CHAPTER 8
CONCLUSION AND FUTURE WORK

The primary objective of the proposed methods finds out the different types of attacks using SVM based intrusion detection system. Three different methods are proposed here to find out the attacks Probe, DoS, U2R, R2L and they were tested for performance metrics detection rate of attacks, false alarm rate of attacks and accuracy. Two databases namely, KDD Cup’99 and NSL-KDD datasets were used during experimentation.

This research work proposes three different methods to find out the malicious behaviors in the networks. They are

- Kernelized Support Vector Machines (KSVM)
- Granular Support Vector Machines (GSVM)
- GSVM-Repetitive Under Sampling (GSVM-RU)

8.1 FINDINGS OF THE STUDY

From the experimental results the following interpretations were arrived:

- With both the datasets, the maximum accuracy was produced by the GSVM-RU method. GSVM stood second and the KSVM produced the least accuracy for both the KDD Cup’99 and NSL-KDD datasets.
- The fastest algorithm among the three proposed methods was GSVM-RU method and the slowest was the KSVM method.
- While comparing the methods for DoS attacks, GSVM-RU method produced the highest accuracy for both the datasets, which is 1% increase when compared with GSVM method and 4% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99
dataset, GSVM-RU is 2% increases than GSVM and 3.4% increases than KSVM.

- While comparing the proposed methods for probe attacks, GSVM-RU method produced the highest accuracy for both the datasets, which is 3.5% increase when compared with GSVM method and 5.5% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 1.9% increases than GSVM and 4.9% increases than KSVM.

- While comparing the proposed methods for U2R attacks, GSVM-RU method produced the highest accuracy for both the datasets, which is 3.3% increase when compared with GSVM method and 4% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 3.3% increases than GSVM and 6% increases than KSVM.

- While comparing the proposed methods for R2L attacks, GSVM-RU method produced the highest accuracy for both the datasets, which is 3.5% increase when compared with GSVM method and 5.5% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 1.5% increases than GSVM and 7.5% increases than KSVM.

- With both the datasets, the maximum Detection Rate of Attacks was produced by the GSVM-RU method. GSVM stood second and the KSVM produced the least Detection Rate of Attacks for both the KDD Cup’99 and NSL-KDD datasets.

- While comparing the methods for DoS attacks, GSVM-RU method produced the higher Detection Rate for both the datasets, which is 3.9% increase when compared with GSVM method and 3% increase
when compared with KSVM for DoS attacks of NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 2.1% increases than GSVM and 5.1% increases than KSVM.

- While comparing the proposed methods for probe attacks, GSVM-RU method produced the higher Detection Rate for both the datasets, which is 2% increase when compared with GSVM method and 2.3% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 2.3% increases than GSVM and 3.4% increases than KSVM.

- While comparing the proposed methods for U2R attacks, GSVM-RU method produced the higher Detection Rate for both the datasets, which is 1.9% increase when compared with GSVM method and 3.5% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 3.7% increases than GSVM and 3.1% increases than KSVM.

- While comparing the proposed methods for R2L attacks, GSVM-RU method produced the higher Detection Rate of Attacks for both the datasets, which is 2% increase when compared with GSVM method and 4.7% increase when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 1.9% increases than GSVM and 4.5% increases than KSVM.

- With both the datasets, the minimum False Alarm Rate was produced by the GSVM-RU method. KSVM stood second and the GSVM produced the higher False Alarm Rate for both the KDD Cup’99 and NSL-KDD datasets.

- While comparing the methods for DoS attacks, GSVM-RU method produced the lowest False Alarm Rate for both the datasets, which is
0.07% decrease when compared with GSVM method and 0.1% decrease when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 0.22% decreases than GSVM and 0.1% decreases than KSVM.

- While comparing the proposed methods for probe attacks, GSVM-RU method produced the lowest False Alarm Rate for both the datasets, which is 0.04% decrease when compared with GSVM method and 0.16% decrease when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 0.07% decreases than GSVM and same as KSVM.

- While comparing the proposed methods for U2R attacks, GSVM-RU method produced the lowest False Alarm Rate for both the datasets, which is 0.01% decrease when compared with GSVM method and 0.25% decrease when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 0.06% decreases than GSVM and 0.16% decreases than KSVM.

- While comparing the proposed methods for R2L attacks, GSVM-RU method produced the lowest False Alarm Rate for both the datasets, which is 0.06% decrease when compared with GSVM method and 0.31% decrease when compared with KSVM for NSL-KDD dataset. For KDD Cup’99 dataset, GSVM-RU is 0.03% decreases than GSVM and 0.3% decreases than KSVM.

- Thus the proposed methods produce less False Alarm Rate, high accuracy and reliable intrusion detection results and prove that they are the best when compared to the traditional SVM method.
8.2 CONCLUSION

For the security and trust of a computer system, intrusion detection system is used which helps to detect several types of malicious behaviors in it. In this work, three different support vector machines based intrusion detection methods are proposed to find out the attacks types in the networks. The attacks are classified using SVM technique. The performance of the modified classification methods KSVM, GSVM and GSVM-RU is tested for the metrics detection rate of attacks, false alarm rate and accuracy using the datasets KDD Cup’99 and NSL-KDD dataset.

At first the SVM is kernelized by the Gaussian radial basis kernel function. The modified training sets are formed by resampling from original training set; classifiers are constructed using these training sets and then combined. This gives better result when compared with traditional SVM approach.

Then next approach is designed by using the principles of granular computing. This granular computing based learning framework called Granular Support Vector Machines (GSVM) extracts a sequence of information granules and then builds support vectors on some of these granules if necessary. The GSVM based intrusion detection will speed up classification process by eliminating redundant data locally. The performance of the GVSM is compared with traditional SVM approach.

Finally the Granular Support Vector is modified by using Repetitive Under sampling with it. The RU is effective as it can minimize the negative effect of information loss while maximizing the positive effect of data cleaning in the under sampling process. GSVM-RU is efficient by extracting much less support vectors, and hence greatly speeding up SVM prediction. This is best in terms of both effectiveness and efficiency for the intrusion detection of attacks in networks.
8.3 FUTURE WORK

This approach for intrusion detection can be further extended towards investigating the classification process for any other high dimensional and imbalanced datasets. The detection of attacks is performed only for four attacks here but other new types of attacks can also be included in the dataset. It is essential for researchers to improve their network based intrusion detection system to be able to detect stealthy attacks in better manner, or combination with host based methods also be extended. And some intrusion prevention techniques are also to be developed and added with the proposed system.