Table1: Machine Learning Methods for IDS

Source# 1 & Reference	Roy & Cheung (2018). A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network. IEEE
Type of Learning	DL
Attack	Network attacks (the Sinkhole attack, Denial-of-Service attacks, Man-in-the-Middle (MiM) attacks, etc) targeting the network layer of IOT
Detection Mechanism	BLSTM RNN intrusion detection Model, implemented using the Python program language, Google Tensor Flow and Keras.
Method	DL (to build an IDS for IoT using the Bi-directional Long Short-Term Memory Recurrent Neural Networks (BLSTM RNN) approach)
Dataset	reduced dataset of the novel benchmark data set: UNSWNB15 for training and Testing
Evaluation Parameters	Precision, Recall, f-1 score and FAR
Pros	Ability to distinguish abnormal traffic from normal traffic of IOT + ability to detect 5 types of security attacks that an IoT network may encounter +comprehensive data set used (45 features)
Cons	Reduced data set was used + Binary classification attack only (attack or normal) so not a multiclass classification for attack types.
Relevance	9/10 -Although not a reinforced learning, very relevant due to BIG data
Achievement and contribution	Long Short-Term Memory Recurrent Neural Network (BLSTM RNN) is highly efficient for building high accuracy intrusion detection model and offers a novel research methodology.
Accuracy	95%
Future work	More experiments to further analyse the proposed model using large data sets, especially data sets containing dedicated IoT. Improve detection accuracy and the trade-offs between detection parameters.

Table1: Machine Learning Methods for IDS

Source# 2 & Reference	Vinayakumar et al (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE
Type of Learning	DLm
Attack	**CICIDS2017 & WSN-DS dataset:** The various attacks injected were Brute Force FTP, Brute Force SSH, 'DoS(Blackhole, Grayhole, Flooding, and Scheduling)Heartbleed, Web Attack, In_ltration, Botnet and 'DDoS. **UNSW-NB15 data set:** Fuzzers ,analysis,backdooors, Exploits,DoS,Geneeric,Reconnaissance,shellcode and worms **ADFA**-LD:adduser,java-meterpreter,Hydra-FTP,Hydra-SSH,Webshel
Detection Mechanism	Hybrid intrusion detection alert system using a highly scalable IDS framework(SHIA) on commodity hardware server which has the capability to analyse the network and host-level activities
Method	Hyper parameter selection methods.
Dataset	KDDCup 99 dataset + NSL-KDD, UNSW-NB15, Kyoto, WSN-DS, and CICIDS 2017,
Evaluation Parameters	Accuracy, Precision, , F-1 score, True Positive rate (TPR) or Recall ,False Positive Rate(FPR) and Receiver Operating Characteristics (ROC) curve
Pros	Collected host-based and network-based features in real-time in a distributed manner using DNNs + Included both Binary and multiclass classification for attack types
Cons	Due to extensive computational cost associated with complex DNNs architectures, they were not trained in this research using the benchmark IDS datasets. Due to the confidential nature of the research, the scalable framework details could not be disclosed
Relevance	**9/10** IDS & DL covered extensively
Achievement and contribution	proposed a highly scalable and hybrid DNNs framework called scale-hybrid-IDS-AlertNet (SHIA)which can be used in real-time to effectively monitor the network traffic and host-level events to proactively alert possible cyber attacks. + Comparative experimentation using various benchmark datasets
Accuracy	95-99% for KDDCup 99 and NSLKDD +65-75% for UNSW-NB15 and WSN-DS
Future work	performance can be further improved by training complex DNNs architectures on advanced hardware through distributed approach e.g. adding a module for monitoring the DNS and BGP events in the networks

Table1: Machine Learning Methods for IDS

Source# 3 & Reference	HaddadPajouh et al (2018). A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting.
Type of Learning	DL
Attack	Malware attack
Detection Mechanism	n-gram technique to detect metamorphic malicious malware
Method	Use RNN DL to analyse ARM-based IoT applications' execution operation codes (OpCodes).
Dataset	Collected ARM based IoT application dataset comprising 281 malware and 270 benign ware.
Evaluation Parameters	Accuracy, True Positive rate (TP), False Positive Rate(FP) FN ad TN in relationship to Depth, bidirectional, Number of neurons, dropout rate, epochs, window size, batch size, weight and regularization.)
Pros	Ability to mine own data set
Cons	The dataset we used is small in comparison to the real-world cyber threats
Relevance	7/10
Achievement and contribution	achieved a detection accuracy of 98% against IoT malware not used in the training. AND the finding that ''add'' OpCode is most frequently found in both malware and normal applications. This Opcode along with ''xor, mov, sub and pop'' have a high frequency pattern in our dataset samples
Accuracy	98%
Future work	implementing the proposed approach in a real-world environment and evaluating its effectiveness in identifying both known malware and new malware.+ explore and design DL approach for increasing speed, accuracy and scalability of IOT malware detection

