Analysis and design of a model for the classification of attacks on IoT devices

Angela Arul, 2021A7PS0005U

Abstract

Over the past few years, tremendous growth has been seen in the fields of Internet of Things(IoT). There have been various researches and experimentations carried out in this field, especially with respect to the security of IoT networks. Therefore, in order to categorize and investigate more on the different IoT attacks, we need an intrusion detection system. In this research paper, we have used both Machine Learning and Deep Learning approaches to go about with the categorization of the attacks based on two different datasets: the UNSW_NB15 and the latest 2018_attack_dataset. First we applied the datasets on the Deep Learning Model(DNN) model and then we applied the same dataset on Feed Forward Neural Network(FNN) model. Moreover, Sampling was performed on the datasets so as to resolve the class imbalance involved . This helped to boost the performance of the models when applied to both the datasets and thereby gave better accuracy rates. In order to understand and comprehensively analyze the DL models, we have used Explainable AI tools to provide the explanation of the performance of the models. For a better understanding, we have used Local Interpretable Model-agnostic Explanations(LIME) method.

ANALYSIS

Table- dataset -UNSW_NB15

model	Accuracy	Accuracy
K-nn	0.841	0.77
Decision tree	0.86	0.761
SVM		0.77
DNN	0.9338	0.8
FNN	0.9687	-
1D cnn	0.9323	0.799

Table-dataset-New dataset

model	Accuracy
K-nn	0.99
Decision tree	
SVM	0.99
DNN	0.908
FNN	
1D cnn	

LITERATURE REVIEW

Literature survey Table

Ref No.	Objective	Problem Statement	Methodology	Advantages	Disadvantages	Software Tool used	Performance Measure
1.	-To propose a lightweight and efficient intrusion detection method based on feature grouping	-Existing IoT oriented intrusion detection systems usually only support the detection Accuracy -Difficulty involved in selecting traffic features with a good detection effect by ML and DL automatically This results in low detection accuracy and high computational complexity for IDSs.	-Feature extraction is performed -The sessions which are based on different protocols of feature extraction are merged -Feature grouping is performed	-The proposed method reaches a high accuracy score for the three datasets based on which experiments were conducted and thereby outperforms the baseline models - Moreover, it requires fewer computational resources and is able to achieve outstanding classification performance	---	-The Pyshark library has been used to preprocess the data.	-The performance evaluation metrics of the model are accuracy, precision, recall and f1-score
2.	To capture and analyze the interplay of stage	- Increasing security concerns of IoT devices in an ADIoTs.	-The approach is based on distributed voting based detection.	-With the help of this approach, the effect of attack strategies		- SPN(Stochastic Petri Net) mathematical tool	-The performance of the experiment is measured based on the MTTF (Mean Time to

	and defense strategies for intrusion and detection in an autonomous distributed IOT system		-SPN based models are used here for the specification and analysis of voting based IDS functions. -The application of the above mentioned approach was done on a selected set of attack-defense strategies and the optimal defense settings were identified to maximize the lifetime of the IOT network.	were analyzed on system failure conditions and system lifetime. -The most damaging attack strategy was identified -New defense strategies have been suggested for maximizing the system's mean time to failure(MTTF)	-		Failure) and T_{IDS} (Intrusion detection interval).
3.	To propose an edge-centric IoT defense scheme termed as the FlowGuad which helps to detect, mitigate , identify and classify IoT DDoS attacks	- Insecurity of IoT devices with respect to DDoS attacks - The Protective strategies developed and researched are largely insufficient and impractical for IoT devices.	-A new DDoS attack detection algorithm is formulated based on the traffic variations -Further, two machine learning models are designed for the identification and classification of DDoS attacks.	-The models satisfactorily meet the delay requirement of IoT when used in edge servers with higher computational powers than that of a personal computer.	-	-Keras and TensorFlow -simulators: BoNeSi and SlowHTTPTest	-The performance of the two machine learning models is measured based on a large dataset generated using simulators and real-world data -The performance metrics used to measure the model are accuracy and efficiency
4.	-To propose ADEPT, a security	-Attacks on IoT devices generally	-ADEPT works in 3 phases:	-ADEPT was able to successful		-WEKA software platform was used for the	-The different performance measures used in the

	framework that correlates suspicious activities across space and time to detect patterns and classify them into possible attack stages.	consist of multiple stages and are dispersed spatially and temporally, thereby making it challenging to detect and identify the attack stages using solutions that tend to be localized in space and time.	--First ,network traffic of IoT devices is processed locally for detecting anomalies with respect to their benign profiles. --Any alerts corresponding to a potential anomaly is sent to a security manager. In the security manager, the aggregated request are mined using frequent itemset mining(FIM), for detecting patterns correlated across both time and space. --Lastly using both alert-level and pattern-level information as features, a machine learning approach is employed where a classification model is built to identify individual attack stages in the generated alerts.	ly detect attack patterns up to five times more than two baselines that have been evaluated and is able to classify them to the corresponding attack stages with an accuracy of 99%. -ADEPT can not only detect anomalies but also extract and identify attack stages in coordinate large-scale cyberattacks.	--	implementation of the models. -The FIM algorithms were using the Java-based SPMF software library.	attack-stage detection are precision, accuracy, recall, and F1-score.

