SUMMARY

Computer security can be implemented by various methodologies. The question arises whether these methodologies are sufficient enough to provide better security to the computer system. The proposed approaches in this thesis (1) security by decision tree, (2) security by artificial neural network and (3) security by genetic algorithm; are better than the existing methodologies.

These proposed approaches work on the process level, hence other existing approaches (like antivirus tools) also work within the system. If any antivirus cannot identify any virus in the computer system, the operating system of the computer system executes the virus and creates its processes. Then our proposed approaches will identify these virus’s processes as non-self processes and user can take action against these non-self processes.

Since the existing security tools need regular monitoring and updating there is no need for regular monitoring and updating with the existing approaches. A new training data and test data set can be used for updating the structure of decision tree, for updating of weight of artificial neural network. For genetic approach the population of detectors can be replaced by generating new offspring with the help of the detectors who identify most non-self processes.

At last, we can say that the computer security by using the concept of computer immunology, artificial immune system, soft computing and machine learning play an important role. By using these concepts, we can get better security, which cannot be achieved by the existing security tools.