Source# 4 & Reference	Zhao, et al. (2017). Intrusion detection using deep belief network and probabilistic neural network. In *2017 IEEE*. 1, pp. 639-642). IEEE.
Type of Learning	DL
Attack	DoS, R2L, and U2R
Detection Mechanism	DBN using PNN
Method	DL (DBN and PNN))
Dataset	KDD CUP 99
Evaluation Parameters	Precision, Detection accuracy, Detection rate. false alarm rate (FAR)
Pros	detection rate is the highest, and the detection time is shorter than that the network without reducing the dimension
Cons	deficiencies in the KDDCUP'99 dataset
Relevance	**7/10**
Achievement and contribution	The experiment result shows that the method performs better than the traditional PNN, PCA-PNN and unoptimized DBN-PNN.
Accuracy	99.14%
Future work	Therefore, the next step is to apply the method to the real network, through the feedback in the network to improve the method

Table1: Machine Learning Methods for IDS

Source# 5 Reference	Alrawashdeh, K., & Purdy, C. (2016, December). Toward an online anomaly intrusion detection system based on deep learning. In *2016 15th IEEE*
Type of Learning	DL
Attack	DoS, Probe, R2L, and U2R
Detection Mechanism	DL using RBM
Method	RBM and LR-DBN (Logistic Regression Deep Belief Networks) learning method
Dataset	10% KDD CUP 99
Evaluation Parameters	Accuracy, FAR
Pros	results produced a low false negative result of 2.48% and a true positive of 97.5%
Cons	deficiencies in the KDDCUP'99 dataset
Relevance	**8/10**
Achievement and contribution	Presents machine learning approaches for predicting attacks with a reasonable challenge. able to produce a low false negative rate of 2.47%
Accuracy	97.9%
Future work	Applying our machine learning strategy to larger and more challenging datasets, which include larger classes of attacks.

Source# 6 Reference	Yin, et al (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE*.
Type of Learning	DL
Attack	DoS U2R R2L Probe
Detection Mechanism	Not explicitly stated
Method	recurrent neural networks (RNN-IDS by using most current and broadest deep learning frameworks - Theano
Dataset	NSL -KDD
Evaluation Parameters	Accuracy, Precision , Detection Rate(DR) TPR, FPR
Pros	higher accuracy rate and detection rate with a low false positive rate, especially under the task of multiclass classification on the NSL-KDD dataset
Cons	deficiencies in the KDD dataset
Relevance	**8/10**
Achievement and contribution	RNN-IDS model performance is superior to that of traditional machine learning classification methods in both binary and multiclass classification + provides a new research method for intrusion detection.
Accuracy	83.28%
Future work	to reduce the training time using GPU acceleration, avoid exploding and vanishing gradients, and study the classification performance of LSTM, Bidirectional RNNs algorithm in the field of intrusion detection

Table1: Machine Learning Methods for IDS

Source# 7 Reference	Wang et al (2017, July). End-to-end encrypted traffic classification with one-dimensional convolution neural networks. *IEEE*
Type of Learning	DL
Attack	Not explicitly stated
Detection Mechanism	one-dimensional convolution neural networks.
Method	end-to-end encrypted traffic classification method
Dataset	ISCX VPN-nonVPN traffic dataset
Evaluation Parameters	Accuracy, Precision F1-score
Pros	CNN is proposed to minimize the data pre-processing requirements
Cons	The 1D-CNN performance of_non-VPN services is not very good. The precision is only 85.5% and 85.8%; the recall rate is only 85.8% and 85.9%.
Relevance	7/10
Achievement and contribution	First time to apply an end-to-end method to the encrypted traffic classification domain.
Accuracy	97.3%
Future work	Because different classes of traffic have different types of packets, the more appropriate byte number needs to be further studied. to study how to improve the 1D-CNN performance when training data is imbalanced. the experiment results show that Non-VPN traffic has relatively worse performance. We plan to analyse the detail reason and make corresponding improvement.