5.	-To address the problem of adversarial attack generation and mitigation in IoT environments while focusing on smart home applications	- Research has shown the neural networks and deep networks are prone to adversarial manipulation when image and audio data is used. -These attacks cause the data points to be misclassified into a specific class and thereby reduces the accuracy of the ML classification model.	-Develop a white-box attack mechanism to generate adversarial examples for data obtained from smart meters of residential houses. - Demonstrate outlier detection methods will not be able to combat these adversarial examples. This showcases the need for training and deploying ML models for IOT applications which remain unaffected against such attacks.	-The devised methodology helped to reduce the severity of adversarial attacks to a certain extent.	-Despite the effectiveness of the defense method devised, the adversarial attack was still able to increase the error rate by a sizeable margin thereby causing the result to tilt in favor of the proposed adversarial attack.	-Deep Learning classification techniques used.	-The performance of the models are measured based on the error rates.
6.	-To verify threat of adversarial attacks on individual device identification, and explore the factors that affect the effectiveness of nontargeted and targeted attacks.	-The increasing security risks faced by IoT with respect to DL models, thereby posing a greater threat to the training process, testing process and privacy	-Creation of individual Identification Data Sets -Generation of Adversarial Examples -Combine Evaluation Indicators of Logits	-With the help of this study, the effects of targeted and nontargeted adversarial attacks on CNN-based device identification was analyzed -These insights will provide to	-	-Keras and TensorFlow machine learning frameworks were used	-The performance measures used are accuracy and ASR(Attack Success Rate)

		security of the model.		be useful for the design of robust DL-based IoT systems.			
7.	-To propose a hybrid deep learning model for detecting replay and DDoS attacks in a real life smart city platform.	-In general Cyber-attacks threaten the ability of smart cities to supply consistent, trusted and timely services to their citizens . - Threatens citizens' privacy of information -Attacks such as DDoS attacks obscure services from end users through a set of distributed agents created by attackers.	-The proposed model consists of an input layer, deep RBM model with 2 hidden layers, deep CNN with seven hidden layers, a global average pooling layer, and a softmax output layer. -Three algorithms were proposed based on which the network is trained:- - Algorithm1-describes the training procedure for the proposed hybrid model - Algorithm2-describes the replay attack model - Algorithm3 -describes the DDoS attack model -The network is then trained	-The proposed model outperforms all the others models with a high detection accuracy -It also has the capacity to detect more different types of attacks, apart from being just trained to detect attacks such as DDoS and replay.	-The model can only detect DDoS and replay attacks since it has only been trained to detect these attacks.	-All models were implemented in Python 3.7 using Keras and TensorFlow frameworks.	-The measure used to evaluate the performance of the models is accuracy

			based on these algorithms, tested and evaluated				
8.	-To propose the federated DL(FDL) method for zero-day botnet attack detection to avoid data privacy leakage in IoT-edge devices.	-Detecting zero-day cyber attacks using traditional centralized DL methods cannot be done without breaching the data privacy rights of the users.	-Proposal of FDL algorithm -Building Deep neural network - To determine the optimal neural network architecture for efficient network traffic classification, 16 DNN models were trained and tested with the BoT-IoT and N-BaIoT datasets. -Models such as CDL,LDL,DDL,FDL were developed for zero-day botnet attack detection in 5 IoT-edge devices.	- Experimental results show that the FDL model: - Successfully detects zero-day botnet attacks with high classification performance - Guarantees data privacy and security -Has low communication overhead -has low network latency	-The proposed model takes a longer training time.	-TensorFlow and Keras frameworks were used for the DNN local models in the CDL,LDL,DDL and FDL methods -IBM framework was used for FL in the FDL method. -Models were trained using the Spyder IDE.	-The performance of the proposed methodology is evaluated using the performance measures: accuracy, precision, recall, and F1 score
9.	-To verify the reliability of the detection approach when the network encounters an attack that it was not trained on before.	-Security risks posed to IoT devices by Botnet attacks - Overfitting issue faced by neural networks.	-Data preparation -Training the regularizer DL model based on the CNN and L1 and L2 -Testing the model under three different scenarios: -Scenario1: Testing classifiers	-The introduction of regularization technique such as L1 and L2 have helped to solve to the issue of overfitting and moreover, using	-The CNN models took a longer time to train	-All the experiments were executed in Anaconda which includes the python interpreter, many useful libraries and Spyder IDE using Python programming language(v3.8).	-The performance of the model was evaluated using measures such as accuracy, F1-score, precision, recall, and ROC curves

			on DDoS attack data -Scenario2: Testing classifiers on OS Fingerprint attack data -Scenario3: Testing classifiers on Service Scan attack -Evaluating the performance of the model	these methods gives a higher performance with regards to all evaluation metrics compared to the standard CNN model. -The enhanced CNN technique helps to improvise the capability of IDSs in the detection of unseen intrusion events -The proposed CNN model outperforms the standard ML algorithms across all assessment measures		-Libraries such as Keras, TensorFlow, numpy, pandas, and SciKit-Learn were used for the execution of the models	
10.	-To propose a novel two-fold approach to prevent botnet attack during the premature stage -To detect DDoS	-Based on existing studies, the performance of most of the existing machine learning based botnet detection	-The proposed solution involves two machine learning models:- -First fold: here, a ResNet-18 model is trained for scanning	-The proposed ResNetScan-1 and ResNetDDoS-1 models persisted in their performance and were able to outperfor	-The performance of all ResNetScan and ResNetDDoS models except ResNetScan-1 and ResNetDDoS-1 model	-Three different network traffic generator tools have been used for experimentation:-Nmap,Hping3 and Dmitry.	-The performance measures used for evaluating the models are accuracy, F1-score,precision ,and recall

