Recent work adopts a wide range of Artificial Intelligence techniques in Intrusion Detection Systems. Another domain of research in this paradigm is Data Mining that offers flexibility and has been a focus of research in the recent years. Intrusion detection can be automated by making the system learn using classifiers/clusters from a training set. A benefit of Machine Learning is that the techniques are capable of generalizing from known attacks to variations, or even can detect new types of intrusion. Recent research focuses more on the hybridization of techniques to improve the detection rates of Machine Learning classifiers. Artificial Neural Networks and Decision Trees have been applied to develop Intrusion Detection Systems and have become popular. Several evaluations performed to date indicate that Intrusion Detection Systems are moderately successful in identifying known intrusions and quite a bit worse at identifying those that have not been seen before. This provides a prospect area for research and commercial communities to design Intrusion Detection Systems.

The research work presented in this thesis models the Intrusion Detection System by ensemble approach using Outlier Detection, Change Point and Relevance Vector Machines. The current new hybrid detection model developed combines the individual base classifiers and Machine Learning paradigms to maximize detection accuracy and minimize computational complexity. Results illustrate that the proposed hybrid systems provide more accurate detection rate. Real time dataset is used in the experiments to demonstrate that Relevance Vector Machines can greatly improve the classification accuracy and the approach achieves higher detection rate with low false alarm rates and is scalable for large datasets, resulting in an effective Intrusion Detection System.

We first introduce the Single Layer Feedforward Network as the core intrusion detector. This can be used to build a scalable and efficient network Intrusion Detection Systems which are accurate in attack detection. Experimental
results further demonstrate that our system is robust and is better than other systems such as the Decision Trees and the Naive Bayes. We then introduce a logging framework for network data collection and perform modeling using Change Point and Outlier Detection to build real time Intrusion Detection System. Experimental results performed on data sets collected in real time confirm that Change Point and Outlier Detection algorithms are particularly well suited to detect attacks. Experiments were also conducted with Support Vector Machines and compared performance of the Decision Trees with this model.

In my research work a new method for developing Intrusion Detection System using Relevance Vector Machine is implemented. Compared with other classifier algorithms, Relevance Vector Machine has the advantage of utilizing the sparseness and reduces the false alarms while still maintaining desirable detection rate.