**Network intrusion detection system based on recursive feature addition and bigram technique**

In this paper, [Tarfa Hamed](https://www.sciencedirect.com/science/article/pii/S0167404817302274#!), [Rozita Dara](https://www.sciencedirect.com/science/article/pii/S0167404817302274#!) [Stefan and C.Kremer](https://www.sciencedirect.com/science/article/pii/S0167404817302274#!) have proposed a NIDS (Network Intrusion Detection System) which is based on a feature selection method called Recursive Feature Addition (RFA) and bigram technique. They tested the model on the ISCX 2012 data set. Moreover they have proposed a bigram technique to encode payload string features into a useful representation that can be used in feature selection. They have also proposed a new evaluation metric called that combines accuracy, detection rate and false alarm rate in a way that helps in comparing different systems and selecting the best among them[1].

# Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines

In this paper, [SetarehRoshan](https://www.sciencedirect.com/science/article/pii/S0016003217302995#!) ,[YoanMiche,](https://www.sciencedirect.com/science/article/pii/S0016003217302995" \l "!) [AntonAkusok](https://www.sciencedirect.com/science/article/pii/S0016003217302995#!) and [AmauryLendasse](https://www.sciencedirect.com/science/article/pii/S0016003217302995#!) have proposed a new intrusion detection system and addressed the problem of adaptability in the field of intrusion detection.The proposed IDS is an adaptive solution which provides the capability of detecting known and novel attacks as well as being updated according to the new input from human experts in a cost-effective manner[2].

**Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning**

This paper deals with the evaluation and statistical analysis of labelled flow based CIDDS-001 dataset used for evaluating Anomaly based (NIDS) Network Intrusion Detection Systems . They basically used two techniques, k-means clustering and k-nearest neighbour classification to measure the complexity in terms of prominent metrics. On the basis of evaluation they concluded that both k-means clustering k-nearest neighbour classification perform well over CIDDS-001 datset in terms of used prominent metrics. Hence the dataset can be used for the evaluation of Anomaly based Network Intrusion Detection Systems[3].

REFERENCES

[1]” Network intrusion detection system based on recursive feature addition and bigram technique” [TarfaHamed](https://www.sciencedirect.com/science/article/pii/S0167404817302274#!)[RozitaDara](https://www.sciencedirect.com/science/article/pii/S0167404817302274" \l "!)[Stefan C.Kremer](https://www.sciencedirect.com/science/article/pii/S0167404817302274" \l "!) School of Computer Science, University of Guelph, Guelph, ON, Canada.

# [2] “Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines” [SetarehRoshan](https://www.sciencedirect.com/science/article/pii/S0016003217302995" \l "!) [YoanMiche](https://www.sciencedirect.com/science/article/pii/S0016003217302995" \l "!) [AntonAkusok](https://www.sciencedirect.com/science/article/pii/S0016003217302995" \l "!) [AmauryLendasse](https://www.sciencedirect.com/science/article/pii/S0016003217302995#!)

[3]” Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning” [AbhishekVerma](https://www.sciencedirect.com/science/article/pii/S1877050917328594" \l "!) [VirenderRanga](https://www.sciencedirect.com/science/article/pii/S1877050917328594" \l "!) Department of Computer Engineering, NIT Kurukshetra, India.

# Decision table

# Decision tables are a brief visual representation which on a basis of given conditions  specifies which actions to perform. They are [algorithms](https://en.wikipedia.org/wiki/Algorithm) whose output is a set of actions. The information that are given in decision tables could also be represented in a [programming language](https://en.wikipedia.org/wiki/Programming_language) as a series of  [switch-case](https://en.wikipedia.org/wiki/Switch_statement) and [if-then-else](https://en.wikipedia.org/wiki/Conditional_(programming)) statements or as [decision trees](https://en.wikipedia.org/wiki/Decision_tree).

Each decision resembles to a relation, predicate or variable whose possible values are given among the condition alternatives. The data given in the table specify whether (or in what order) the action is to be performed and each action is a procedure or operation to perform,for the set of condition alternatives the data corresponds to.

many decision tables include in their condition alternatives a [don't care](https://en.wikipedia.org/wiki/Don%27t-care_term) symbol. This can be a blank or hyphen,to make them more brief.

If the decision tree includes every possible combination of input variables then table is considered balancedor complete.

**K Nearest Neighbour**

In [pattern detection](https://en.wikipedia.org/wiki/Pattern_recognition), the ***k*-nearest neighbors algorithm** (***k*-NN**) is a [non-parametric](https://en.wikipedia.org/wiki/Non-parametric_statistics) method that is used for both [regression](https://en.wikipedia.org/wiki/Regression_analysis) and classification predictive problems. Moreover, it is more broadly used in classification problems than regression problems in the industry. To calculate any method we generally look at 3 important steps:

1. Calculation time

2. Ease to interpret output

3. Predictive Power

It is one of the most simplest of all [machine learning](https://en.wikipedia.org/wiki/Machine_learning) algorithms.

Both for classification and regression, a useful technique can be to assign weight to the contributions of the neighbors, so that the nearer neighbours contribute more to the average than the more distant ones.

.

A speaciality of the *k*-NN algorithm is that it is sensitive to the local structure of the data.