	attack in IoT network in case an attacker compromises an IoT device and starts performing a DDoS attack.	models is limited to a specific dataset on which they are trained. As a consequence, the solutions do not perform well on other datasets due to the diversity of attack patterns.	attack detection. -Second fold: here, a ResNet-18 model is trained for DDoS attack detection. Stages involved in building the two models:- --Data collection -- preprocessing the data -- Performing feature selection --Training the ML model for scan detection --Testing the model and model evaluation	m all the other models. Therefore, the proposed two fold-approach is efficient and robust to prevent and detect IoT botnet attacks with a large attack pattern coverage.	crucially reduced when these models were tested over the test-set of other datasets on which they were not trained.		
11.	-To propose a new effective feature selection technique for the problem of effective feature selection for cyberattacks in IOT network traffic by using the Bot-IoT dataset and to improve the	-The inability to select effective features due to which several ML models are prone to misclassifying mostly malicious traffic flows.	-Proposal of a new feature selection algorithm-CorrAUC which is developed using the AUC metric and BoT-IoT dataset -The proposed algorithm consists of CAE and combines with the AUC(Area under curve) metric to overcome the problem of effective	-Results show that al the attacks and normal traffics are very effectively detected by using the selected feature set. -Thereby, it is clear that the proposed feature selection technique is effective for the selection	----	-----	-The different performance metrics used are accuracy, precision, sensitivity and specificity

	performance of ML techniques.		feature selection. -Then, Shannon entroy TOPSIS was applied based on a bijective soft set for the validation of the selected features for Bot-IoT attacks traffic identification in the IoT network.	of features for the Bot-IoT detection in the IoT network environment			
12.	-To propose a novel secure network model to enhance network security and employees' privacy in an edge-enabled industrial IoT.	-Data insecurity of industrial resources and employees' data in storage platforms as well as in cloud	-The proposed approach was implemented using VHN. -The VHN consists of many honeypots which are used to deceive and trap attackers. -A CS was connected with the VHN to ensure two-way communication in real time. -The CS was further armored with AI to better manage inbound and outbound traffic from/to the VHN. -Further, Two subsets	-The proposed model presents notable performance rates not only against known threats but also against new unknown threats.	-----	-----	-The different performance measures used are accuracy, precision, recall, False positive rate(FPR), F1-score, and Matthews correlation coefficient(MCC)

			of AI-ML and DL are integrated into the CS to analyze CRs to check if they are benign or malicious -An edge-enabled IoT network composed of many industrial devices and sensor nodes that are wirelessly connected with each other was also built.				
13.	-To develop a lightweight machine learning approach to detect DoS attacks in WSNs	-WSNs are more vulnerable to security attacks than other networks, especially DoS attacks. -Requires security solutions that causes very low overhead, which is difficult to achieve.	-Obtaining the Dataset -Perform Feature Selection -Train, Test and Validate the model	-Based on the performance of the classifiers, the proposed approach significantly outperforms the other classifiers in terms of processing time, which is an important factor to consider when dealing with WSNs that face challenge of limited resources.	-Although classifiers such as RF and XGBoost are one of the better performing ensemble classifiers that are capable of improving prediction accuracy, it leads to more computational overhead that does not fit networks with limited resources.	-Orange data mining software used	-The performance measure used was accuracy, recall, precision ,F1 score and ROC curve
14.	-To propose a	-Lack of appropriat	-The dataset IoT-Cross	- Using the		-Use of Cooja environment	-The performance of

	feature engineering and ML framework to detect Distributed-Denial-of-Service(DDoS) attacks of IoT-CIDDS dataset.	e datasets for training and evaluating ML-based IDS(Intrusion Detection System), due to which ML-based IDS lacks accurate and uniform performance advancements.	Layer Intrusion Detection Dataset(IoT-CIDDS) is fetched -Feature Engineering is performed on the dataset -Feature conversion -Feature Extraction -Feature Selection -Feature Normalization. -The models are built based on the finally obtained features -For the improvement of the models, Hyperparameter Optimization is performed -For Analyses , K-fold Cross validation is performed -The models are then evaluated based on their performance	approach, one of the best performing classifiers -Random Forest was obtained due to its high detection rate and minimum false positive and computation time -The study also reveals through experimentation that substantial feature reduction optimizes the performance of ML-based IDS for detecting DDoS attacks in standardized IoT networks.	-	for simulation/emulation of IoT nodes so as to generate real-time traffic in a real IoT testbed network. -Feature Engineering and model training was done at the resource rich 6LBR which takes in packet traces as input and returns the DDoS detection results as output	the model is measured based on the Accuracy, False positive, precision,recall ,F1-score,AUC and Time
15.	-To propose a new framework called FMDADM, which is an SDN-based, four nodule for	-Susceptibility of IoT based networks to DDoS attacks -Inclusion of unrelated features	-Creation of first detection module -Creation of second detection module -Creation of third	- The proposed framework can detect DDoS with high accuracy in multi-node attack scenarios.		-Anconda's Spyder software used -To develop and run the IoT test topologies, the software tools used:	-The performance measures used: accuracy,precision,F1-score, recall, sensitivity, specificity, negative predictive

	DDoS attack detection and mitigation.	renders a less effective model for detecting attacks. -The construction of an effective model depends on packet feature engineering approach which is crucial.	detection module - preprocess the data -Perform Feature Extraction -Training and Testing the model - Classification of data and working of model	-The framework also performs better than the existing ML methods in terms of accuracy, F1-score,recall and false positive rate -The design of the three detection modules results in a reduction in the amount of time needed for training, testing and detection -The proposed framework can effectively identify DDoS attacks at both high and low rates.	-	-VMware Workstation 12 Pro -Mininet-IoT -sFlow-test -sFlow Mininet dashboard	value(NPV), false positive rate(FPR),false discovery rate(FDR), miss or false-negative rate(FNR), and average detection time(ADT)
16.	-To present a modular and flexible SDN-based architecture to detect DDoS attacks	-Although several works have proposed solutions to detect DDoS attacks , most of them did not use	-The proposed architecture consists of four modules: Flow Collector, Preprocessing ,Detection,	-This work was able to test their proposals in a real and simulated network in comparison to the	-The accuracy of the models was slightly reduced on the multiclass metrics, in comparis	-Mininet network emulator and ONOS controllers were used to experiment with the proposed architecture. -Offline preprocessin	-The different performance measures used here are: -Accuracy -F1-score -Precision -Recall

