**PROJECT ABSTRACT**

**Network Intrusion Detection System (NIDS)**

Department of Computer Science and Engineering

GITAM (Deemed to be University)

**PROBLEM STATEMENT**

Today, intrusion detection is one of the major concerns in the task of network administration and security. There is a need to safeguard the networks from known vulnerabilities and at the same time take steps to detect new and unseen, but possible, system abuses by developing more reliable and efficient intrusion detection systems. The system must be accurate in detecting attacks with the minimum number of false alarms (wrong detections).

**ABOUT IDS**

Intrusion detecting system can be classified as host-based and network-based.

• HOST-BASED IDS: Its data is collected from the records of various host activities, including audit record of operation system, system logs, application programs information, and so on.

• NETWORK-BASED IDS: Its data is mainly collected from the network generic stream going through network segments, such as: Internet packets.

Likewise, Intrusion Detection techniques fall into two categories

• ANOMALY DETECTION: is the attempt to identify malicious traffic based on deviations from established normal network traffic patterns.

• MISUSE DETECTION: is the ability to identify intrusions based on a known pattern for the malicious activity.

**SOLUTION**

An Artificial Neural Network based NIDS will be developed so that the accuracy at which the intrusions are detected increases. In this network intrusion detection system, by using the concept of ensemble binary classification and multi-boosting simultaneously it efficiently detects the attack with the low false alarm rate and even at high network traffic. With the use of the Dynamic multi-boosting and the database storage the time taken to detect the attacks has been decreased efficiently. By combining the concepts of the Artificial Neural network and the Data mining technique of classification the drawbacks of the later is overcome.

The NIDS we are going to develop is a **network-based IDS** and it is going to detect any **misuse** of the network resources (misuse detection) i.e. it detects malicious packets in a network.

The network intrusion detection system involves the capturing of the packet in real time and those packets that have been received are classified using our proposed model.

**TOOLS AND TECHNOLOGIES –** Wincap (Packet capturing tool), MySQL, Machine learning and Data mining.

**TEAM (B4, BATCH – D4)**

M. SWAROOP – 1210316426

V.R. KAUSHIK – 1210316458

J. RAHUL VARMA - 1210316419

B. ROHIT – 1210316405

**PROJECT GUIDE:** Prof. P.V. Nageshwara Rao