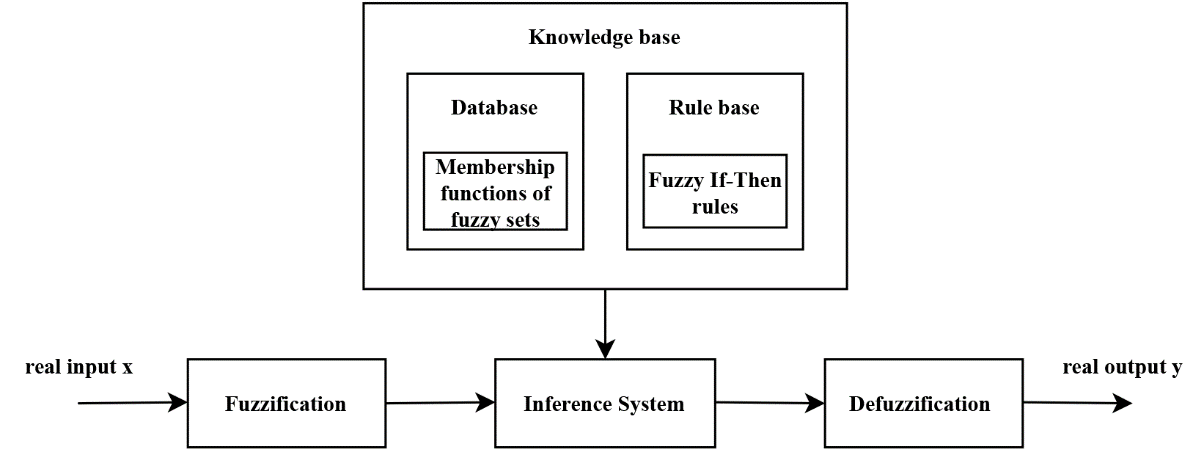
FIS

Fuzzy logic has been applied in various field, from Control Theory to Artificial Intelligence. Fuzzy logic is an extension of Boolean logic which aim to handle problems with approximate solutions instead of fixed or exact solutions. Fuzzy inference system (FIS) is an importance part in Fuzzy logic, which takes the responsibility of making decisions. A FIS model has 4 main components: Fuzzification, Knowledge Base, Fuzzy Inference and Defuzzification, as we can see in Fig 1.



Fuzzification is the first mathematical procedure of the system. It transforms crisp input into fuzzy input with the help of pre-defined membership functions and fuzzy sets. A Knowledge Base consists of a rule base which contain fuzzy If-Then rules and a data base which has the membership functions. Fuzzy Inference can be seen as a mapping mechanism, it maps a fuzzy input to a corresponding fuzzy output using membership functions, logical operations and If-Then rules in the rule base. The degree of membership of fuzzy output is determined based on degree of membership of inputs and the relationship between input sets. Defuzzification is a process which convert fuzzy sets from fuzzy inference to crisp output. In fuzzy system with multiple output variables, this process is implemented independently in similar ways. There are many defuzzification methods and in this research, we used the Centroid method

TLBO

The population-based heuristic can be classified into two groups: evolutionary algorithms (EA) and swarm intelligence (SI) based algorithms. Both of them are probabilistic algorithms and require common controlling parameters like population size, number of generations, elite size, etc. Furthermore, along with these common parameters, different algorithms require their own algorithm-specific control parameters which are very crucial factors that affects the performance of the algorithms. However, more parameters may increase the computational effort. In 2011, teaching-learning-based optimization (TLBO) algorithm was introduced by Rao et al which does not require any algorithm-specific parameters. This algorithm mimics the teaching-learning process and is based on the influence of a teacher on the output of learners in a class. In TLBO algorithm a group of learners is considered as population and different subjects offered to the learners are considered as different design variables of the optimization problem and a learner’s result can be seen as the ‘fitness’ value of the optimization problem.

The algorithm has two phases:

1) Teacher phase: All the students learn from teacher and gain knowledge. The best solution (student with maximum fitness value) in the entire population is considered as the teacher. The equation for generating new solution can be expressed as:

 (1)

Where: r is a random number in range [0,1]

 is the teaching factor and is either 1 or 2

is the solution with maximum fitness value (teacher)

is the mean of all students in the class

 is the new solution (If  is better than then replace with )

2) Learner phase: In this phase, each student in the class chooses a random partner () then interact and exchange their knowledge. New generation can be generated using these equations:





Where:  is the partner solution

 is the fitness value of solution 

 is the fitness value of partner solution 

Similar to the previous phase,  will replace is it has higher fitness value.

DATA PROCESSING

Firstly, local network features such as Stream IDs, source IP addresses, destination IP addresses, and timestamps have been removed from all data sets. NaN values in the dataset are replaced with a value of 0. Next, in order to eliminate large values and speed up the calculation, input feature columns are normalized within a range from -1 to 1. The feature columns of the entire dataset are encoded so that each type in each column represented by a number. With the missing data, we use the mean value of each attack type related to that feature. This means the missing values in a feature column are replaced with the average value corresponding to 16 attack types and attack types of the same kind have values close to the feature's average value. Finally, we extracted the data samples whose labels are Normal, Attack, C&C, C&C-HeartBeat and DDoS and encoded these labels into integer values [0, 1, 2, 3, 4] respectively.