	using multiple ML and DL models	up-to-date datasets which contain the latest threats. -Only a few of the previous works used previous works to assess their solutions.	and Flow Manager. -The ML/DL models used for this architecture are trained with two public datasets which is preprocessed. The models are then tested and Hyper-parameter tuning is done based on the performance of the models. The performance of the models is then evaluated	previous works. -Unlike the previous works, this work covers the comprehensive evaluation of the performance of 7 ML/DL mechanisms in detecting diverse low-volume and high-volume DDoS attacks. Moreover the attack conditions were also varied to assess the robustness of each DL/ML method. -The performances achieved in this work proves that the proposed solution is more realistic and can be implemented in production networks.	on to the binary metrics, which reveals the fact that the models slightly decreased their accuracy to discern among different application-layer attacks.	g of data was performed using R-Software. -To train and test the model, Jupyter notebook and Google colab was used.	
17.	-To propose a novel	-Security risks of IoT	-The proposed framework	-With regards to the results		-COOJA simulator tool and the	-The performance of the proposed

	SDN-based secure IoT framework that can detect the vulnerabilities in IOT devices or malicious traffic generated by IoT devices using the session IP counter and IP Payload analysis.	devices with respect to DDoS attacks	consists of three main modules:- controller module, SINK module and IoT module. -The framework uses two algorithms for DDoS attack detection. The first algorithm is based on packet frequency every node is evaluated that has sent/received packets with exceeding threshold to time. The second algorithm recognizes the malicious packets on behalf of the packet payload size. Both these algorithms run an attack detection module using a log file to monitor the DDoS attack in the SD-IoT network.	and comparative analysis, the proposed framework detects DDoS attacks in the early stage with high accuracy and detection rate from 98% to 100%, having a low false-positive rate -The framework has also proven to be efficient due to its fast analysis and detection time.	-	SDNWISE controller was deployed	framework was evaluated based on different attributes such as:- - packet size -packet frequency - Burst mode Frequency and the utilization of the CPU and the system resources.
18.	-To propose an SD-IoT based framework	-Security risks of IoT devices with	-Creation of the 3 layers of the framework:	-The proposed framework with the C-DAD		-The simulation based-experiments were	-The algorithm and framework were tested through different

	k that provides security services to the IoT network	respect to DDoS attacks	- The first layer consists of security applications that detects the attack -The second layer is the control layer -The third layer is the infrastructure layer -Creation of the Counter based attack Detection application -setting up of the Sensor OpenFlow Switch and IoT node -Building the attack mitigation module	application efficiently detects the DDoS attack by minimizing the time of attack detection with a tolerable impact on CPU and memory.	-	conducted on SDNWISE controller and Cooja simulator	experiments and their overall performance was measured with respect to different factors such as: -CPU utilization -Memory utilization -SD-IoT Network Throughput -SDNWISE Controller Workload -Attack Detection Time
19.	-To propose a practical anomaly-based intrusion Detection System(IDS) that is capable of timely detecting and mitigating DDoS attacks, especially the stealthy ones, which are challenging to detect and	-Security risks of IoT devices with respect to a new type of stealthy DDoS attack , called Mongolian DDoS, which is characterized by its widely distributed nature and small attack size from each source.	-The proposed methodology is based on a statistical anomaly detection algorithm called Online Discrepancy Test(ODIT) that mitigates the attack with minimal interruption of regular services Here, a small modification to the ODIT is proposed where its asymptotic	-Based on the results, the proposed method was successfully able to mitigate the stealthy DDoS attacks	-It is assumed that the nominal behavior of the devices does not change over time, so the IDS needs to be trained only once. However, in real-time they need to be trained periodically. -The feature extraction	-	-The performance of the proposed detection mitigation scheme was evaluated under challenging stealthy DDoS attack scenarios through real and simulated data, as well as an IoT testbed.

	mitigate due to their capability of bypassing traditional filters.		optimality is proven in the minimax sense as the training data size grows. -The time and space complexity of the DDoS attacks is analyzed -A solution is also provided to a dynamic scenario where the number of devices in the network changes -A comprehensive performance evaluation is done using testbed implementation.		playing an important role as number of packets or packet size might not always exactly represent the characteristics of a real-time network.		
20.	-To propose a lightweight architecture that distinguishes attack network flows from normal traffic and retaining its ability to obtain high detection accuracy using simple designs with low computati	-Increasing variations of DDoS attacks have rendered some of the propose detection systems ineffective -Some of the detection systems are very complex, leading to high computational cost, and	-Collection of data -preprocessing of the dataset -Applying Low Variance Filter Feature Selection Technique for selection of relevant features from the dataset -Construction of Decision Tree model using the Decision Tree	-The proposed lightweight Decision Tree model with just 3 selected features is very effective and efficient in distinguishing benign from DDoS attack network traffic flows with a detection accuracy		-WEKA data mining tool and the Scikit-Learn which is a python library were used to construct the Decision Tree model	-The performance of the model was measured using metrics such as accuracy, precision, Misclassification Error Rate, Sensitivity, Specificity and F1-score

	onal cost without affecting the performance of the network.	incurs high overload to the network being monitored	algorithm and training it -Testing the model -Evaluating its performance	of over 99%. -Analysis of the design and its performance reveals that using only 3 features consumes minimal load on the detection system's CPU while still maintaining high detection accuracy.	---		

Summary of papers

Paper1:

Existing IoT oriented intrusion systems usually only support the detection accuracy and moreover, due to the difficulty involved in selecting traffic features with a good detection effect by ML and DL automatically results in low detection accuracy and high computational complexity for Intrusion Detection Systems(IDSs).Therefore due to these issues, a lightweight and efficient intrusion detection method has been proposed in this paper[1] based on feature grouping. The proposed methodology follows steps such as: feature extraction, merging of sessions of feature extraction (each session is based on a different protocol), and feature grouping. Moreover, the performance of this approach is measured using different evaluation metrics such as accuracy, precision, f1-score, and recall. Results show that this paper has been successfully proven to reach a high accuracy score for the

three datasets based on which experiments were conducted and thereby outperforms the baseline models. Also, it requires fewer computational resources and is thereby able to achieve outstanding classification performance.

