses on the effectiveness of different classification methods in detecting DDoS attacks accurately, employing the newly compiled dataset. **Conclusion:** Effectively demonstrates that the RF and ANN, among the others tested, provide the highest accuracy of 98.70% in detecting DDoS attacks using the developed dataset. **Limitations:** The incremental approach used for feature selection, starting with the best feature and adding features to maximize MI, may potentially overlook combinations of features that could yield better performance.				
[86]	2020	N	UNSW-NB15	ANN
FS Techniques: Filter: IG Based **Balancing Techniques:** Not Used **Performance Measure:** Accuracy **Main Idea:** Addressed the shortcomings of traditional IDS in detecting DDoS attacks by incorporating ML techniques. **Contributions:** It highlights the significant impact of feature selection on the accuracy and efficiency of the ML model, detailing how selecting the right features can drastically improve detection performance. **Conclusion:** Demonstrates that a carefully selected set of features can significantly enhance the accuracy and efficiency of a neural network model in detecting DDoS attacks, achieving a high accuracy rate of 97.76%. **Limitations:** The research limited to only detecting DDoS attacks. Only used Accuracy for model evaluation.				
[62]	2020	N	Custom	SVM, NB, kNN,ANN
FS Techniques: Filter: Relief filtering algorithm inspired by instance-based learning; Wrapper: A greedy search-based Sequential Forward Selection (SFS); Embedded: Lasso or L1 algorithm **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Sensitivity, Specificity, F1-Score				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Main Idea: Explored the effectiveness of ML models in detecting DDoS attacks within Software Defined Networks (SDN) environments. It highlights the impact of DDoS attacks on SDN controllers. **Contributions:** Utilizes various feature selection techniques (filter, wrapper, and embedded methods) to reduce model complexity and training time, thereby enhancing the interpretability of ML models. **Conclusion:** Confirms the potential of ML to mitigate DDoS threats in SDN by efficiently detecting attacks, demonstrating that feature selection not only simplifies the ML models but also significantly enhances their performance by focusing on the most relevant features. Using the wrapper feature selection method with kNN yielded the best results. **Limitations:** The research limited to only detecting DDoS attacks.				
[68]	2020	N	KDD99	CNN
FS Techniques: Filter: Newly proposed feature selection algorithm called conditional random field and linear correlation coefficient-based feature selection (CRFLCFS) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy , FAR **Main Idea:** Introduced a new IDS designed for wireless networks, which employs a unique feature selection algorithm—Conditional Random Field and Linear Correlation Coefficient-based Feature Selection (CRF-LCFS). **Contributions:** Adoption of a well-established CNN architecture to classify the features selected by CRF-LCFS, enhancing the overall accuracy of the IDS. **Conclusion:** Successfully implemented an IDS that leverages a novel feature selection algorithm and CNN, resulting in high detection accuracy and efficiency in wireless networks. **Limitations:** The computational complexity introduced by the CRF-LCFS algorithm needs further exploration to ensure scalability to larger network infrastructures.				
[71]	2020	N	NSL-KDD, ISCXIDS 2012	CNN
FS Techniques: Wrapper: FFO **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, DR, FPR/FAR, Attack Detection Precision. **Main Idea:** Focused on enhancing IDS for network security, particularly against DDoS attacks, using a hybrid network-based approach combined with DL techniques, specifically CNN. **Contributions:** Utilizes CNN for its robust feature learning capabilities, applying a DL architecture comprising multiple layers to enhance detection accuracy. **Conclusion:** Concludes that the CNN-based IDS shows significant improvements in detecting DDoS attacks compared to traditional methods. The DL approach allows for better handling of complex and voluminous data, typical of network environments, resulting in a higher detection rate of 99.94% with NSL-KDD and 77% with ICSXIDS 2012 datasets. **Limitations:** The DL model, while accurate, might require significant computational resources, potentially limiting its applicability in resource-constrained environments. Also, the model performed very poorly with ICSXIDS 2012 data.				
[72]	2020	N	An opensource NIDS data from Kaggle	DT
FS Techniques: Embedded: DT **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced "IntruDTree," an ML-based intrusion detection model that prioritizes the ranking and selection of important security features to construct a tree-based generalized model.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed

Contributions: The model prioritizes identifying and ranking important security features, which is crucial for handling high-dimensional data in intrusion detection.

Conclusion: The IntruDTree model effectively balances the need for high predictive accuracy and computational efficiency in intrusion detection. It leverages a tree-based approach to reduce the complexity of the model while maintaining high performance.

Limitations: Utilizes a dataset from Kaggle whose reliability and representativeness may not be fully verified.

