Chapter 7

RESULTS

The screenshots of the Naive Bayes Classifier and the accuracy results of the designed system are outlined below.

7.1 Screenshots

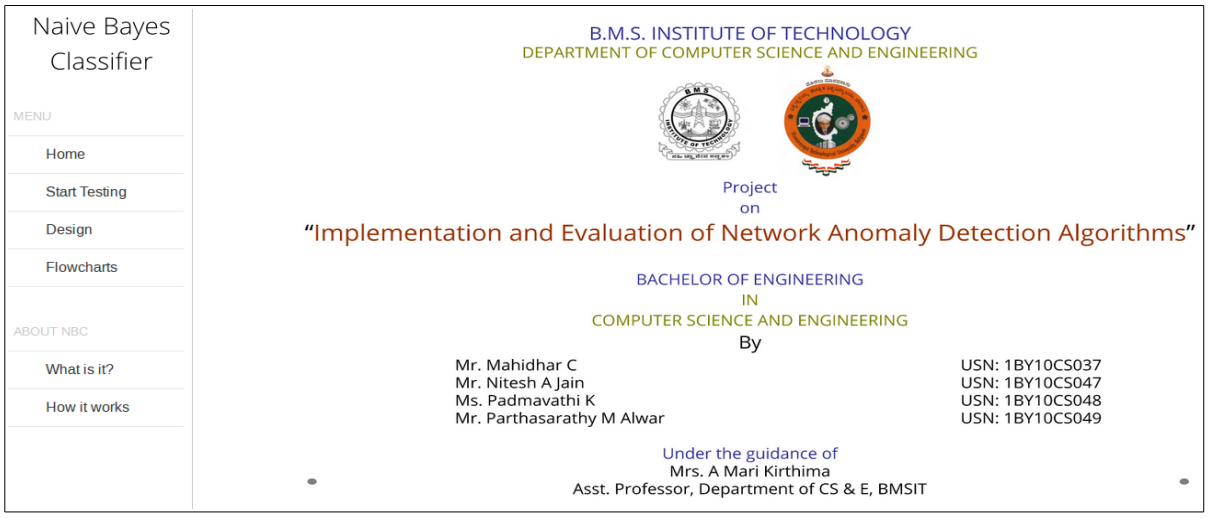

Figure 7.1 Home Page

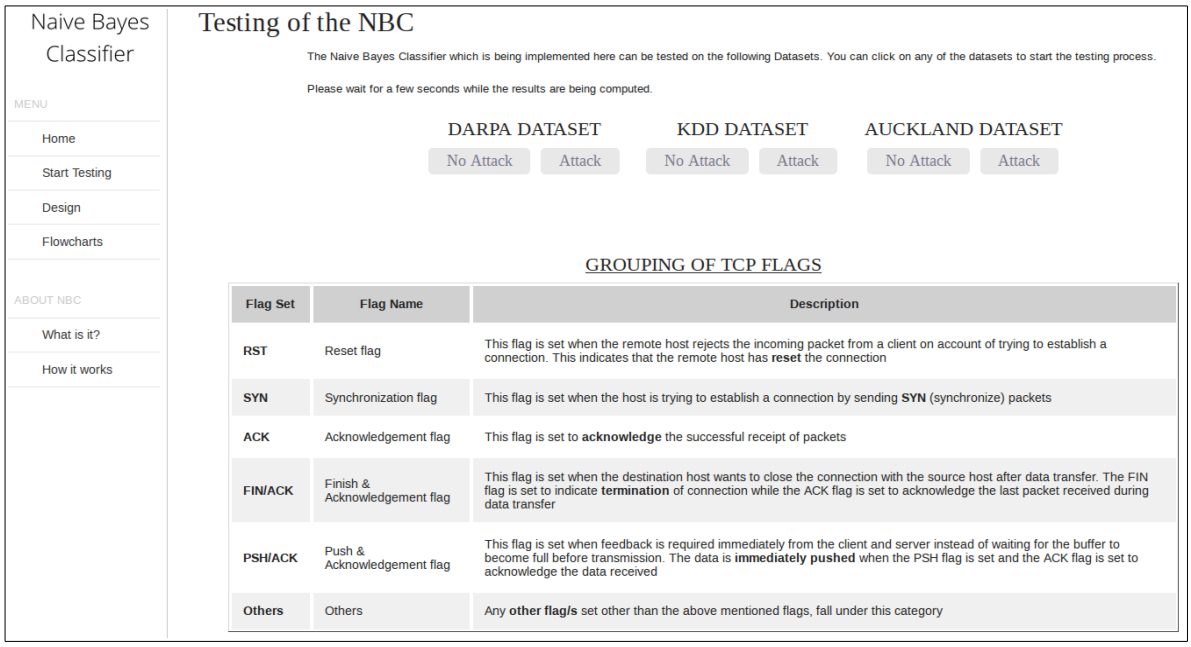

Figure 7.2 Testing Page

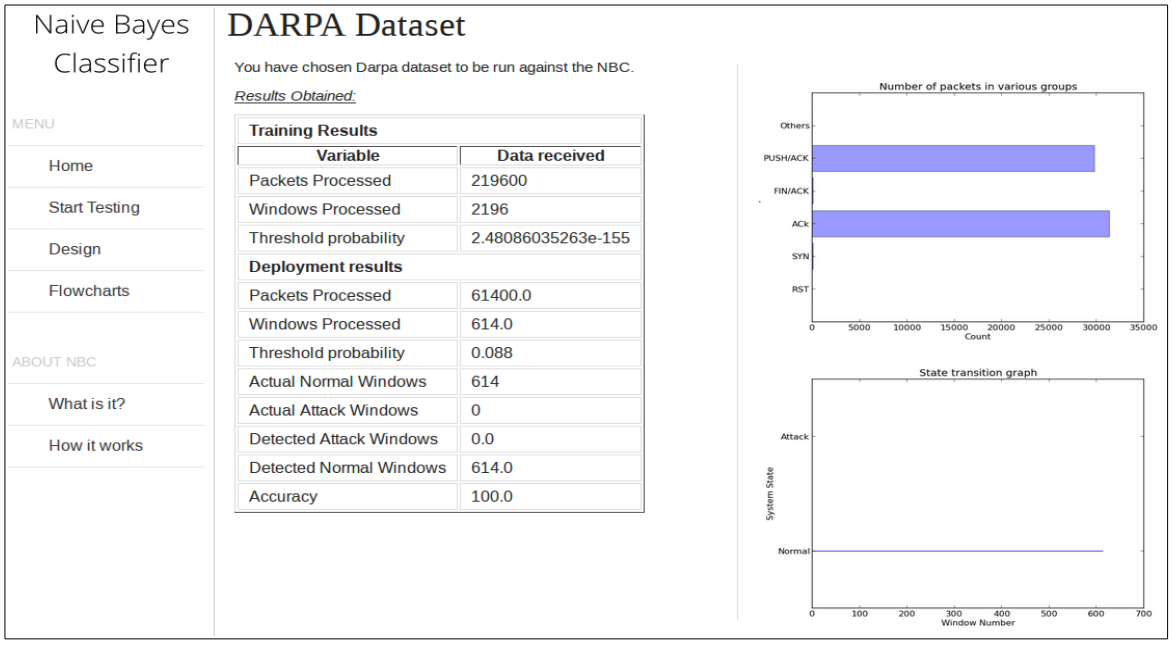

Figure 7.3 DARPA No Attack Results

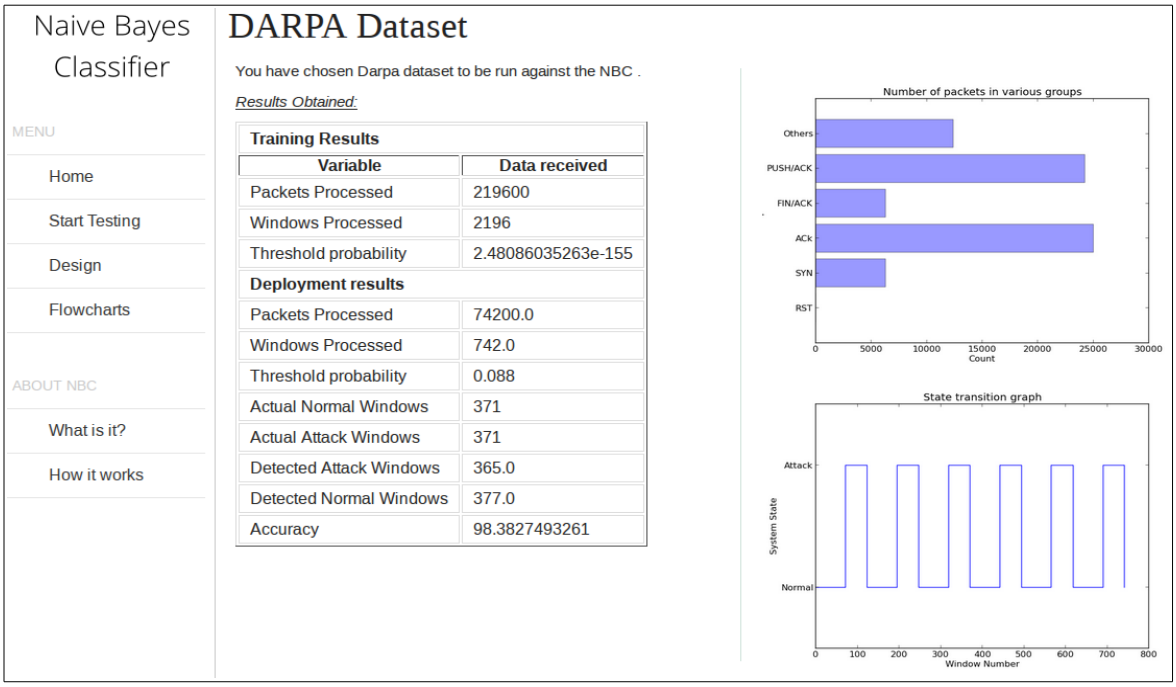

Figure 7.4 DARPA Attack Results

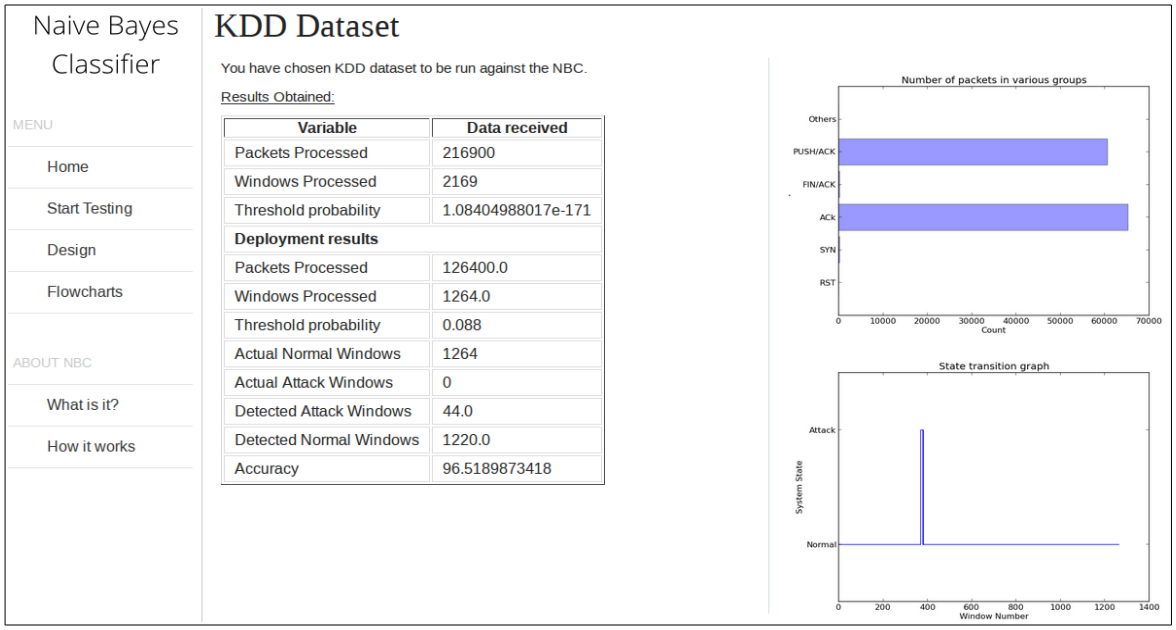

Figure 7.5 KDD No Attack Results

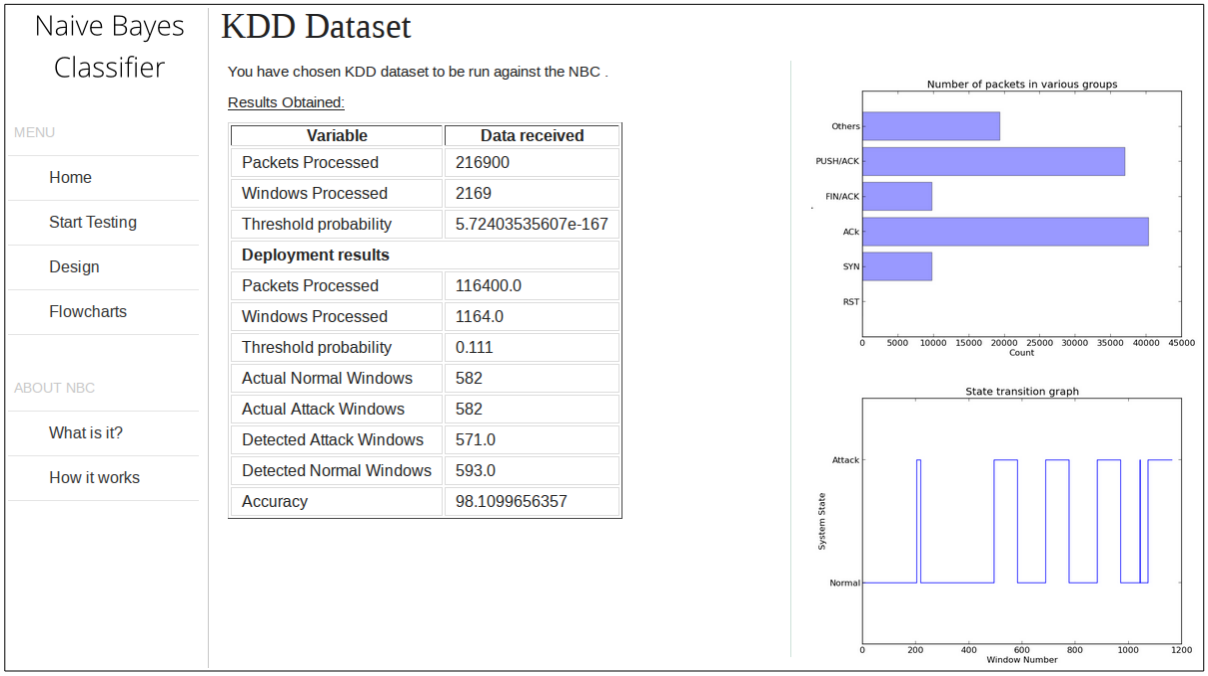