The main objective of this paper[2] is to capture and analyze the interplay of stage and defense strategies for intrusion detection in an autonomous distributes IOT system (ADIoTs) . The increasing security concerns of IoT devices in an ADIoTs is the main motivation for this approach. The approach considered in this paper is based on distributed voting based detection. SPN based models were used here for the specification and analysis of the voting based IDS functions. Moreover, the application of the above mentioned approach was done on a selected set of attack-defense strategies and the optimal defense settings were identified to maximize the lifetime of the IoT network. The performance of the approach was measured based on the MTTF(Mean Time to Failure) and T_{avg} (Intrusion detection interval). With the help of the approach, the effect of attack strategies can be analyzed on system failure conditions and system lifetime. Moreover, the most damaging attack from the set of attacks taken into consideration was efficiently identified by the model. New defense strategies have also been suggested in this paper for maximizing the systems' mean time to failure(MTTF).

In paper[3], The aim is to propose an edge-centric IoT defense scheme termed as the FlowGuard which helps to detect, mitigate, identify and classify IoT DDoS attacks. Insecurity of IoT devices with respect to DDoS attacks and the insufficiency of the protective strategies developed being impractical for IoT devices are the main motivations for the proposed methodology. In this paper, A new DDoS attack detection algorithm is formulated based on the traffic variations. Further, two machine learning models are designed for the identification and

classification of DDoS attacks. Results show that the models satisfactorily meet the delay requirement of IoT when used in edge servers with higher computational powers than that of a personal computer. The performance of the two machine learning models is measured based on a large dataset generated using simulators and real-world data and the metrics used are accuracy and efficiency.

In paper[4], A security framework called ADEPT has been proposed. This framework helps to correlate suspicious activities across space and time to detect patterns and classify them into possible attack stages. Attacks on IoT devices generally consist of multiple stages and are dispersed spatially and temporally thereby making it challenging to detect and identify the attack stages using solutions that tend to be localized in space and time. Therefore, this solution has been proposed to counteract these problems. ADEPT works in 3 phases: Firstly, network traffic of IoT devices is processed locally for detecting anomalies with respect to their benign profiles. Any alerts corresponding to a potential anomaly is sent to a security manager. In the security manager, the aggregated request are mined using frequent itemset mining(FIM),for detecting patterns correlated across both time and space. Lastly using both alert-level and pattern-level information as features, a machine learning approach is employed where a classification model is built to identify individual attack stages in the generated alerts. The performance of the model measured based on the accuracy reveals that the proposed framework was able to successfully detect attack patterns up to five times more than two baselines that have been evaluated and is able to classify them to the corresponding attack stages with an accuracy of 99%. Moreover, it can not only detect anomalies but also extract and identify attack stages in coordinate large-scale cyberattacks.

The aim of paper[5] is to address the problem of adversarial attack generation and mitigation in IoT environments while focusing on smart home applications. Researches have shown that neural networks and deep networks are prone to adversarial manipulation when data such as image and audio data is used. These attacks tend to the misclassification of data points into a specific class and thereby reduces the accuracy of the ML classification model. Hence, with regards to these problems, this following methodology has been proposed; a white-box attack mechanism is developed to generate adversarial examples for data obtained from smart meters of residential houses. Moreover, the demonstration of outlier detection methods will not be able to combat these adversarial examples. This showcases the need for training and deploying ML models for IOT applications which tend to remain unaffected against such attacks. The performance of the models were measured based on the error rates. Results based on the performance of the model reveals that the devised methodology helped to reduce the severity of adversarial attacks to a certain extent.

Paper[6] proposes a methodology to verify threat of adversarial attacks on individual device identification, and explore the factors that affect the effectiveness of nontargeted and targeted attacks. The increasing security risks faced by IoT with regards to DL models, thereby posing a greater threat to the training process, testing process and privacy security of the model is the main motivation of this paper. The methodology involves the creation and identification of individual datasets followed by the generation of adversarial examples and lastly the combining of evaluation indicators of Logits. The performance of this approach was evaluated based on the accuracy and attack success rate(ASR).To sum up, the proposed methodology has proven to be useful as it helps in the analysis of targeted and nontargeted adversarial attacks on CNN-based device identification and these insights are very much useful for the design of robust DL-based IoT systems.

Paper[7] proposes a hybrid deep learning model for detecting replay and DDoS attacks in real life smart city platform. Cyber attacks in general threaten the ability of smart cities to supply consistent, trusted and timely services to their citizens and also tends to threaten citizen's privacy of information. Moreover , attacks such as DDoS attacks obscure services from services from end users through a set of distributed agents created by attackers. The proposed methodology helps to counteract these issues through a hybrid deep learning model. The model consists of an input layer deep RBM model with 2 hidden layers, deep CNN with seven hidden layers, a global average pooling layer, and a SoftMax output layer. Three algorithms have been proposed on which this network is trained; Algorithm1 describes procedure for the proposed hybrid model, Algorithm2 describes the replay attack model and lastly Algorithm3 describes the DDoS attack model. The network is then trained on bases of these proposed algorithms, tested and evaluated using performance measures such as accuracy. Based on its performance, the proposed model outperforms all the other models with a high detection accuracy and also has the capacity to detect more different types of attacks, apart from being jus trained to detect attacks such as DDoS and replay attacks.