[88]	2021	N	NSL-KDD	LCVAE, CNN

FS Techniques: Not Used

Balancing Techniques: LCVAE

Performance Measure: Accuracy, Precision, Recall, F1-Score

Main Idea: Introduced a novel DL-based intrusion detection method called Log-Cosh Conditional Variational Autoencoder (LCVAE), designed to enhance the detection accuracy of network intrusions, particularly in scenarios with imbalanced data types and unknown attack classes.

Contributions: The LCVAE method integrates a log-cosh loss function to handle the discrete properties of intrusion data better, maintaining a balance between data generation and reconstruction, which is crucial for dealing with imbalanced classes.

Conclusion: LCVAE method gave an accuracy of 85.51% and F1-Score of 80.78% that are greater than the other data balancing techniques based DNN.

Limitations: While the proposed model boasts a training time of 18 minutes and an evaluation time of 0.9 milliseconds, it relies on high-performance computational resources, specifically an NVIDIA 2080 Ti GPU, which may not be readily available or feasible for all deployment scenarios.

[89]	2020	N	NSL-KDD	SAVAER, DNN

FS Techniques: Not Used

Balancing Techniques: Supervised Variational Autoencoder(SAVAER)

Performance Measure: Accuracy, DR, F1-Score, FPR

Main Idea: Introduced the Supervised Variational Auto Encoders (SAVAER)-DNN. This novel network intrusion detection model combines SAVER with DNN to enhance the detection of known, unknown, and low-frequency attacks in network systems.

Contributions: Presented a unique integration of supervised VAE data generation with WGAN-GP adversarial learning, enhancing feature extraction and data synthesis to improve network intrusion detection.

Conclusion: This hybrid approach not only improves detection rates across various types of network attacks but also enhances the model's ability to generalize across different attack scenarios.

Limitations: The complexity of model training and the computational resources required might limit the deployment in resource-constrained environments.

[93]	2020	N	1% NSL-KDD KDDTrain, UNSW- NB15	FSL

FS Techniques: Embedding: CNN, DNN

Balancing Techniques: Hybrid Sampling

Performance Measure: Accuracy, Precision, DR, FAR, F1-Score

Main Idea: Introduced an innovative intrusion detection method using FSL, specifically designed to address the scarcity of abnormal samples in network security datasets.

Contributions: IDS was constructed utilizing less than 1% of the NSL-KDD KDDTrainC dataset for training, the method achieves significantly higher accuracy compared to traditional models that use 20% of the training data.