Source# 8 Reference	Huang 2018- Towards Experienced Anomaly Detector through Reinforcement Learning
Type of Learning	DRL
Attack	Not explicitly stated
Detection Mechanism	Reinforcement Learning (RL)
Method	RNN(using LSTM and Q learning)
Dataset	Yahoo benchmark datasets (Laptev, Amizadeh, and Flint 2015) which includes 367 labelled time series.
Evaluation Parameters	The learning rate, outcome value also referred to as the reward value.
Pros	1) No assumption about the underlying mechanism of anomaly patterns, 2) refrains from the cumbersome work of threshold setting for good anomaly detection performance under specific scenarios, and 3) keeps evolving with the growth of anomaly detection experience.
Cons	None
Relevance	9/10
Achievement and contribution	Initial promising results of +it is expected that the anomaly detector keeps evolving and is able to perform nicely in general and unseen anomaly detection problems.
Accuracy	approximate 100%
Future work	To extend the applicability of the method, the problem of generating accurately labelled time-series datasets of various types for anomaly detection training is considered

Table1: Machine Learning Methods for IDS

Source# 9 Reference	Tang et al (2018). Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks.IEEE
Type of Learning	DL
Attack	ZERO day attack
Detection Mechanism	Gated Recurrent Unit Recurrent Neural Network (GRU-RNN)
Method	DL
Dataset	NSL-KDD (Reduced redundant and sampled)
Evaluation Parameters	Precision (P), Recall (R), F-measure (F) and accuracy (ACC)
Pros	Uses a minimum number of features compared to other state-of-the-art approaches. + GRU-RNN does not deteriorate the network performance.
Cons	None stated
Relevance	7/10
Achievement and contribution	1) This is the first attempt to use GRU-RNN for an IDS in the SDN environment. 2) approach is significantly potential for real time detection
Accuracy	89%
Future work	Optimize our model and use other features to increase the accuracy. We will also try to implement our approach in a distributed manner to reduce the overhead on the controller

Source# 10 Reference	Yan et al (2018). A Comparative Study of Off-Line Deep Learning Based Network Intrusion Detection.IEEE
Type of Learning	DL
Attack	DoS, Probe, U2R and R2L
Detection Mechanism	multiple advanced deep learning models (SVM,MLP,RBM,SAE,WnD)
Method	DL (off-line deep learning based NIDSes)
Dataset	(NSL-KDD + UNSW-NB15 datasets
Evaluation Parameters	Accuracy, Precision and Recall
Pros	Reputable data set used
Cons	None stated
Relevance	8/10
Achievement and contribution	Sparce autoencoder achieves accuracy similar to the existing machine learning solutions; for the NSW-NB15 dataset+ deep neural network models with greater generalization capability deliver better accuracy than SVM based solutions.
Accuracy	UNSW-NB15 : A recall of 99.5, 99.0, 97.8, 98.7 & 99.4 for SVM ,MLP,RBM, SAE, and WhD respectively
Future work	Not stated

Table1: Machine Learning Methods for IDS

Source# 11 Reference	De La Bourdonnaye et al (2017). Learning of Binocular Fixations using Anomaly DS with D-RL. HAL achieves-ouvertes
Type of Learning	**D-RL**
Attack	N/a
Detection Mechanism	convolutional autoencoders
Method	Reward noise removal method
Dataset	sensor data
Evaluation Parameters	Rewards
Pros	Learn binocular fixations without such prior information.
Cons	1) The environment cannot vary during learning. Otherwise, the autoencoder must be adapted (this task is difficult since during learning, the object is in the environment). 2) _ The method works in a rather simple setting and has not been adapted yet to a cluttered environment with many objects.
Relevance	7/10
Achievement and contribution	showing that the environment encoding step can replace the prior information
Accuracy	Not stated
Future work	1) Make the auto encoder adaptive to increase the systems robustness. 2) To validate the method on a physical robot learning in the real world. 3) To adapt our method to other types of task such as object reaching or grasping.