Paper[8] proposes a federated DL(FDL) method for zero-day botnet attack detection to avoid data privacy leakage in IoT-edge devices. Detecting zero-day cyber attacks using traditional centralized DL methods cannot be done without breaching the data privacy rights of the users; thereby to avoid this privacy breach this methodology has been proposed. In this approach, an FDL algorithm has been proposed based on which a Deep neural network is built. In this manner 16 DNN models were built, trained and tested with the BoT-IoT and N-BaIoT datasets so as to determine the optimal neural network architecture for efficient network traffic classification. The performance of the model is

evaluated using performance measures such as accuracy, precision, recall, and F1-score. Based on the results, the proposed FDL models are successfully able to detect zero-day botnet attacks with high classification performance and guarantees data privacy and security. Moreover, it has low communication overhead and low network latency.

Paper[9] proposes an methodology to verify the reliability of the detection approach when the network encounters an attack that it was not trained on before. This methodology is proposed to counteract problems such as security risks proposed to IoT devices by botnet attacks and overfitting problems faced by neural networks. In this methodology , a regularized DL model is built on the basis of CNN , L1 and L2 regularizers. The model is then tested under three different scenarios: Scenario1 where the classifiers are tested on DDoS attack data, Scenario2 where the classifiers are tested on OS Fingerprint attack data and Scenario3 where the classifiers are tested on Service Scan attack. The performance of the model is then evaluated based on measures such as accuracy, F1-score, precision, recall and ROC curves. The performance of the model evaluated using measures such as accuracy, F1-score, precision, recall, and ROC curves, reveals that the introduction of regularization technique such as L1 and L2 have helped to solve the issue of overfitting and moreover, usage of these methods gives a higher performance with regards to all the evaluation metrics compared to the standard CNN model. In addition to this, the enhanced CNN technique also helped to improvise capability of IDSs in the detection of unseen intrusion events.

(Base)Paper[10] proposes a novel two-fold approach to prevent botnet attack during the premature stage and to detect DDoS attack in IoT network in case an attacker compromises an IoT device and starts performing a DDoS attack. Based on existing studies, the performance

of most of the existing machine learning based botnet detection models is limited to a specific dataset on which they are trained. As a consequence, the solutions do not perform well on other datasets due to the diversity of attack patterns. The proposed methodology in this paper solves the issue by building two machine learning models: First fold/model is a ResNet-18 model which is trained for scanning attack detection and the Second fold/model is another ResNet-18 model trained for DDoS attack detection. The different stages involved in building the models are data collection, preprocessing the data, performing feature selection, training the ML model for scan detection and lastly testing the model and model evaluation. In this paper, the different evaluation measures used are accuracy, f1-score, precision, and recall. Based on the results, the performance of ResNetScan-1 and ResNetDDoS-1 models persisted in their performance and were able to outperform all the other models. To sum up, the proposed two fold-approach is efficient and robust to prevent and detect IoT botnet attacks with a large attack pattern coverage.

Paper [11] talks about a new effective feature selection technique for the problem of effective feature selection for cyberattacks in IOT network traffic by using the Bot-IoT dataset and to improve the performance of ML techniques. The inability to select effective features due to which several ML models are prone to misclassifying mostly malicious traffic flows is the main motivation for this approach. The proposed methodology involves the proposal of a new feature selection algorithm- CorrAUC which is developed using the AUC metric and BoT-IoT dataset. It also involves a newly introduced algorithm that consists of CAE and combines with the AUC(Area Under Curve) metric so as to over the problem of effective feature selection. Then the Shannon entropy TOPSIS was applied based on a bijective soft set for the

validation of the selected features for Bot-IoT attacks traffic identification in the IoT network. The performance of the model was measured using metrics such as accuracy, precision, sensitivity, and specificity. Results of the performance of the model show that the attacks and the normal data traffics are very effectively detected by using the selected feature set, thereby making it clear that the proposed feature selection technique is effective for the selection of features for the BoT-IoT detection in the IoT network .

Paper[12] talks about a novel secure network model to enhance network security and employees' privacy in an edge-enabled industrial IoT. Data insecurity of industrial resources and employees' data in storage platforms as well as in the cloud is one of the main motivations for this approach. The proposed approach was implemented using VHN. The VHN consists of many honeypots which are used to deceive and trap the attackers. A CS is connected with the VHN to ensure two-way communication in real time. The CS was further armored with AI to better manage inbound and outbound traffic from and to the VHN. Further, two Further, Two subsets of AI-ML and DL are integrated into the CS to analyze CRs to check if they are benign or malicious. In addition to all this, an edge-enabled IoT network composed of many industrial devices and sensor nodes with wireless connection with was also built. The performance of the model was measured using different metric such as accuracy, precision, recall, False positive rate(FPR), F1-score, and Matthews correlation coefficient(MCC). Results show that the proposed model reveals notable performance rates not only against known threats but also against new unknown threats.

(base)Paper[13] proposes to develop a lightweight machine learning approach to detect DoS attacks in WSNs. The vulnerability of WSNs to

security attacks than other DoS attacks and difficulty involved in achieving such security solutions are the main motivations for proposed approach in this paper. The proposed methodology involves obtaining the dataset, performing feature selection, training , and validating the machine learning model. The performance of the model was evaluated using various metrics such as accuracy, F1-score, recall, precision and ROC curve. Based on its performance, the proposed approach significantly outperforms the other classifiers in terms of processing time, which is an important factor to consider when dealing with WSNs that face the challenge of limited resources.