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Conclusion: Proposed FSL-based intrusion detection method effectively addresses the challenge of sample scarcity and imbalance in network security datasets. Utilizing a balanced resampling method and advanced embedded feature selection techniques achieves a high accuracy of 92% and significantly improves detection rates for rare attack categories like R2L 75.93% and U2R 81.50%. **Limitations:** The effectiveness of FSL depends heavily on the quality and representativeness of the few samples used as support sets, which may not always capture the full variability of network attacks. Also, there is still room for improvement in detecting minority attacks.				
[97]	2020	N	UNSW-NB15	Multiscale CNN-LSTM
FS Techniques: Wrapper: GA **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, FAR, FNR **Main Idea:** Introduced a novel IDS leveraging a combined Multiscale CNN with LSTM (MSCNN-LSTM) model to enhance the accuracy of detecting network intrusions. **Contributions:** Integrated the MSCNN-LSTM model to enhance the detection capabilities of the IDS by processing both spatial and temporal data, going beyond what conventional neural networks offer. **Conclusion:** MSCNN-LSTM model exhibits significant improvements in handling high-dimensional and complex datasets, bypassing the need for traditional feature engineering techniques commonly used in IDS. It particularly excels in reducing the FAR to 0.9% for rare attacks like worms. **Limitations:** The integration of MSCNN and LSTM may lead to increased computational demands, potentially affecting deployment in resource-constrained environments.				
[51]	2021	N	NSL-KDD, CSE-CIC-IDS2018	RF, SVM, XGB, LSTM, AlexNet, Mini-VGGNet
FS Techniques: Not Used **Balancing Techniques:** Difficult Set Sampling Technique(DSSTE) **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Addressed the challenge of imbalanced network traffic in NIDS by introducing a novel DSSTE algorithm. **Contributions:** Introduced the DSSTE algorithm to handle class imbalance by compressing majority class samples and augmenting minority class samples in 'difficult' sets. **Conclusion:** DSSTE algorithm effectively addresses the imbalance in network traffic datasets, enabling more accurate classification of network intrusions. It enhances the learning focus on minority classes, which are typically harder to detect, thus improving the overall detection capabilities of NIDS, as demonstrated by an accuracy of 82.84%. **Limitations:** The approach's effectiveness is contingent on the correct initial segmentation into 'difficult' and 'easy' sets, which may not always capture the complexity of real-world data distributions. Also, there is a significant drop in the detection of infiltration attacks.				
[9]	2023	N	Kitsune Network Attack Dataset	LSTM
FS Techniques: Wrapper:Modified Equilibrium Optimization Algorithm (MEOA) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score, AUC **Main Idea:** Introduced the MEOA with DL-based DDoS Attack Classification (MEOADL-ADC) method tailored for 5G networks, employing advanced ML techniques to enhance the classification and detection of DDoS attacks effectively.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Developed the MEOADL-ADC technique integrating a MEOA for feature selection and an LSTM model for classification. Utilized the Tunicate Swarm Algorithm (TSA) for hyperparameter tuning of the LSTM model, demonstrating a novel approach to optimizing DL cybersecurity models. **Conclusion:** The MEOADL-ADC method offers an effective solution for addressing DDoS attacks in 5G networks by combining feature selection, LSTM classification, and sophisticated hyperparameter tuning and display an accuracy of 97.60%. **Limitations:** While the MEOADL-ADC method shows promising results, the computational intensity and complexity of the algorithms may limit their applicability in real-time scenarios without substantial hardware resources.				
[15]	2023	N	NSL-KDD	DBN, LSTM
FS Techniques: African Vulture Optimization (AVO) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Introduced an innovative intrusion detection strategy for smart grids that combines DL-based DBN-LSTM and AVO techniques to enhance cybersecurity. **Contributions:** Extracted a diverse set of features, including statistical measures and data relationships, followed by the implementation of the African Vulture Optimization Algorithm for feature selection. **Conclusion:** The proposed AVOA-DBN-LSTM method significantly improves the detection of cyber threats in smart grid systems, showcasing enhanced accuracy of 98.99%. **Limitations:** While the method shows high accuracy, the complexity of the DBN-LSTM model and the optimization algorithm may require substantial computational resources, potentially limiting real-time applications.				
[21]	2023	N	CTU-13, Malware Capture Facility Project (MCFP), CIC-AndMal2017	SVM, RF, XGB
FS Techniques: Filter: MI Based **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, Precision, Recall, F1-Score **Main Idea:** Proposed a comprehensive ML framework for detecting malicious network traffic, particularly encrypted traffic like HTTPS. It optimizes feature selection using MI to enhance detection accuracy and execution time. **Contributions:** Developed a framework incorporating protocol-agnostic and TLS/SSL-specific features to improve the accuracy of malicious traffic detection. Extensively evaluated the framework using multiple datasets. **Conclusion:** Uses ML to detect malicious traffic encrypted by protocols like HTTPS. The proposed model achieves low FPR while maintaining high detection accuracy across various datasets. **Limitations:** The real-world application of the model, particularly in systems with extensive access levels, may experience elevated operational costs due to an increase in false alarms.				
[30]	2023	N	NSLKDD	CNN
FS Techniques: Wrapper: Hyper Parallel Optimization (HPO) **Balancing Techniques:** Not Used **Performance Measure:** Accuracy, precision, Sensitivity, Specificity **Main Idea:** Introduced the Fully Streaming Big Data Framework (FSBDL) based on optimized DL for cybersecurity, incorporating HPO techniques utilizing Adam and RMSprop algorithms to enhance real-time intrusion detection.				

Appendix 1: Summary of Intrusion Detection Systems

Ref	Year	IoT Focused?	Dataset(s) Used	ML/DL Algorithms Employed
Contributions: Implemented parallel optimization techniques with Adam and RMSprop to enhance model accuracy, stability, and generalization. Introduced an optimized CNN specifically tailored to handle imbalanced NSL-KDD data and a user interface for better interaction and timely detection of network behaviors.				
Conclusion: The FSBDL achieves superior performance metrics over traditional methods with an accuracy of 99.94%, demonstrating the effectiveness of the proposed DL enhancements in real-time intrusion detection.				
Limitations: While the FSBDL shows high accuracy, its complexity and resource demands may limit deployment in resource-constrained environments.				

References

[1] Abdulameer, H., Musa, I., and Al-Sultani, N. (2023). Three level intrusion detection system based on conditional generative adversarial network. 13(2):2240–2258.

[2] Adefemi Alimi, K. O., Ouahada, K., Abu-Mahfouz, A. M., Rimer, S., and Alimi, O. A. (2022). Refined lstm based intrusion detection for denial-of-service attack in internet of things. *Journal of Sensor and Actuator Networks*, 11(3).

[3] Al-Daweri, M. S., Zainol Ariffin, K. A., Abdullah, S., and Md. Senan, M. F. E. (2020). An analysis of the kdd99 and unsw-nb15 datasets for the intrusion detection system. *Symmetry*, 12(10).