Figure 7.6 KDD Attack Results

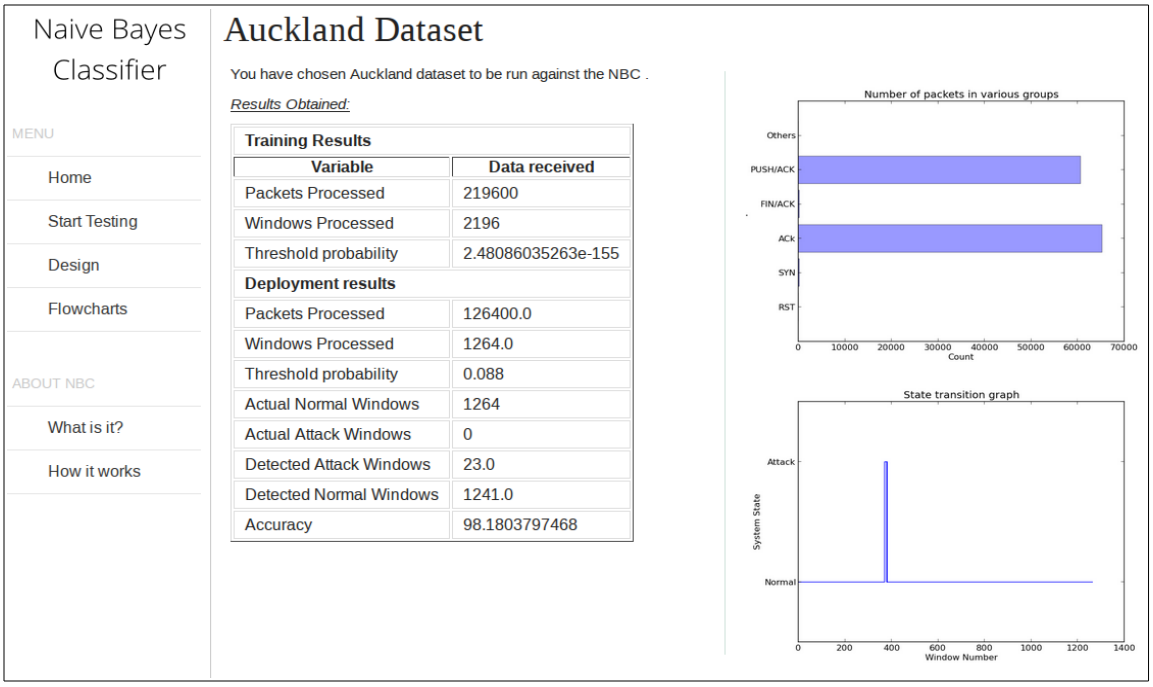

Figure 7.7 Auckland No Attack Results

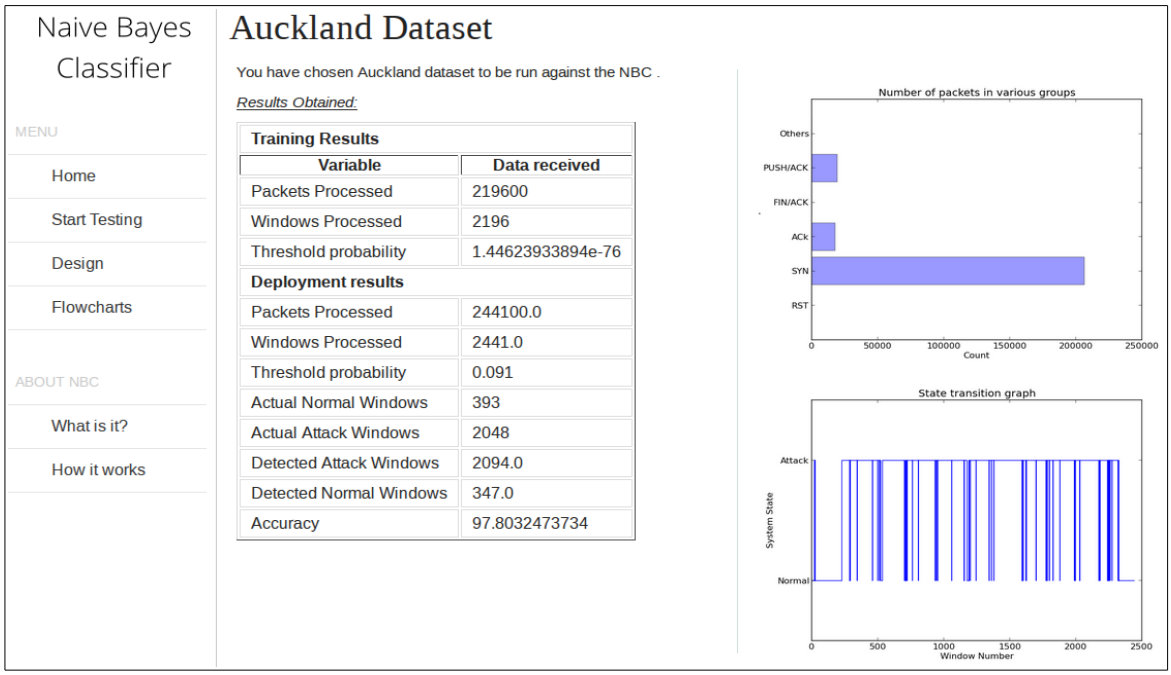

Figure 7.8 Auckland Attack Results

The different screenshots are explained in this section.

Figure 7.1 shows the first page when the application is started. This is the main page for navigating to different pages like testing, design considerations, flowcharts etc. The menu can be found on the left hand side using which the user can navigate the application pages.