Paper[14] proposes a feature engineering and ML framework to detect distributed-Denial-of-service(DDoS) attacks of IoT-CIDDS dataset. One of the many problems faced by ML frameworks based on which Intrusion Detection Systems(IDSs) are designed is that they lack appropriate datasets for their training and evaluation thereby causing them to lack accurate and uniform performance advancements. The solution proposed here helps to counteract this problem is to design ML frameworks. For this, an IoT-Cross Layer Intrusion Detection Dataset(IoT-CIDDS) is fetched. After fetching the appropriate dataset, feature engineering is performed on the dataset followed by feature conversion, feature extraction, feature selection and feature normalization. After the preprocessing phase, the ML models are then built based on the finally obtained features. Moreover, for the improvement of the models built, Hyperparameter Optimization is performed. For analyses purposes, K-fold Cross validation is performed. The models are then evaluated based on their performance which is measured by various metrics such as accuracy, false positive, precision, recall, f1-score, AUC and time. Using this approach, one of the best performing classifiers – Random forest was obtained due to its high

detection rate and minimum false positive and computation time. In addition to this, the study also reveals through experimentation that substantial feature reduction optimizes the performance of ML-based IDS for detecting DDoS attacks in standardized IoT networks.

Paper[15] proposes a new framework called FMDADM, which is an SDN-based, four module framework for DDoS attack detection and mitigation. Susceptibility of IoT based networks to DDoS attacks, Inclusion of unrelated features renders a less effective model for detecting attacks, and the significance of packet engineering are some of the main problems faced with respect to ML models used for detecting DDoS attacks. The proposed methodology involves creation of three detection modules, followed by preprocessing of data, then feature extraction, training and testing the model, and lastly evaluating its performance. The performance of the model has been evaluated using measures such as accuracy, precision, F1-score, recall, precision, sensitivity, specificity, negative predictive values(NPV), false positive rate(FPR),false discovery rate(FDR), miss or false-negative rate(FNR), and average. Results show that the proposed framework can detect DDoS with high accuracy in multi-node attack scenarios at both high and low rates and thereby was able to outperform the existing ML methods in terms of the mentioned evaluation metrics. Moreover, the design of the three detection modules resulted in the successful reduction of time needed for training, testing and detection.

Paper[16] presents a modular and flexible SDN-based architecture used to detect DDoS attacks using multiple ML and DL models. Although several works have proposed solutions to detect DDoS attacks , most of them did not use up-to-date datasets which contain the latest threats.

Moreover, only a few of the previous works used previous works to assess their solutions. The methodology proposed in this paper solves the above issues by proposing an architecture that consists of four modules: Flow collector, Preprocessing, Detection, and Flow manager. The ML/DL models used for this architecture are trained with two public datasets which are preprocessed. The models are then tested and Hyper-parameter tuning is done based on the performance of the models. The performance of the models is then evaluated using different measure such as accuracy, F1-score, precision, and recall. The proposed work in this paper was able to test their proposals in a real and simulated network in comparison what has been done in the previous works. Unlike them, this work covers the comprehensive evaluation of the performance of 7 ML/DL mechanisms in detecting diverse low-volume and high-volume DDoS attacks. Also, the attack conditions were also varied to assess the robustness of each DL/ML method. To conclude, the performances achieved in this work proves that the proposed solution is more realistic and can be implemented in production networks.

Paper[17] proposes a novel SDN-based secure IoT framework that can detect the vulnerabilities in IOT devices or malicious traffic generated by IoT devices using the session IP counter and IP Payload analysis. Security risks of IoT devices with respect to DDoS attacks is the main motivation of this paper. The proposed framework consists of three main modules :- the controller module, SINK module and IoT module. The framework uses two algorithms for DDoS attack detection; The first algorithm is based on packet frequency where every node that has sent/received packets is evaluated with exceeding threshold to time and the second algorithm recognizes the malicious packets on behalf of the packet payload size. Both these algorithms run an attack detection

module using a log file to monitor the DDoS attack in the SD-IoT network. The performance of the proposed framework was evaluated based on different attributes such as packet size, packet frequency, Burst mode Frequency and the utilization of the CPU and the system resources. With regards to the results and comparative analysis, the proposed framework detects DDoS attacks in the early stage with high accuracy and detection rate from 98% to 100%, having a low false-positive rate. To conclude, the framework has proven to be efficient due to its fast analysis and detection time.

Paper[18] proposes an SD-IoT based framework that provides security services to the IoT network. The proposed methodology helps to counteract with problems such as security risks with respect to DDoS attacks in an IoT network. In this paper, the proposed framework consists of 3 layers; the first layer consists of security applications that detects the attack, the second layer is the control layer and the third layer is the infrastructure layer. Moreover, the methodology also involves the creation of Counter based attack Detection application, setting up of the Sensor OpenFlow Switch and IoT node and building of the attack mitigation module. Both the algorithm and the framework were tested through different experiments and their overall performance was measured with respect to different factors such as, CPU utilization, Memory utilization ,SD-IoT Network Throughput , SDNWISE Controller Workload and Attack Detection Time. In conclusion, the proposed framework with the C-DAD application efficiently detects the DDoS attack by minimizing the time of attack detection with a tolerable impact on CPU and memory.

Paper[19] proposes a practical anomaly based intrusion Detection System(IDS) that is capable of timely detecting and mitigating DDoS attacks, especially the stealthy ones, which are challenging to detect

and mitigate due to their capability of bypassing traditional filters. Security risks faced by many IoT devices with respect to a new type of stealthy DDoS attack called Mongolian DDoS characterized by its widely distributed nature and small attack size from each source is one of the main motivations of the proposed solution in this paper. To start with, the proposed methodology is based on a statistical anomaly detection algorithm called Online Discrepancy Test(ODIT) that mitigates the attack with minimal interruption of regular services. A small modification has been proposed for this where its asymptotic optimality is proven in the minimax sense as the training data size grows. Moreover, the time and space complexity of the DDoS attacks have also been analyzed in this paper and a solution has also been provided to a dynamic scenario where the number of devices in the network tends to change. Further, a comprehensive performance evaluation was also conducted using testbed implementation. The performance of the proposed detection mitigation scheme was evaluated under challenging stealthy DDoS attack scenarios through real and simulated data, as well as on an IoT testbed.pap. Based on the results of the performance of the model, the proposed method was successfully able to mitigate the stealthy DDoS attacks.