[4] Alajmi, M., Mengash, H. A., Alqahtani, H., Aljameel, S. S., Hamza, M. A., and Salama, A. S. (2023). Automated threat detection using flamingo search algorithm with optimal deep learning on cyber-physical system environment. *IEEE Access*, 11:127669–127678.

[5] Alazab, M., Awajan, A., Alazzam, H., Wedyan, M., Alshawi, B., and Alturki, R. (2024). A novel ids with a dynamic access control algorithm to detect and defend intrusion at iot nodes. *Sensors*, 24(7).

[6] Albulayhi, K., Abu Al-Haija, Q., Alsuhibany, S. A., Jillepalli, A. A., Ashrafuzzaman, M., and Sheldon, F. T. (2022). Iot intrusion detection using machine learning with a novel high performing feature selection method. *Applied Sciences*, 12(10).

[7] Aldhyani, T. H. H. and Alkahtani, H. (2022). Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. *Sensors*, 22(1).

[8] Alghamdi, M. I. (2022). A hybrid model for intrusion detection in iot applications. *Wireless Communications and Mobile Computing*, 2022(1):4553502.

[9] Aljebreen, M., Alrayes, F. S., Maray, M., Aljameel, S. S., Salama, A. S., and Motwakel, A. (2023). Modified equilibrium optimization algorithm with deep learning-based ddos attack classification in 5g networks. *IEEE Access*, 11:108561–108570.

[10] Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., and Razaque, A. (2020). Deep recurrent neural network for iot intrusion detection system. *Simulation Modelling Practice and Theory*, 101:102031. Modeling and Simulation of Fog Computing.

[11] Almuqren, L., Alqahtani, H., Aljameel, S. S., Salama, A. S., Yaseen, I., and Alneil, A. A. (2023). Hybrid metaheuristics with machine learning based botnet detection in cloud assisted internet of things environment. *IEEE Access*, 11:115668–115676.

[12] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., and Ming, H. (2019). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0305–0310.

[13] Alrowais, F., Althahabi, S., Alotaibi, S. S., Mohamed, A., Hamza, M. A., and Marzouk, R. (2023a). Automated machine learning enabled cybersecurity threat detection in internet of things environment. *Computer Systems Science and Engineering*, 45(1):687–700.

[14] Alrowais, F., Eltahir, M. M., Aljameel, S. S., Marzouk, R., Mohammed, G. P., and Salama, A. S. (2023b). Modeling of botnet detection using chaotic binary pelican optimization algorithm with deep learning on internet of things environment. *IEEE Access*, 11:130618–130626.

[15] Alsirhani, A., Mujib Alshahrani, M., Hassan, A. M., Taloba, A. I., Abd El-Aziz, R. M., and Samak, A. H. (2023). Implementation of african vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. *Alexandria Engineering Journal*, 79:105–115.

[16] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., and Burnap, P. (2019). A supervised intrusion detection system for smart home iot devices. *IEEE Internet of Things Journal*, 6(5):9042–9053.

[17] Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M., Abdelhaq, M., and Alsaqour, R. (2023). Iot empowered smart cybersecurity framework for intrusion detection in internet of drones. *Scientific Reports*, 13(1):18422.

[18] Ayoob Almotairi, Samer Atawneh, O. A. K. and Khafajah, N. M. (2024). Enhancing intrusion detection in iot networks using machine learning-based feature selection and ensemble models. *Systems Science & Control Engineering*, 12(1):2321381.

[19] Banaamah, A. M. and Ahmad, I. (2022). Intrusion detection in iot using deep learning. *Sensors*, 22(21).

[20] Basati, A. and Faghih, M. M. (2022). Dfe: efficient iot network intrusion detection using deep feature extraction. *Neural Computing and Applications*, 34(18):15175–15195.

[21] Bui, T., Duc, T., Linh Giang, N., Hien, N., Thanh, N., and Khanh, N. (2023). A machine learning-based framework for detecting malicious https traffic. In *Proceedings of the 12th International Symposium on Information and Communication Technology*, SOICT '23, page 769–776, New York, NY, USA. Association for Computing Machinery.

[22] Chaudhary, P. and Gupta, B. B. (2019). Ddos detection framework in resource constrained internet of things domain. In *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, pages 675–678.

[23] Dahou, A., Abd Elaziz, M., Chelloug, S. A., Awadallah, M. A., Al-Betar, M. A., Al-qaness, M. A. A., and Forestiero, A. (2022). Intrusion detection system for iot based on deep learning and modified reptile search algorithm. *Computational Intelligence and Neuroscience*, 2022(1):6473507.