Source# 12 Reference	Kotenko et al (2018). Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning. IEEE
Type of Learning	**ML**
Attack	smart meter energy consumption profiling and surveillance camera robbery,
Detection Mechanism	Support vector machine k-nearest neighbours' method, Gaussian naïve Bayes, artificial neural network and decision tree.
Method	A multi-level scheme for combining the classifiers was used for carrying out the experiments
Dataset	"Detection_of_IoT_botnet_attacks_N_BaIoT" dataset
Evaluation Parameters	Accuracy (ACC), TPR and FPR
Pros	None stated
Cons	None stated
Relevance	7/10
Achievement and contribution	The offered framework provides the gain in information processing productivity and the higher accuracy of detection of attacks.
Accuracy	Table 1 Presents various comparison values SVM, k-NN, GNB, ANN, DT PV, WV, SV and classifiers used
Future work	Examine and experimentally investigate other methods of machine learning for the detection of anomalies, such as dynamic Bayesian networks (DBNs) and deep learning neural networks (DLNNs). + developed framework in the environment of the special software such as Hadoop and Spark

Table1: Machine Learning Methods for IDS

Source# 13 Reference	Torres, et al (2016, June). An analysis of recurrent neural networks for botnet detection behaviour. In *2016 IEEE*
Type of Learning	DL
Attack	Botnet, SMTP-SPAM-Attempts
Detection Mechanism	LSTM Detection Model
Method	RNN
Dataset	2 different datasets coming from network traffic captures taken from CVUT university campus networks. Both datasets are publicly available as part of the Malware Capture Facility Project (MCFP) + BOTNET and normal traffic captured by MCFP
Evaluation Parameters	Attack Detection rate (ADR) and FAR
Pros	The way information is represented to LSTM was not efficient (So as to help could help in differentiating traffic behaviours)
Cons	LSTM model has, however, failed to correctly identify most of the HTTP and HTTPS traffic as well as some of the traffic labelled as Established including SMTP-Established- SPAM.
Relevance	7/10
Achievement and contribution	RNN is capable of classifying the traffic with a high attack detection rate and an very small false alarm rate,
Accuracy	99.9%
Future work	Analysing with more details other possible solutions regarding the per-connection imbalance situations

Source# 14 Reference	Hansen et al (2019).Fast deep reinforcement learning using online adjustment from the past. In *Advances in Neural Information Processing Systems* (pp. 10567-10577).
Type of Learning	**DRL**
Attack	N/A
Detection Mechanism	Ephemeral Value Adjustments (EVA)
Method	Convolutional Neural networks
Dataset	N/A but 55 Atari games were used
Evaluation Parameters	Awards, learning rate and other Atari hyper parameters
Pros	EVA improves the overall rate of learning.
Cons	None stated
Relevance	7/10
Achievement and contribution	Show that EVA is performant on a demonstration task and Atari games.
Accuracy	N/A
Future work	Showing the complementary effects of EVA with other algorithms.

Table1: Machine Learning Methods for IDS

Source# 15 Reference	15 Mc Elwee et al (2017). Deep Learning for prioritizing and responding to IDS alerts. IEEE
Type of Learning	DL
Attack	Network attacks
Detection Mechanism	Federated Analysis Security Triage Tool prototype. (FASTT**),a** network-based IDS
Method	Using the DNN classifier implemented using Tensor-floor. Presented with Pandas Data Frame + Hidden layer used (ReLU) transfer function + The output layer made use of a softmax function and six output neurons, (= six labels in the training data) + adaptive moment estimation (Adam) was used to train the neural network. Xavier Algorithm for Weight initialization + feature vector optimization using feature ranking algorithm for Tensor Flow
Dataset	Training data was created by retrieving alert data from representative categories and subcategories of alerts from McAfee Network Security Platform (NSP). Evaluation data was created using the same approach, but without the labels, and was applied directly to the DNN classifier to evaluate the accuracy
Evaluation Parameters	DNN classifier accuracy
Pros	Generated own data
Cons	human analyst review
Relevance	9/10
Achievement and contribution	1) a significant time-saving value in applying ML to the initial triage of security alerts received from an IDS – (up to a 70% increase in productivity for elimination of previously known alerts/events. 2) transferring security alerts to an intermediate system for indexing and visualization is valuable to security analysts (prioritize alerts.) 3- FASTT prototype demonstrates the value of semi-automated report generation for threat information sharing.
Accuracy	98%
Future work	1) User feedback can be incorporated into the user interface to allow analysts to change the triage category for security alerts and allow the DNN classifier to use this feedback during the next model training cycle. 2) speed up the human analyst review and will complement the automated triage of events through clustering following the initial triage classification