(base)Paper[20] talks about the proposal of a lightweight architecture that distinguishes attack network flows from normal traffic and retaining its ability to obtain high detection accuracy using simple designs with low computational cost without affecting the performance of the network. Some of the proposed detection systems have become ineffective due to the Increasing variations of DDoS attacks and also, Some of the systems tend to be very complex, leading to high computational cost, thereby incurring high overload to the network being monitored. The proposed approach in this paper helps in solving these issues by building a lightweight architecture that helps to detect DDoS attacks. This is done by firstly fetching the required dataset, preprocessing it, applying Low Variance Filter Feature Selection

Technique for selecting the relevant features. With the help of these features, a Decision Tree model is constructed and trained using the Decision Tree algorithm. After this, the model is tested and its performance is evaluated using measures such as accuracy, precision, Misclassification Error Rate, Sensitivity, Specificity and F1-score. Based on the results obtained, it can be incurred that the proposed lightweight Decision Tree model with just 3 selected features is very effective and efficient in distinguishing the benign from DDoS attack network traffic flows with a detection accuracy of over 99%. Moreover, Analysis of the design and its performance reveals that using only 3 features consumes minimal load on the detection system's CPU while still maintaining high detection accuracy.

References

[1] M. He, Y. Huang, X. Wang, P. Wei and X. Wang, "A Lightweight and Efficient IoT Intrusion Detection Method Based on Feature Grouping," in IEEE Internet of Things Journal, vol. 11, no. 2, pp. 2935-2949, 15 Jan.15, 2024, doi: 10.1109/JIOT.2023.3294259.

[2] H. Al-Hamadi, I. -R. Chen, D. -C. Wang and M. Almashan, "Attack and Defense Strategies for Intrusion Detection in Autonomous Distributed IoT Systems," in IEEE Access, vol. 8, pp. 168994-169009, 2020, doi: 10.1109/ACCESS.2020.3023616.

[3] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020, doi: 10.1109/JIOT.2020.2993782.

[4] K. L. K. Sudheera, D. M. Divakaran, R. P. Singh and M. Gurusamy, "ADEPT: Detection and Identification of Correlated Attack Stages in IoT Networks," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6591-6607, 15 April15, 2021, doi: 10.1109/JIOT.2021.3055937.

[5] A. Singh and B. Sikdar, "Adversarial Attack and Defense Strategies for Deep-Learning-Based IoT Device Classification Techniques," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2602-2613, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3138541.

[6] Z. Bao, Y. Lin, S. Zhang, Z. Li and S. Mao, "Threat of Adversarial Attacks on DL-Based IoT Device Identification," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 9012-9024, 1 June1, 2022, doi: 10.1109/JIOT.2021.3120197.

[7] A. A. Elsaeidy, A. Jamalipour and K. S. Munasinghe, "A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart

City," in IEEE Access, vol. 9, pp. 154864-154875, 2021, doi: 10.1109/ACCESS.2021.3128701.

[8] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh and O. Jogunola, "Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3930-3944, 1 March1, 2022, doi: 10.1109/JIOT.2021.3100755.

[9] B. I. Hairab, M. Said Elsayed, A. D. Jurcut and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," in IEEE Access, vol. 10, pp. 98427-98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[10] F. Hussain et al., "A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks," in IEEE Access, vol. 9, pp. 163412-163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[11] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.

[12] V. A. Memos, K. E. Psannis and Z. Lv, "A Secure Network Model Against Bot Attacks in Edge-Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 11, pp. 7998-8006, Nov. 2022, doi: 10.1109/TII.2022.3162837.

[13] M. A. Elsadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach," in IEEE Access, vol. 11, pp. 83537-83552, 2023, doi: 10.1109/ACCESS.2023.3303113.

[14] Kamaldeep, M. Malik and M. Dutta, "Feature Engineering and Machine Learning Framework for DDoS Attack Detection in the Standardized Internet of Things," in IEEE Internet of Things Journal, vol.

10, no. 10, pp. 8658-8669, 15 May15, 2023, doi: 10.1109/JIOT.2023.3245153.

[15] W. I. Khedr, A. E. Gouda and E. R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," in IEEE Access, vol. 11, pp. 28934-28954, 2023, doi: 10.1109/ACCESS.2023.3260256.

[16] N. M. Yungaicela-Naula, C. Vargas-Rosales and J. A. Perez-Diaz, "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," in IEEE Access, vol. 9, pp. 108495-108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[17]J. Bhayo, R. Jafaq, A. Ahmed, S. Hameed and S. A. Shah, "A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN," in IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3612-3630, 1 March1, 2022, doi: 10.1109/JIOT.2021.3098029.

[18] J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.

[19] K. Doshi, Y. Yilmaz and S. Uludag, "Timely Detection and Mitigation of Stealthy DDoS Attacks Via IoT Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. 2164-2176, 1 Sept.-Oct. 2021, doi: 10.1109/TDSC.2021.3049942.

[20]G. Lucky, F. Jjunju and A. Marshall, "A Lightweight Decision-Tree Algorithm for detecting DDoS flooding attacks," 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 2020, pp. 382-389, doi: 10.1109/QRS-C51114.2020.00072.