[24] Dat-Thinh, N., Xuan-Ninh, H., and Kim-Hung, L. (2022). Midsiot: A multistage intrusion detection system for internet of things. *Wireless Communications and Mobile Computing*, 2022(1):9173291.

[25] EMEC, M. and OZCANHAN, M. H. (2022). A hybrid deep learning approach for intrusion detection in iot networks. *Advances in Electrical and Computer Engineering*, 22(1):3–12.

[26] Gad, A. R., Haggag, M., Nashat, A. A., and Barakat, T. M. (2022). A distributed intrusion detection system using machine learning for iot based on ton-iot dataset. *International Journal of Advanced Computer Science and Applications*, 13(6).

[27] Gupta, L., Salman, T., Ghubaish, A., Unal, D., Al-Ali, A. K., and Jain, R. (2022). Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach. *Applied Soft Computing*, 118:108439.

[28] Hasan, M., Islam, M. M., Zarif, M. I. I., and Hashem, M. (2019). Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. *Internet of Things*, 7:100059.

[29] Hazman, C., Guezzaz, A., Benkirane, S., and Azrour, M. (2024). Enhanced ids with deep learning for iot-based smart cities security. *Tsinghua Science and Technology*, 29(4):929–947.

[30] Hussen, N., Elghamrawy, S. M., Salem, M., and El-Desouky, A. I. (2023). A fully streaming big data framework for cyber security based on optimized deep learning algorithm. *IEEE Access*, 11:65675–65688.

[31] Huč, A. and Trček, D. (2021). Anomaly detection in iot networks: From architectures to machine learning transparency. *IEEE Access*, 9:60607–60616.

[32] Ioannou, C. and Vassiliou, V. (2019). Classifying security attacks in iot networks using supervised learning. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 652–658.

[33] Jiang, K., Wang, W., Wang, A., and Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, 8:32464–32476.

[34] Jithish, J., Alangot, B., Mahalingam, N., and Yeo, K. S. (2023). Distributed anomaly detection in smart grids: A federated learning-based approach. *IEEE Access*, 11:7157–7179.

[35] Karatas, G., Demir, O., and Sahingoz, O. K. (2020). Increasing the performance of machine learning-based idss on an imbalanced and up-to-date dataset. *IEEE Access*, 8:32150–32162.

[36] Karthikeyan, M., Manimegalai, D., and RajaGopal, K. (2024). Firefly algorithm based wsn-iot security enhancement with machine learning for intrusion detection. *Scientific Reports*, 14(1):231.

[37] Kasongo, S. M. and Sun, Y. (2020a). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security*, 92:101752.

[38] Kasongo, S. M. and Sun, Y. (2020b). A deep long short-term memory based classifier for wireless intrusion detection system. *ICT Express*, 6(2):98–103.

[39] Kasongo, S. M. and Sun, Y. (2020c). Performance analysis of intrusion detection systems using a feature selection method on the unsw-nb15 dataset. *Journal of Big Data*, 7(1):105.

[40] Kaushik, S., Bhardwaj, A., Alomari, A., Bharany, S., Alsirhani, A., and Mujib Alshahrani, M. (2022). Efficient, lightweight cyber intrusion detection system for iot ecosystems using mi2g algorithm. *Computers*, 11(10).

[41] Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., and Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, 61(12):9395–9409.

[42] Khammassi, C. and Krichen, S. (2020). A nsga2-lr wrapper approach for feature selection in network intrusion detection. *Computer Networks*, 172:107183.

[43] Kilichev, D., Turimov, D., and Kim, W. (2024). Next–generation intrusion detection for iot evcs: Integrating cnn, lstm, and gru models. *Mathematics*, 12(4).

[44] Kocher, G. and Kumar, G. (2021). Analysis of machine learning algorithms with feature selection for intrusion detection using unsw-nb15 dataset. 13(1):21–31.

[45] Kumar, P., Gupta, G. P., and Tripathi, R. (2021). Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks. *Arabian Journal for Science and Engineering*, 46(4):3749–3778.

[46] Lai, T., Farid, F., Bello, A., and Sabrina, F. (2024). Ensemble learning based anomaly detection for iot cybersecurity via bayesian hyperparameters sensitivity analysis. *Cybersecurity*, 7(1):44.

[47] Latif, S., Boulila, W., Koubaa, A., Zou, Z., and Ahmad, J. (2024). Dtl-ids: An optimized intrusion detection framework using deep transfer learning and genetic algorithm. *Journal of Network and Computer Applications*, 221:103784.

[48] Latif, S., Zou, Z., Idrees, Z., and Ahmad, J. (2020). A novel attack detection scheme for the industrial internet of things using a lightweight random neural network. *IEEE Access*, 8:89337–89350.