Source# 16 Reference	Dong and Wang (2016). Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection. IEEE
Type of Learning	DL
Attack	DOS, U2R, R2L, Probing
Detection Mechanism	Support Vector Machine (SVM) and restricted Boltzmann machine (RBM).
Method	SVM-RBMs learning method to classify normal traffic- with and without SMOTE for precision Comparison)
Dataset	KDD-99
Evaluation Parameters	*Precision+ Recall*
Pros	None stated
Cons	The system faces certain limitations that include sanctity of data used to generate inputs and outputs. + demand for faster and efficient data assessment.
Relevance	8/10
Achievement and contribution	The system has enabled the exhaustive and conclusive assessment of network security e.g. able to analyse big set of data, uses data pattern to detect problem (difficult for human)', provide accurate information on abnormal behaviour from the start.

Table1: Machine Learning Methods for IDS

Accuracy	Not specified
Future work	Not stated

Source# 17 Reference	Van Hasselt et al (2015). Deep Reinforced Learning with Double Q-Learning. GOOGLE DEEPMIND
Type of Learning	D-RL
Attack	N/A
Detection Mechanism	Double Deep Q-Learning Networks DQN
Method	DQN using convolution network
Dataset	Dataset 49 Atari games
Evaluation Parameters	*CNN Network Parameter* (Weights), *Performance, And Rewards*
Pros	leads to much higher scores on several games
Cons	None stated
Relevance	8/10
Achievement and contribution	shown why Q-learning can be overoptimistic in large-scale problem ,+ shown that these overestimations are more common and severe in practice than previously acknowledged + Double Q-learning can be used at scale to successfully reduce this over optimism, resulting in more stable and reliable learning.+ proposed a specific implementation called Double DQN, that uses the existing architecture and deep neural network of the DQN algorithm without requiring additional networks or parameter + Double DQN finds better policies, obtaining new state-of-the-art results on the Atari 2600 domain.
Accuracy	Performance (MEDIAN) No ops: DQN=93.5 % V s double DQN=114.7% while Random start (DQN =56.6 and Double DQN= 86.9). MEAN 241.1% VS 330.3% & 146.0% VS 883.3% for No ops and random starts respectively
Future work	None stated

Source# 18 Reference	Zambaldi et al (2019). Deep RL with Relational Inductive Biases. Published as a conference paper at ICLR. DeepMind, London.UK
Type of Learning	D-RL
Attack	n/a
Detection Mechanism	StarCraft II Mini games
Method	structured perception and relational reasoning into deep RL architectures
Dataset	n/a
Evaluation Parameters	Hyper parameter across mini-games such as Learning Rate, Entropy loss scaling, Number of blocks and heads
Pros	this approach can offer advantages in efficiency, generalization, and interpretability
Cons	None stated
Relevance	8/10

Table1: Machine Learning Methods for IDS

Achievement and contribution	to introduce techniques for representing and reasoning about states in model-free deep reinforcement learning agents via relational inductive biases
Accuracy	Not explicitly stated
Future work	Scale up to meet some of the most challenging test environments in modern artificial intelligence. + exploring perceiving complex scenes via more structured formats, such as scene graphs

Source# 19 Reference	Nair et al (2015). Massively Parallel Methods for Deep Reinforcement Learning *rXiv preprint arXiv:1507.04296*.
Type of Learning	D-RL
Attack	Massively distributed architecture for D-RL made up of parallel actors that generate new behaviour; parallel learners that are trained from stored experience; a distributed neural network (DQN) to represent the value function or behaviour policy; and a distributed store of experience.
Detection Mechanism	N/A
Method	Evaluate 49 Atari games using Gorila (General RL Architecture) DQN
Dataset	49 games from Atari 2600 games from the Arcade Learning Environment,
Evaluation Parameters	Parameter Rewards (change in score)
Pros	Parallel parameter server and actors
Cons	None stated
Relevance	8/10
Achievement and contribution	Outperformed single GPU DQN on 41 games, outperformed human professional on 25 games.10times faster than non. distributes version
Accuracy	N/A But Gorila DQN significantly outperformed single GPU DQN on 41 out of 49 games
Future work	None stated

