|  |
| --- |
| Article1:  *Detecting DDoS attacks in Software Defined Networks Through Feature Selection Methods and Machine Learning Models*   * Goal:   *Detecting DDoS attacks in SDN using Machine Learning based models*   * Data source:   *Generated using “hping3” packet generator in virtual machines.*   * Dataset:   *12 features and 129,000 attributes*   * Feature Engineering Techniques:   *Filter, Embedded and Wrapper methods*   * Machine Learning Algorithm:   *Support Vector Machine, Naïve Bayes, Artificial Neural Network, K-Nearest Neighbors*   * Result:   *Dataset selected with wrapper feature selection method with KNN classifier achieved the highest accuracy rate of ~ 98%.*   * Validation Techniques:   *Receiver Operating Characteristic (ROC), K-fold cross validation*   * Conclusion:   *With 97.7% sensitivity KNN classifier can detect a DDOS attack by lightening the burden of the controller.* |
| Article 2:  *Smart Detection: An Online Approach for DoS/DDoS Attack*  *Detection Using Machine Learning*   * Goal:   *Detecting and combat DDOS attack on the internet in a modern collaborative way.*   * Data source:   [*https://www.unb.ca/cic/datasets/ids-2017.html*](https://www.unb.ca/cic/datasets/ids-2017.html)   * Dataset:      * Feature Engineering Techniques   *Recursive Feature Elimination with cross validation*   * Machine Learning Algorithm   *Random Forest, Decision Tree, Logistic Regression, Stochastic Gradient Descent, Perceptron, AdaBoost*   * Result   *Random forest algorithm showed the highest accuracy of 99.94% with 20 features.*   * Validation Techniques   *10 - fold* *Cross validation*   * Conclusion   *Random forest tree algorithm showed the highest accuracy of greater than 93%.* |
| Article 3:  *Analysis & Detection of DDOS attacks using ML Techniques.*   * Goal:   *Classifying whether it was DDOS Attack 0r Benign.*   * Data source:   [*https://www.unb.ca/cic/datasets/ddos-2019.html*](https://www.unb.ca/cic/datasets/ddos-2019.html)   * Dataset:   *88 Attributes*   * Feature Engineering Techniques:   *One-Hot Encoding, Dimensionality Reduction*   * Machine Learning Algorithm:   *Decision Tree, Linear Support Vector Machine*   * Result:   *Decision Tree performs well than SVM Models with better accuracy.*   * Validation Techniques:   *K-Fold Cross Validation. Where, K=5*   * Conclusion:   *The results of ML Models, which included decision tree and linear support vector machine models, demonstrated that DDOS and Benign attacks were classified where the accuracy rates of around 100% were achieved.* |
| Article 4:  *ML DDOS Detection Using Stochastic Gradient Boosting*   * Goal:   *Classifying whether it was DDOS Attack 0r Benign*   * Data source:   [*https://www.kaggle.com/devendra416/ddos-datasets*](https://www.kaggle.com/devendra416/ddos-datasets)   * Dataset:   *170 Attributes (2 Files: Balanced Data, Unbalanced Data)*   * Feature Engineering Techniques:   *Dimensionality Reduction*   * Machine Learning Algorithm:   *Decision Tree, KNN, Naïve Bayes, Random Forest, SG Boost*   * Result:   *SGB accuracy was better compared to other ML Algorithms implemented*   * Validation Techniques:   *K-Fold Cross Validation. Where, K=10*   * Conclusion:   *All ML models used were trained & tested both on Balanced & Unbalanced dataset. SGBoost had better accuracy than other ML Models.* |