**Intrusion Detection System using KDD dataset**

**Synopsis**

Development of internet or mobile technology number of users increases day by day which also makes ease of communication. But the use of lots of internet network compromise with rigorous type of security threats or intrusion which persuade the performance of the system. Due to the lack of satisfaction in intrusion detection is makes possible to develop such system which can detect the intrusion efficiently.

Now a days the use of internet and multimedia technology is growing rapidly, it facilitate us for the purpose of communication or sharing the resources but use of these technology our network suffered from the network security or information security. The security can be break by injecting the intrusion or threats in the network of the system. The security of these now becomes a very challenging task and for detection of the intrusion or threats various organization has started their work. With the use of the effective intrusion detection system we can protect or network or information. Intrusion detection is the ability of detection unsuitable, erroneous, or anomalous activity. It is the method of monitoring and analyzing the incident occurring in a computer system in order to perceive signs of security problems. Intrusion detection is an imperative component of infrastructure protection mechanism. An intrusion detection system is the most requisite part of the security infrastructure for the network linked to the internet because of the numerous ways to conciliating the stability and security of the network. IDS can be used to scrutinize computer or network for unauthorized activities. Predominantly, network based IDS scrutinize the network traffic coming into the network to detect, identify, and track the intruders. An intrusion detection system is categorized into two kinds: network based or host based system.

The network based attacks may be either misuse or anomaly based attacks. The network based attacks are detected from the interconnection of computer systems. Since the system communicates with each other, the attack is sent from one computer system to another computer system by the way of routers and switches. The misuse or signature based intrusion detection system detects the intrusion by comparing with its existing signatures in the database. If the detecting attacks and signatures match, it is an intrusion.

The signature based intrusions are called known attacks whenever the users are detecting the intrusion by matching with the signatures log files. The log file contains the list of known attacks detected from the computer system or networks. The anomaly based intrusion detection is called as unknown attacks and this attack is observed from network as it deviates from the normal attacks. The host based attacks are detected only from a single computer system and is easy to prevent the attacks. These attacks mainly occur from some external devices which are connected. The web based attacks are possible when systems are connected over the internet and the attacks can be spread into different systems through the email, chatting, downloading the material etc. Nowadays many computer systems are affected from web based dangerous attacks. To ensure performance for intrusion detection system, we can evaluate it basically using KDD intrusion detection datasets.

The KDD data set is a well known benchmark in the research of Intrusion Detection techniques. A lot of work is going on for the improvement of intrusion detection strategies while the research on the data used for training and testing the detection model is equally of prime concern because better data quality can improve offline intrusion detection. This paper presents the analysis of KDD data set with respect to four classes which are Basic, Content, Traffic and Host in which all data attributes can be categorized. The analysis is done with respect to two prominent evaluation metrics, Detection Rate (DR) and False Alarm Rate (FAR) for an Intrusion Detection System (IDS). As a result of this empirical analysis on the data set, the contribution of each of four classes of attributes on DR and FAR is shown which can help enhance the suitability of data set to achieve maximum DR with minimum FAR.

Network security is a foremost issue these days as the network usage is growing in multi-dimensions due to increased use of handheld devices. Intrusion Detection Systems can help detect malign intentions of network users without compromising the security of the host and the network. There are many machine learning algorithms available which can learn from the training data and can generalize when exposed to new untrained data. There are two types of intrusion detection technique, the first one is Misuse Detection that can catch the known attacks and hence works on the offline data and the other is Anomaly Detection which can detect any abnormal behaviour and hence can work well on online data. The KDD data set is a standard data set used for the research on intrusion detection systems.