Table1: Machine Learning Methods for IDS

Source# 20 Reference	Van Hasselt et al (2018) .Deep Reinforcement Learning and the Deadly Triad. *Cornell,New York*
Type of Learning	D-RL
Attack	Q-Learning
Detection Mechanism	N/A
Method	Variety of experiments using the Atari Learning Environment (Bellemare et al., 2013) using variants of DQN (Mnih et al., 2015).
Dataset	Not specified but were applied to 57 different Atari games
Evaluation Parameters	Bootstrap targets, number of steps before bootstrapping, prioritisation & Network sizes
Pros	Moderation of overestimation biases and instabilities + early performance can be boosted
Cons	alternatives to the basic Qlearning updates do not, however, fully resolve the issues caused by the deadly triad
Relevance	8/10
Achievement and contribution	Tackled Deadly triad of function approximation, bootstrapping, and off-policy learning
Accuracy	N/A
Future work	General learning dynamics and interactions between (soft)-divergence and control performance could benefit from further study.

Source# 21 Reference	Foerster, J., Assael, I. A., de Freitas, N., & Whiteson, S. (2016). Learning to communicate with deep multi-agent reinforcement learning. In *Advances in Neural Information Processing Systems* (pp. 2137-2145).
Type of Learning	D-RL
Attack	N/A
Detection Mechanism	Reinforced Inter-Agent Learning (RIAL) and Differentiable Inter-Agent Learning (DIAL)
Method	Q-learning and back propagate error derivatives through (noisy) communication channels.
Dataset	Deep networks
Evaluation Parameters	Rewards ,Learning rate and discount factor
Pros	demonstrate end-to-end learning of protocols in complex environments inspired by communication riddles and multi-agent computer vision problems with partial observability.
Cons	n/a
Relevance	7/10
Achievement and contribution	First attempt at learning communication and language with deep learning approaches.
Accuracy	n/a
Future work	The gargantuan task of understanding communication and language in their full splendour, covering compositionality, concept lifting, conversational agents, and many other important problems still lies ahead

Table1: Machine Learning Methods for IDS

Source# 22 **Reference**	Deverett, B., Faulkner, R., Fortunato, M., Wayne, G., & Leibo, J. Z. (2019). Interval timing in deep reinforcement learning agents. *arXiv preprint arXiv:1905.13469*.
Type of Learning	D-RL
Attack	time perception
Detection Mechanism	Interval Timing
Method	Deep Neural network using Recurrent (LSTM)
Dataset	Psych lab Frame input
Evaluation Parameters	Reward ,temporal measurements(interval timing), sample interval" delay
Pros	Non stated
Cons	Non stated
Relevance	7/10
Achievement and contribution	Found that both recurrent and feedforward agents could solve the task in an end-to-end manner. + open-sourcing apart from open-sourcing,other timing tasks that are commonly used in the animal literature, such as temporal production (15) and temporal discrimination
Accuracy	Near perfect accuracy
Future work	explore the ways in which different environmental and agent architectural constraints alter the solutions of the agent + 2 other future works from the article

Table1: Machine Learning Methods for IDS

Source# 23 **Reference**	Abeshu & Chilamkurt(2018). Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. IEEE
Type of Learning	DL
Attack	Primarily R2U, and R2U (These attacks constitute a major category of attacks on fog-to-things interaction as most of the IoT devices are accessed remotely for updates and management)
Detection Mechanism	distributed deep-learning-driven fog-to-things computing attack detection scheme
Method	A pretrained stacked autoencoder has been employed in feature engineering, while softmax was used for classification
Dataset	publicly available NSL-KDD dataset
Evaluation Parameters	accuracy, detection rate (DR), false alarm rate (FAR), ROC curve, and scalability
Pros	deep models used are superior to shallow models in detection accuracy, false alarm rate, and scalability
Cons	None stated
Relevance	9/10
Achievement and contribution	conclude that training attack detection systems using deep learning models on distributed IoT networks supported by fog nodes could improve the accuracy and efficiency of cyber-attack detection as sharing the parameter updates avoids local minima at each node
Accuracy	99.20 % percent when it trained with 25 worker nodes in parallel. 95.22 (with 5 worker)
Future work	Investigate its performance on different datasets and other neural networks.

