Experimental Analysis of Data Mining Application for Intrusion Detection with Feature reduction

Abstract:

Using Internet is increasing day by day. This tremendous growth of using internet and relying more on network information, network security is now becoming one of the great challenge in modern world. As Internet information are more open than ever before, there may increase risks associated with network attacks. To access this information from internet, several types of user visit the network. Some of them are normal and some are anomaly such as firewall. Network security becomes essential for these anomalies. Records made available by the Pentagon show that they logged over 79,000 attempted intrusions in 2005 with about 1,300 successful ones. Once, most of all depended on handcrafted signatures just like anti-viruses. But there have number of drawbacks for signatures system.

Existing System:

We presented a new data-mining based technique for intrusion detection using Decision table classifier with feature selection methods. Our model employed a precise but compact way to construct the model with complex set of rules and their corresponding actions. It was chosen for several reasons like powerful visualization, compact and structured presentation, easier to prevent error, avoid incompleteness & inconsistency, modular knowledge organization, group related rules into single table, and combine tables to take decision.

Disadvantages:

- It is difficult or sometimes impossible to provide absolutely security through a useful system.
- These have to be updated continuously in order to detect new attacks.

Proposed System:

We have proposed a new feature selection method with Decision Table rules based algorithm. The new framework which builds by new feature selection method with DT algorithm, use the network intrusion dataset with labeled samples. This labeled dataset then used by some other kinds of bayes based, function based, tree based and rules based classifier. Among them best two classifier DT and BN are selected according to detection rate, false positive rate and cost. And also them, DT performs better than BN in all kind of outputs for any number of features. However, it takes more time to build the model.

Advantages:

- Provides Security.

Modules:

- Intrusion Detection system.
- Decision Table.
- Bayesian Network.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	:	Pentium –III
RAM	:	256 MB (min)
Hard Disk	:	20 GB

Key Board	:	Standard Windows Keyboard
Mouse	:	Two or Three Button Mouse
Monitor	:	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.
Database	:	MySQL 5.0
Database Connectivity	:	JDBC