[49] Le, K.-H., Nguyen, M.-H., Tran, T.-D., and Tran, N.-D. (2022). Imids: An intelligent intrusion detection system against cyber threats in iot. *Electronics*, 11(4).

[50] Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., Zhao, Y., and Cui, L. (2020). Robust detection for network intrusion of industrial iot based on multi-cnn fusion. *Measurement*, 154:107450.

[51] Liu, L., Wang, P., Lin, J., and Liu, L. (2021). Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access*, 9:7550–7563.

[52] Lopez, M. M., Shao, S., Hariri, S., and Salehi, S. (2023). Machine learning for intrusion detection: Stream classification guided by clustering for sustainable security in iot. In *Proceedings of the Great Lakes Symposium on VLSI 2023*, GLSVLSI '23, page 691–696, New York, NY, USA. Association for Computing Machinery.

[53] Malathi, C. and Padmaja, I. N. (2023). Identification of cyber attacks using machine learning in smart iot networks. *Materials Today: Proceedings*, 80:2518–2523. SI:5 NANO 2021.

[54] Maslan, A., Mohamad, K. M. B., and Feresa, B. M. F. (2020). Feature selection for DDoS detection using classification machine learning techniques. *IAES International Journal of Artificial Intelligence (IJ-AI)*, 9(1):137–145.

[55] Moody Alhanaya, K. H. A. A.-S. (2023). Performance analysis of intrusion detection system in the iot environment using feature selection technique. *Intelligent Automation & Soft Computing*, 36(3):3709–3724.

[56] Morshedi, R., Matinkhah, S. M., and Sadeghi, M. T. (2024). Intrusion detection for iot network security with deep learning. *Journal of AI and Data Mining*, 12(1):37–55.

[57] Nguyen, X.-H., Nguyen, X.-D., Huynh, H.-H., and Le, K.-H. (2022). Realguard: A lightweight network intrusion detection system for iot gateways. *Sensors*, 22(2).

[58] Otoum, S., Kantarci, B., and Mouftah, H. T. (2019). On the feasibility of deep learning in sensor network intrusion detection. *IEEE Networking Letters*, 1(2):68–71.

[59] Otoum, Y., Liu, D., and Nayak, A. (2022). Dl-ids: a deep learning–based intrusion detection framework for securing iot. *Transactions on Emerging Telecommunications Technologies*, 33(3):e3803. e3803 ett.3803.

[60] Pantelakis, V., Bountakas, P., Farao, A., and Xenakis, C. (2023). Adversarial machine learning attacks on multiclass classification of iot network traffic. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA. Association for Computing Machinery.

[61] Patil, R., Dudeja, H., and Modi, C. (2019). Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Computers & Security*, 85:402–422.

[62] Polat, H., Polat, O., and Cetin, A. (2020). Detecting ddos attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability*, 12(3).

[63] Qureshi, A. S., Khan, A., Shamim, N., and Durad, M. H. (2020). Intrusion detection using deep sparse auto-encoder and self-taught learning. *Neural Computing and Applications*, 32(8):3135–3147.

[64] Raghuvanshi, A., Singh, U. K., Sajja, G. S., Pallathadka, H., Asenso, E., Kamal, M., Singh, A., and Phasinam, K. (2022). Intrusion detection using machine learning for risk mitigation in iot-enabled smart irrigation in smart farming. *Journal of Food Quality*, 2022(1):3955514.

[65] Rahman, M. A., Asyhari, A. T., Wen, O. W., Ajra, H., Ahmed, Y., and Anwar, F. (2021). Effective combining of feature selection techniques for machine learning-enabled iot intrusion detection. *Multimedia Tools and Applications*, 80(20):31381–31399.

[66] Rani, D., Gill, N. S., Gulia, P., and Chatterjee, J. M. (2022). An ensemble-based multiclass classifier for intrusion detection using internet of things. *Computational Intelligence and Neuroscience*, 2022(1):1668676.

[67] Rezvy, S., Luo, Y., Petridis, M., Lasebae, A., and Zebin, T. (2019). An efficient deep learning model for intrusion classification and prediction in 5g and iot networks. In *2019 53rd Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6.

[68] Riyaz, B. and Ganapathy, S. (2020). A deep learning approach for effective intrusion detection in wireless networks using cnn. *Soft Computing*, 24(22):17265–17278.

[69] Roopak, M., Tian, G. Y., and Chambers, J. (2020). An intrusion detection system against ddos attacks in iot networks. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0562–0567.

[70] Roopak, M., Tian, G.-Y., and Chambers, J. A. (2019). Deep learning models for cyber security in iot networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0452–0457.

[71] Saraeian, S. and Golchi, M. M. (2020). Application of deep learning technique in an intrusion detection system. *International Journal of Computational Intelligence and Applications*, 19(02):2050016.