Table1: Machine Learning Methods for IDS

Source# 24 **Reference**	AKSU & Aydin (2018) .Detecting Port Scan Attempts with Comparative. IEEE
Type of Learning	DL
Attack	158.930 port scan attempts
Detection Mechanism	Deep learning and SVM.S
Method	The SVM and deep learning algorithms were used to detect port scan attempts based on the CICIDS2017 dataset.
Dataset	Up-to-date CICIDS2017 dataset -presented comparatively, & 67% training data and 33% testing data.
Evaluation Parameters	Accuracy (0.99,0), Recall (0.99,070), and F1 Score (0.99,0.65) for DP & SVM respectively and Precision
Pros	Comparative Study approach was used
Cons	Only port scan attempts were studied
Relevance	9/10
Achievement and contribution	DL algorithm performed significantly better results than SVM
Accuracy	DL=97.80%, SVM=69.79%
Future work	To use not only port scan attempts but also other attack types with machine learning and deep learning algorithms, apache hadoop and spark technologies together based on this dataset in the future.

Table1: Machine Learning Methods for IDS

Source# 25 **Reference**	McDermontt et al (2018). Botnet Detection in the I oT using DP approach.IEEE
Type of Learning	DL
Attack	Mirai, botnet,DoS udp, and dns attack
Detection Mechanism	BLSTM-RNN detection model is compared to a LSTM-RNN for detecting four attack vectors used by the mirai Botnet
Method	DL using BLSTM-RNN In conjunction with Word Embedding methodology to create a botnet detection model
Dataset	Labelled dataset was generated as part of this research
Evaluation Parameters	Accuracy and loss.
Pros	Comparison approach between (BLSTM-RNN) and unidirectional LSTM-RNN
Cons	The attack vector metrics were shown to be less favourable+ bidirectional approach adds overhead to each epoch, and increases processing time
Relevance	9/10
Achievement and contribution	better progressive model over time+ helping consumers become aware when their device is infected + generated mirai botnet dataset has been made public and is available upon request.
Accuracy	Results for mirai, udp, and dns were very encouraging with 99%, 98%, 98% validation accuracy and 0.000809, 0.125630, 0.116453 validation loss metrics respectively
Future work	Second more comprehensive dataset will be generated, incorporating all ten attack vectors used by the mirai botnet malware. Altogether a third mutated version of dataset for comparisons. + further investigate ways to improve situational awareness of botnet activity within the IoT

Table1: Machine Learning Methods for IDS

Source# 26 **Reference**	Tang et al (2018).Deep Learning Approach for Network Intrusion Detection in Software Defined Networking. IEEE
Type of Learning	DL
Attack	DoS, probe,U2R and R2L
Detection Mechanism	DL-Use a NSL-KDD dataset on a deep neural Network and implement the IDS on the controller of a SDN architecture
Method	Using a Deep Neuro Network with input and three hidden layers and an output layer Use 6 features of a NSL-KDD dataset to train the model in an IDS placed on the controller of a SDN architecture.
Dataset	NSL-KDD
Evaluation Parameters	Accuracy, precision, recall, F-measure(precision and recall)
Pros	Worked with flow based traffic
Cons	Did not use the full features of the data set and not focused on a specific type of attack
Relevance	7/10
Achievement and contribution	Used deep learning for the flow-based anomaly detection system
Accuracy	82.02%
Future work	Focus on one type attack (DDoS) while use a DNN model with varying the number of hidden layers and hidden neurons for better performance (e.g.). Implement this approach in a real SDN environment with real network traffic and evaluate the performance of the whole network in terms of latency and throughput.
Source# 27 **Reference**	Niyaz et al (2016). A Deep Learning Approach for Network Intrusion Detection System. *EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21-26)
Type of Learning	DL
Attack	DoS, probe, U2R and R2L
Detection Mechanism	DL- Used Self-taught Learning (STL)
Method	Used the NSL-KDD dataset for training and testing of the model. Conducted two approaches. The first one used a dataset for training and testing from the same environment and the second approach used training and testing data collected in different environments. (Rates not clearly indicated)
Dataset	NSL-KDD
Evaluation Parameters	Accuracy, precision, recall
Pros	The approach of using testing data from a different environment from which training data is obtained gives a different output from using both training and testing dataset from the same environment.
Cons	Rates not indicated of the two approaches against each other
Relevance	7/10
Achievement and contribution	the proposed NIDS performed very well compared to previously implemented NIDSs for the normal/anomaly detection when evaluated on the test data.

