**MODULES:**

There are three modules can be divided here for this project they are listed as below

* Upload dataset
* Manual Adding data
* Classifying Attacks
* Graphical Representation

From the above three modules, project is implemented. Bag of discriminative words are achieved

**MODULE DESCRIPTION:**

1. **UPLOAD DATASET**

Users search the any link notably, not all network traffic data generated by malicious apps correspond to malicious traffic. Many malware take the form of repackaged benign apps; thus, malware can also contain the basic functions of a benign app. Subsequently, the network traffic they generate can be characterized by mixed benign and malicious network traffic. This dataset is upload.

1. **MANUAL ADDING DATA**

User handling for some various times of smart phones ,desktops laptops and tablets .If any kind of devices attacks for some unauthorized malware softwares.In this malware on threats for user personal dates includes for personal contact, bank account numbers and any kind of personal documents are hacking in possible. So add the network data in manualy.

1. **CLASSIFYING ATTACKS**

Here, we compare the classification performance of SVM with other popular machine learning algorithms. We have selected several popular classification algorithms. For all algorithms, we attempt to use multiple sets of parameters to maximize the performance of each algorithm. Using SVM algorithms classification for malware bag-of-words weightage.

1. **GRAPHICAL REPRESENTATION**

The main part of the project is to analysis the attack types in the network dataset. The user data analysis of the data can be done by charts format. This is the place where admin have ability to come for particular solution about proposed system. The pictorial representations of collected data are shown in the form of graphs. The different graphs give the best analysis of the system.