[72] Sarker, I. H., Abushark, Y. B., Alsolami, F., and Khan, A. I. (2020). Intrudtree: A machine learning based cyber security intrusion detection model. *Symmetry*, 12(5).

[73] Sarwar, A., Alnajim, A. M., Marwat, S. N. K., Ahmed, S., Alyahya, S., and Khan, W. U. (2022). Enhanced anomaly detection system for iot based on improved dynamic sbpso. *Sensors*, 22(13).

[74] Sarwar, N., Bajwa, I. S., Hussain, M. Z., Ibrahim, M., and Saleem, K. (2023). Iot network anomaly detection in smart homes using machine learning. *IEEE Access*, 11:119462–119480.

[75] Shafiq, M., Tian, Z., Sun, Y., Du, X., and Guizani, M. (2020). Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city. *Future Generation Computer Systems*, 107:433–442.

[76] Shtayat, M. M., Hasan, M. K., Sulaiman, R., Islam, S., and Khan, A. U. R. (2023). An explainable ensemble deep learning approach for intrusion detection in industrial internet of things. *IEEE Access*, 11:115047–115061.

[77] Soe, Y. N., Santosa, P. I., and Hartanto, R. (2019). Ddos attack detection based on simple ann with smote for iot environment. In *2019 Fourth International Conference on Informatics and Computing (ICIC)*, pages 1–5.

[78] Song, H. M., Woo, J., and Kim, H. K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, 21:100198.

[79] Sun, Z., An, G., Yang, Y., and Liu, Y. (2024). Optimized machine learning enabled intrusion detection 2 system for internet of medical things. *Franklin Open*, 6:100056.

[80] Taher, K. A., Mohammed Yasin Jisan, B., and Rahman, M. M. (2019). Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, pages 643–646.

[81] Ullah, I. and Mahmoud, Q. H. (2021). A framework for anomaly detection in iot networks using conditional generative adversarial networks. *IEEE Access*, 9:165907–165931.

[82] Ullah, S., Ahmad, J., Khan, M. A., Alkhammash, E. H., Hadjouni, M., Ghadi, Y. Y., Saeed, F., and Pitropakis, N. (2022). A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering. *Sensors*, 22(10).

[83] Usoh, M., Asuquo, P., Ozuomba, S., Stephen, B., and Inyang, U. (2023). A hybrid machine learning model for detecting cybersecurity threats in iot applications. *International Journal of Information Technology*, 15(6):3359–3370.

[84] Verma, A. and Ranga, V. (2020). Machine learning based intrusion detection systems for iot applications. *Wireless Personal Communications*, 111(4):2287–2310.

[85] Vishwakarma, M. and Kesswani, N. (2022). Dids: A deep neural network based real-time intrusion detection system for iot. *Decision Analytics Journal*, 5:100142.

[86] Wirawan Muhammad, A., Feresa Mohd Foozy, C., , and Azhari, A. (2020). Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection. *International Journal Of Artificial Intelligence Research*, 4(1):1–8.

[87] Woo, J., Song, J.-Y., and Choi, Y.-J. (2019). Performance enhancement of deep neural network using feature selection and preprocessing for intrusion detection. *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 415–417.

[88] Xu, X., Li, J., Yang, Y., and Shen, F. (2021). Toward effective intrusion detection using log-cosh conditional variational autoencoder. *IEEE Internet of Things Journal*, 8(8):6187–6196.

[89] Yang, Y., Zheng, K., Wu, B., Yang, Y., and Wang, X. (2020). Network intrusion detection based on supervised adversarial variational auto-encoder with regularization. *IEEE Access*, 8:42169–42184.

[90] Yang, Y., Zheng, K., Wu, C., Niu, X., and Yang, Y. (2019a). Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks. *Applied Sciences*, 9(2).

[91] Yang, Y., Zheng, K., Wu, C., and Yang, Y. (2019b). Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network. *Sensors*, 19(11).

[92] Yaras, S. and Dener, M. (2024). Iot-based intrusion detection system using new hybrid deep learning algorithm. *Electronics*, 13(6).

[93] Yu, Y. and Bian, N. (2020). An intrusion detection method using few-shot learning. *IEEE Access*, 8:49730–49740.

[94] Zakariyya, I., Kalutarage, H., and Al-Kadri, M. O. (2023). Towards a robust, effective and resource efficient machine learning technique for iot security monitoring. *Computers & Security*, 133:103388.

[95] Zeng, Y., Qiu, M., Zhu, D., Xue, Z., Xiong, J., and Liu, M. (2019). Deepvcm: A deep learning based intrusion detection method in vanet. In *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 288–293.