Table1: Machine Learning Methods for IDS

Accuracy	88.39%
Future work	Implement a real-time NIDS for actual networks using deep learning technique. Additionally, on-the-go feature learning on raw network traffic headers instead of derived features.
Source# 28 **Reference**	Potluri & Diedrich, (2016, September). Accelerated deep neural networks for enhanced Intrusion Detection System. IEEE
Type of Learning	DL
Attack	DoS, R2L, U2R and Probe
Detection Mechanism	DL-Deep Neural Network (DNN) based IDS
Method	Preprocess converting the dataset intro numeric Normalization the dataset by mapping all the different values for each feature Feed the dataset t into the DNN by training and fine tuning through back propagation. Test the DNN using NSL-KDD test dataset
Dataset	NSL-KDD
Evaluation Parameters	Accuracy
Pros	Used all the 41 features of the NSL-KDD dataset to train the DNN however epoch varying at each layer
Cons	Used insufficient data for training therefore U2R and R2L were not well detected and this reduces the overall detection accuracy.
Relevance	9/10
Achievement and contribution	The parallel computing capabilities of the neural network make the Deep Neural Network (DNN) to effectively look through the network traffic with an accelerated performance.
Accuracy	97.70%
Future work	The selection of different features out of all 41 features to improve the detection accuracies Additional features along with the existing 41 features given to the training phase can also improve the detection accuracies and this is also considered in future.

Table1: Machine Learning Methods for IDS

Source# 29 **Reference**	Zhang Li and Wang (2019) IDS for IoT Based on Improved Genetic Algorithm and Deep Belief Network.IEEE
Type of Learning	DL
Attack	DoS, Probe, R2L, U2L
Detection Mechanism	intrusion detection model based on improved genetic algorithm (GA) and deep belief network (DBN)
Method	DBN model optimized with GA is trained with the training sets and then evaluated using the test set. At the same time, we compared our method with the methods TANN, FC-ANN, SA-DT-SVMS, and BPNN proposed by others researchers.
Dataset	NSL-KDD dataset was used to simulate and evaluate the model and algorithms
Evaluation Parameters	Accuracy, Detection Rate, FAR, Precision, Recall
Pros	Self-adaptive model to change the network structure for different attack types.
Cons	Not stated
Relevance	9/10
Achievement and contribution	Results show that the improved intrusion detection model combined with DBN. Can effectively improve the recognition rate of intrusion attacks and reduce the complexity of the neural network structure.
Accuracy	Than 99% of detection rate. i.e. 99.45, 99.37, 97.78, 98.68 % for DoS, Probe,R2L, and U2R respectively
Future work	Optimize the other parameters of the deep network, reduce the training time and improving the detection accuracy.

Source# 30 **Reference**	Rezvy et al (2019).An efficient DL model for intrusion classification andand prediction in 5G and IoT networks.IEEE
Type of Learning	DL
Attack	Flooding, Impersonation and Injection type of attacks
Detection Mechanism	Deep auto encoder, dense neural network(DNN) .
Method	Auto encoded DNN algorithm for detecting intrusion or attacks in 5G and IoT network
Dataset	Benchmark Aegean Wi-Fi Intrusion dataset. (AWID-CLS-R) contain real traces of both normal and intrusive 802.11 WLAN
Evaluation Parameters	Precision, Recall or TPR, and F-measure
Pros	Comparison of Proposed Autoencoded DNN with other learning methods such as stacked autoencoder, Neural network, Random forest, Majority voting etc.
Cons	None stated

Table1: Machine Learning Methods for IDS

Relevance	8/10
Achievement and contribution	Presented a comparison with recent approaches used in literature which showed a substantial improvement in terms of accuracy and speed of detection with the proposed algorithm
Accuracy	99.9%
Future work	Provide extensions or modifications of the proposed algorithm for larger attack types, mobile and IoT security platforms as suggested in ref [18] using intelligent agents such as soft computing and advanced unsupervised clustering algorithms. +improve the detection accuracy and to reduce the rate of false negatives and false positives