GROUP NO: 02

INTRUSION DETECTION IN COMPUTER NETWORKS USING ML ALGORITHMS

Department of Computer Science and AI Engineering,
Amrita Vishwa Vidyapeetham,
Amritapuri Campus, Kollam.

Adithya R	- AM.EN.U4AIE20005
Advaith AJ	- AM.EN.U4AIE20006
G Sabarinath	- AM.EN.U4AIE20026 (P)
Tharun S Kumar	- AM.EN.U4AIE20071

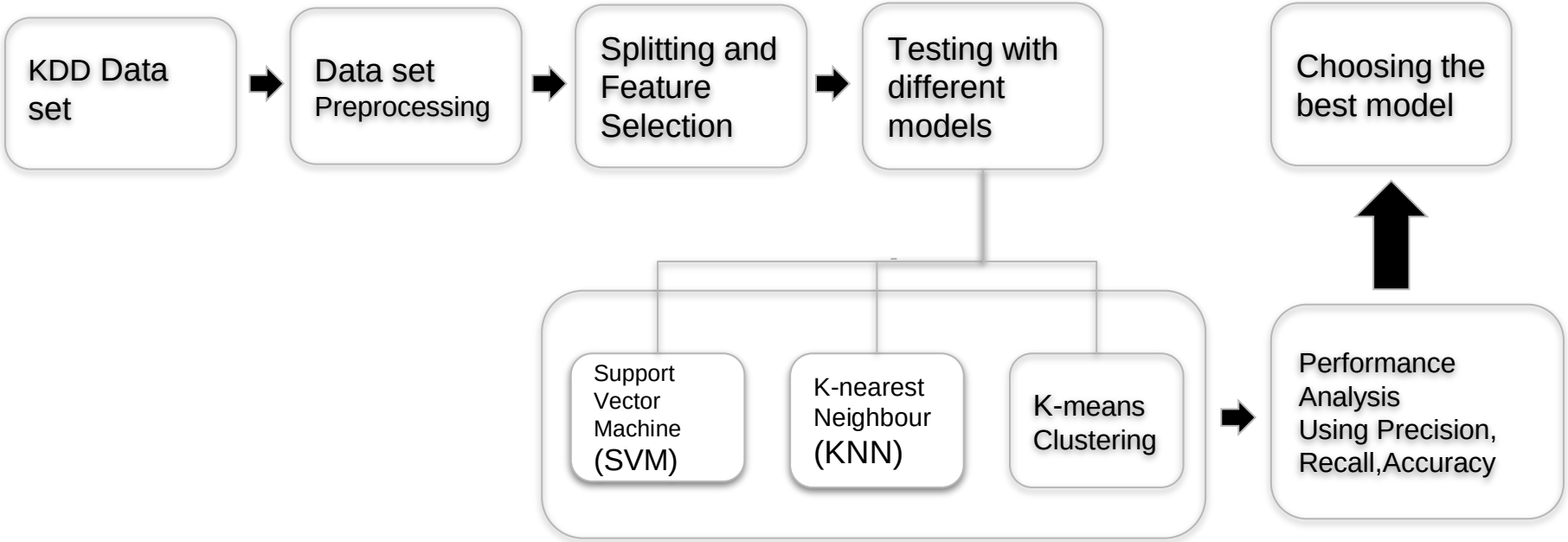
Project Guide :

Dr. Gopakumar G, Asst. Professor(Sl. Gr.),
Dept. of Computer Science and Engineering

Objective

The objective of the project is to make a performance analysis of following algorithms: KNN, k-means clustering and SVM on intrusion detection.

Methods


KDD Data set
Data set Preprocessing
Splitting and Feature Selection
Testing with different models
Choosing the best model
Support Vector Machine (SVM)
K-nearest Neighbour (KNN)
K-means Clustering
Performance Analysis Using Precision, Recall,Accuracy

Result and Discussion

Algorithm	Accuracy(%)			
	Binary Class		Multi-class	
	Train	Test	Train	Test
KNN	95.94	91.67	94.19	90.40
SVM	96.01	94.39	95.91	93.24

Algorithm	Accuracy(%)	
	Train	Test
K-Means Clustering	70.08	70.84

No. of Features : 42

Data Filtering : Label Encoding, Interpolation, Normalization

Feature Selection : PCA (15 comp.)

Performance analysis of ML algorithms for intrusion detection on KDD CUP 99 dataset is done for both binary and multiclass attacks, and found that SVM algorithm performs better compared to KNN and K- Means Clustering.

Reference List

1. Z. Xiaofeng, H. Xiaohong, “Research on Intrusion Detection Based on Improved Combination of K-means and Multi-level SVM”, International Conference on Communication Technology, IEEE (2017)
2. J. Jha , L.Ragha, “Intrusion Detection System using Support Vector Machine “in International Conference & workshop on Advanced Computing ,ICWAC,IEEE(2013).
3. K. Ghanem, F. J. Aparicio-Navarro, K. G. Kyriakopoulos, S. Lambotharan, J. A. Chambers, “Support Vector Machine for Network Intrusion and Cyber-Attack Detection” in Sensor Signal Processing for Defence Conference (SSPD), IEEE,2017.
4. “An Anomaly Detection Model based on One-class SVM to Detect Network Intrusion”, M. Zhang, B. Xu, J. Gong, 11th International Conference on Mobile Ad-hoc and Sensor Networks(2015).
5. S. D. D. Anton, S. Sinha, H. D. Schotten, “Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forest.” in: 27th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2019.
6. M. K. Siddiqui, S. Naahid, “Analysis of KDDCUP99 Dataset using Clustering based Data Mining ”, International Journal of Database Theory and Application. 2013
7. K. A. A. Nazeer, M. P. Sebastian, “Improving the Accuracy and Efficiency of the k-means Clustering Algorithm”, Proceedings of the World Congress on Engineering,2009