[96] Zhang, H., Huang, L., Wu, C. Q., and Li, Z. (2020a). An effective convolutional neural network based on smote and gaussian mixture model for intrusion detection in imbalanced dataset. *Computer Networks*, 177:107315.

[97] Zhang, J., Ling, Y., Fu, X., Yang, X., Xiong, G., and Zhang, R. (2020b). Model of the intrusion detection system based on the integration of spatial-temporal features. *Computers & Security*, 89:101681.

[98] Zhang, Y., Li, P., and Wang, X. (2019). Intrusion detection for iot based on improved genetic algorithm and deep belief network. *IEEE Access*, 7:31711–31722.

Appendix 2: Detailed Summary of Acronyms Used in the Study

Acronym	Definition
AE	Auto Encoder
AI	Artificial Intelligence
AIDS	Anomaly-based Intrusion Detection System
ANN	Artificial Neural Network
AOA	Arithmetical Optimization Algorithm
AUC	Area Under the ROC Curve
AVO	African Vulture Optimization
BBA	Binary Bat Algorithm
BiLSTM	Bidirectional Long Short-Term Memory
BIRCH	Balanced Iterative Reducing and Clustering using Hierarchies
BN	Bayesian Networks
BPNN	Back Propagation Neural Network
CAN	Controller Area Network
CART	Classification and Regression Tree
CBOA	Chaotic Butterfly Optimization Algorithm
CBPOA	Chaotic Binary Pelican Optimization Algorithm
CFA	Cuttlefish Algorithm
CFNN	Cascade Forward Neural Network
CGAN	Conditional Generative Adversarial Network
CNN	Convolutional Neural Network
CPS	Cyber-physical Systems
CVAE	Convolutional Variational Auto Encoders
DBN	Deep Belief Network
DCNN	Deep Convolutional Neural Network
DDoS	Distributed Denial of Service
DL	Deep Learning
DLSTM	Deep Long Short-term Memory
DNN	Deep Neural Network
DoS	Denial of Service
DR	Detection Rate
DSSTE	Difficult Set Sampling Technique
DT	Decision Tree
DTL	Deep Transfer Learning
D-CFA	Discrete variant of the Cuttlefish Algorithm
ETC	Extra Tree Classifier
FAR	False Alarm Rate
FFO	Firefly Optimization
FPR	False Positive Rate
GA	Genetic Algorithm
GAN	Generative Adversarial Network
GBM	Gradient Boosting Machine

Continued on next page

Acronym	Definition
GR	Gain Ratio
GRU	Gated Recurrent Unit
HIDS	Host-based Intrusion Detection System
HPO	Hyper Parallel Optimization
IDS	Intrusion Detection System
IDSBPSO	Improved Dynamic Sticky Binary Particle Swarm Optimization
IG	Information Gain
IIoT	Industrial Internet of Things
IoT	Internet of Things
kNN	k-Nearest Neighbours
LDA	Linear Discriminant Analysis
LGBM	Light Gradient Boosting Machine
LR	Logistic Regression
LSTM	Long Short-term Memory
MCC	Matthews Correlation Coefficient
MDPCA	Modified Density Peak Clustering
MEOA	Modified Equilibrium Optimization Algorithm
MESNN	Modified Elman Spike Neural Network
MFO	Mayfly Optimization
MI	Mutual Information
ML	Machine Learning
MLP	Multi-Layer Perceptron
MRFO	Modified Red Fox Optimizer
NB	Naïve Bayes
NIDS	Network-based Intrusion Detection System
NSGA	Non-dominated Sorting Genetic Algorithm
PHICAD	Probabilistic Hierarchical Intrusion Correlation and Detection
PO	Political Optimization
PSO	Particle Swarm Optimization
QDA	Quadratic Discriminant Analysis
RaNN	Random Neural Network
RBF	Radial Basis Function
RBM	Restricted Boltzmann Machine
REDNN	Resource Efficient Deep Neural Network
REFDNN	Resource Efficient Federated Deep Neural Network
RELM	Regularized Extreme Learning Machine
RF	Random Forest
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic Curve
RSA	Reptile Search Algorithm
RT	Random Trees
SAVER	Supervised Variational Auto Encoders
SDN	Software Defined Networks

Continued on next page

Acronym	Definition
SDPN	Stacked-Deep Polynomial Network
SGD	Stochastic Gradient Descent
SLR	Systematic Literature Review
SMA	Slime Mold Algorithm
SMO	Spider Monkey Optimization
SMOTE	Synthetic Minority Over-sampling Technique
SVM	Support Vector Machines
TPR	True Positive Rate
TSA	Tunicate Swarm Algorithm
VANET	Vehicular Ad-hoc Network
WSN	Wireless Sensor Network
XGB	Extreme Gradient Boosting