Figure 7.2 shows the testing page. The Naive Bayes Classifier is tested against the different datasets like DARPA, KDD and Auckland. All the three datasets contain options to run the system against a clean dataset and an attack dataset. The **"No Attack"** dataset consists of **clean** traffic used for training the classifier. The **"Attack"** dataset consists of **mixed** traffic consisting of clean traffic and attack traffic.

Figures 7.3 to 7.8 are screenshots depicting the results obtained for the DARPA, KDD and the Auckland datasets. The result page of each dataset consists of a state graph which shows the transition from **Normal State** to **Attack State** based on the incoming traffic. Also, it contains various information about the threshold probability, number of packets processed, number of attack windows detected along with various performance parameters.

7.2 Results Obtained

The Naive Bayes classifier was tested against the DARPA, KDD and Auckland -II datasets. The formula to calculate the accuracy is as follows

$$Accuracy = \frac{TP + TN}{P + N}$$

where,

TP - True Positives

TN - True Negatives

P - Number of Attack Windows

N - Number of Normal Windows

Using the above formula the accuracies for each dataset are as follows in table 7.1:

Dataset	Accuracy
DARPA	
No Attack	100%
Attack	98.38%
KDD	
No Attack	96.52%
Attack	98.11%
Auckland	
No Attack	98.18%
Attack	97.80%

Table 7.1 Results for various datasets

The window statistics of each dataset is as given in table 7.2. Each window consists of one hundred packets in this implementation. Each dataset had two types of traffic – **Clean** traffic and **Mixed** traffic. The clean traffic has no attacks whereas the mixed traffic has both clean and attack packets. The training data consists of only clean traffic, in order to build the normal profile required to detect the anomalies.

		Actual Window Count		**Detected Window Count**	
		Normal Windows	Attack Windows	Normal Windows	Attack Windows
DARPA	Train File	2196	0	NA	NA
	No Attack File	614	0	607	7
	Attack File	371	371	371	371
KDD	Train File	2169	0	NA	NA
	No Attack File	1264	0	1210	54
	Attack File	582	582	550	614
Auckland	Train File	2196	0	NA	NA
	No Attack File	1264	0	1241	23
	Attack File	393	2048	347	2094

Table 7.2 Window statistics of the datasets used